

<<网络攻防技术与实践>>

图书基本信息

书名：<<网络攻防技术与实践>>

13位ISBN编号：9787121138027

10位ISBN编号：7121138026

出版时间：2011-6

出版时间：电子工业出版社

作者：诸葛建伟

页数：509

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<网络攻防技术与实践>>

### 内容概要

诸葛建伟的《网络攻防技术与实践》是一本面向网络安全技术初学者和相关专业学生的基础书籍，全面介绍了网络攻防的基本理论知识、技术方法和工具软件。

在介绍每一部分网络攻防技术之后，通过一些自主设计和从社区借鉴的实践作业，来引导读者在具体实战答题过程中，更加深入地去理解所讲解的攻防理论知识与技术原理，并培养核心的安全攻防实战技能。

《网络攻防技术与实践》共分为四个部分12章，系统地介绍了网络攻防技术的基础知识体系、核心技术方法，并在每章中结合实际案例讲解、

hands-on动手实践、实践作业，来引导读者学习和掌握网络攻防的实战技能。

#### 本书附带的DVD

光盘中包含了各个章节的演示案例、hands-on实践作业与部分实战的视频演示或示范解答。

#### 本书支持网站

[netsec.ccert.edu.cn/hacking](http://netsec.ccert.edu.cn/hacking)上提供了搭建本书设计的网络攻防实验环境所需的定制虚拟机镜像，可供读者下载使用。

在某种程度上，本书也是一本网络攻防技术的参考手册。

本书适合于网络和系统安全技术的爱好者、信息安全专业学术、网络与系统安全方向的研究生、网络与系统管理员，以及网络安全从业人员。

## 作者简介

诸葛建伟，博士，现为清华大学网络与信息安全实验室副研究员、狩猎女神科研团队负责人、CCERT 应急响应组成员、著名开源信息安全研究团队the Honeynet Project的正式成员。以及中国蜜网项目组([WWW.honeynet.org.cn](http://WWW.honeynet.org.cn))团队发起人和现任负责人、信息安全领域培训讲师和自由撰稿人。期望与志同道合之士一起通过科研创新、开源开发、知识传播和社会服务，为提升中国互联网的安全水平以及国家信息安全软实力做出贡献。

# <<网络攻防技术与实践>>

## 书籍目录

### 第一部分 概述

#### 第1章 网络攻防技术概述

##### 1.1 网络攻防实际案例——黛蛇蠕虫

###### 1.1.1 黛蛇蠕虫事件过程

###### 1.1.2 黛蛇蠕虫机理

###### 1.1.3 黛蛇蠕虫的取证分析与追踪

###### 1.1.4 重现黛蛇蠕虫传播场景

##### 1.2 黑客与黑客道

###### 1.2.1 黑客与骇客

###### 1.2.2 黑客道起源

###### 1.2.3 黑客道的分化

###### 1.2.4 黑客道“现代史”

###### 1.2.5 中国的黑客道

##### 1.3 网络攻防技术概述

###### 1.3.1 网络攻防技术框架

###### 1.3.2 网络攻击剖析图

##### 1.4 物理攻击与社会工程学

###### 1.4.1 物理攻击

###### 1.4.2 社会工程学

##### 1.5 黑客道德与法律法规

###### 1.5.1 黑客应有的态度

###### 1.5.2 黑客道德

###### 1.5.3 法律法规

##### 1.6 小结

##### 实践作业

##### 参考与进一步阅读

#### 第2章 网络攻防实验环境

##### 2.1 虚拟化网络攻防实验环境

###### 2.1.1 为什么需要实验环境

###### 2.1.2 虚拟化网络攻防实验环境

##### 2.2 网络攻防实验环境配置

###### 2.2.1 网络攻防虚拟机镜像

###### 2.2.2 个人版网络攻防实验环境

###### 2.2.3 专业版网络攻防实验环境

##### 2.3 网络攻防的活动与竞赛形式

##### 2.4 小结

##### 实践作业

##### 参考与进一步阅读

### 第二部分 网络安全攻防技术与实践

#### 第3章 网络信息收集技术

##### 3.1 网络信息收集概述

##### 3.2 网络踩点

###### 3.2.1 网络踩点概述

###### 3.2.2 Web信息搜索与挖掘

###### 3.2.3 DNS与IP查询

## <<网络攻防技术与实践>>

3.2.4 网络拓扑侦察

3.2.5 利用网络踩点技术追踪“黑客”案例演示

3.2.6 动手实践：DNS与IP查询

3.3 网络扫描

3.3.1 网络扫描的目的与类型

3.3.2 主机扫描

3.3.3 端口扫描

3.3.4 系统类型探查

3.3.5 动手实践：nmap

3.3.6 漏洞扫描

3.3.7 动手实践：Nessus

3.3.8 网络扫描完整解决方案

3.4 网络查点

3.4.1 网络服务旗标抓取

3.4.2 通用网络服务查点

3.4.3 类UNIX平台网络服务查点

3.4.4 Windows平台网络服务查点

3.4.5 网络查点防范措施

3.5 小结

实践作业

参考与进一步阅读

第4章 网络嗅探与协议分析

4.1 网络嗅探

4.1.1 网络嗅探技术概述

4.1.2 网络嗅探的原理与实现

4.1.3 网络嗅探器软件

4.1.4 网络嗅探的检测与防范

4.1.5 动手实践：tcpdump

4.2 网络协议分析

4.2.1 网络协议分析技术

4.2.2 网络协议分析工具Wireshark

4.2.3 动手实践：Wireshark

4.3 小结

实践作业

参考与进一步阅读

第5章 TCP/IP网络协议攻击

5.1 TCP/IP网络协议栈攻击概述

5.1.1 网络安全属性与攻击模式

5.1.2 TCP/IP网络协议栈安全缺陷与攻击技术

5.1.3 原始报文伪造技术及工具

5.2 网络层协议攻击

5.2.1 IP源地址欺骗

5.2.2 ARP欺骗

5.2.3 ICMP路由重定向攻击

5.3 传输层协议攻击

5.3.1 TCP RST攻击

5.3.2 TCP 会话劫持攻击

## <<网络攻防技术与实践>>

5.3.3 TCP SYN Flood拒绝服务攻击

5.3.4 UDP Flood拒绝服务攻击

5.4 TCP/IP网络协议栈攻击防范措施

5.5 小结

实践作业

参考与进一步阅读

第6章 网络安全防范技术

6.1 安全模型

6.2 网络防范技术与系统

6.2.1 防火墙技术概述

6.2.2 防火墙技术和产品

6.2.3 Linux开源防火墙：netfilter/iptables

6.2.4 动手实践：防火墙配置

6.2.5 其他网络防御技术

6.3 网络检测技术与系统

6.3.1 入侵检测技术概述

6.3.2 开源网络入侵检测系统：Snort

6.3.3 动手实践：Snort

6.4 网络安全事件响应技术

6.5 小结

实践作业

参考与进一步阅读

第三部分 系统安全攻防技术与实践

第7章 Windows操作系统安全攻防

7.1 Windows操作系统基本框架概述

7.1.1 Windows操作系统的发展与现状

7.1.2 Windows操作系统的基本结构

7.2 Windows操作系统的安全体系结构与机制

7.2.1 Windows安全体系结构

7.2.2 Windows身份认证机制

7.2.3 Windows授权与访问控制机制

7.2.4 Windows安全审计机制

7.2.5 Windows的其他安全机制

7.3 Windows远程安全攻防技术

7.3.1 Windows系统的安全漏洞生命周期

7.3.2 Windows远程口令猜测与破解攻击

7.3.3 Windows网络服务远程渗透攻击

7.3.4 动手实践：Metasploit Windows Attack

7.4 Windows本地安全攻防技术

7.4.1 Windows本地特权提升

7.4.2 Windows敏感信息窃取

7.4.3 Windows掩踪灭迹

7.4.4 Windows远程控制与后门程序

7.5 小结

实践作业

参考与进一步阅读

第8章 Linux操作系统安全攻防

## &lt;&lt;网络攻防技术与实践&gt;&gt;

## 8.1 Linux操作系统基本框架概述

## 8.1.1 Linux操作系统发展与现状

## 8.1.2 Linux系统结构

## 8.2 Linux操作系统安全机制

## 8.2.1 Linux身份认证机制

## 8.2.2 Linux授权与访问控制机制

## 8.2.3 Linux安全审计机制

## 8.3 Linux系统远程攻防技术

## 8.3.1 Linux远程口令字猜测攻击

## 8.3.2 Linux网络服务远程渗透攻击

## 8.3.3 攻击Linux客户端程序和用户

## 8.3.4 攻击Linux路由器和监听器

## 8.3.5 动手实践：使用Metasploit进行Linux远程渗透攻击

## 8.4 Linux系统本地安全攻防技术

## 8.4.1 Linux本地特权提升

## 8.4.2 Linux系统上的消踪灭迹

## 8.4.3 Linux系统远程控制后门程序

## 8.5 小结

## 实践作业

## 参考与进一步阅读

## 第9章 恶意代码安全攻防

## 9.1 恶意代码基础知识

## 9.1.1 恶意代码定义与分类

## 9.1.2 恶意代码发展史

## 9.1.3 计算机病毒

## 9.1.4 网络蠕虫

## 9.1.5 后门与木马

## 9.1.6 僵尸程序与僵尸网络

## 9.1.7 Rootkit

## 9.2 恶意代码分析方法

## 9.2.1 恶意代码分析技术概述

## 9.2.2 恶意代码分析环境

## 9.2.3 恶意代码静态分析技术

## 9.2.4 动手实践：恶意代码文件类型识别、脱壳与字符串提取

## 9.2.5 恶意代码动态分析技术

## 9.2.6 动手实践：分析Crackme程序

## 9.3 小结

## 实践作业

## 参考与进一步阅读

## 第10章 软件安全攻防——缓冲区溢出和Shellcode

## 10.1 软件安全概述

## 10.1.1 软件安全漏洞威胁

## 10.1.2 软件安全困境

## 10.1.3 软件安全漏洞类型

## 10.2 缓冲区溢出基础概念

## 10.2.1 缓冲区溢出基本概念与发展过程

## 10.2.2 缓冲区溢出攻击背景知识

## <<网络攻防技术与实践>>

10.2.3 缓冲区溢出攻击原理

10.3 Linux平台上的栈溢出与Shellcode

10.3.1 Linux平台栈溢出攻击技术

10.3.2 Linux平台的Shellcode实现技术

10.4 Windows平台上的栈溢出与Shellcode

10.4.1 Windows平台栈溢出攻击技术

10.4.2 Windows平台Shellcode实现技术

10.5 堆溢出攻击

10.6 缓冲区溢出攻击的防御技术

10.7 小结

实践作业

参考与进一步阅读

第四部分 Web安全攻防技术与实践

第11章 Web应用程序安全攻防

11.1 Web应用程序体系结构及其安全威胁

11.1.1 Web应用体系结构

11.1.2 Web应用安全威胁

11.2 Web应用安全攻防技术概述

11.2.1 Web应用的信息收集

11.2.2 攻击Web服务器软件

11.2.3 攻击Web应用程序

11.2.4 攻击Web数据内容

11.2.5 Web应用安全防范措施

11.3 SQL注入

11.3.1 SQL注入攻击原理

11.3.2 SQL注入攻击步骤和过程

11.3.3 SQL注入攻击工具

11.3.4 SQL注入攻击实例

11.3.5 SQL注入攻击防范措施

11.4 XSS跨站脚本攻击

11.4.1 XSS攻击技术原理

11.4.2 XSS攻击类型

11.4.3 XSS攻击实例

11.4.4 XSS攻击防范措施

11.5 小结

课外实践作业

参考与进一步阅读

第12章 Web浏览器安全攻防

12.1 Web浏览器的技术发展与安全威胁

12.1.1 Web浏览器战争与技术发展

12.1.2 Web浏览的安全问题与威胁

12.2 Web浏览端的渗透攻击威胁——网页木马

12.2.1 网页木马安全威胁的产生背景

12.2.2 网页木马的机理分析

12.2.3 网页木马的检测与分析技术

12.2.4 网页木马实际案例分析

12.2.5 动手实践——Web浏览器渗透攻击实验

## <<网络攻防技术与实践>>

12.2.6 网页木马防范措施

12.3 揭开网络钓鱼的黑幕

12.3.1 网络钓鱼技术概述

12.3.2 网络钓鱼攻击的技术内幕

12.3.3 网络钓鱼攻击的防范

12.4 小结

课外实践作业

参考与进一步阅读

## 章节摘录

1.4.1 物理攻击 物理攻击是指攻击者通过各种技术手段绕开物理安全防护体系，从而进入受保护的设施场所或设备资源内，获取或破坏信息系统物理媒体中受保护信息的攻击方式。物理攻击通常需要攻击者真正入侵到受保护的物理空间里，存在着很大风险与挑战，常见于军事、情报部门的特殊行动，以及恐怖及犯罪活动。

物理攻击分为暴力型和技巧型两种方式，暴力型主要依靠装备武器的武装人员，通过破坏性手段对物理安全防护体系进行摧毁，然后进入受保护区域接触目标，达到获取或破坏的目的。

暴力型物理攻击并没有精巧的技术手段与方法，主要依赖高科技武器的威力或武装人员的战斗技巧。而技巧型物理攻击则是人类智慧与行动力的完美结合，期望的目标是在神不知鬼不觉中攻破包括人类守卫在内的物理安全防护体系，在不触动安全警报的情况下，获取或破坏秘密信息。

技巧型物理攻击主要的应用场景是情报部门特工和间谍秘密完成特定的反恐或渗透任务，由于过程紧张刺激，充满悬疑，并常使用吸引眼球的高科技装备，因此历来成为好莱坞电影及国内外影视剧的热门选题。

在大量该类型的好莱坞电影中，最为著名的莫过于《碟中谍》系列与邦德007系列电影。

最经典的片段是《碟中谍1》之潜入中央情报局偷取NOC名单的场景：中央情报局的绝密文件NOC名单保存在一个具有严密安全保护的密室中，只有被授权的人通过3层身份验证才能接触到，而密室周边有高科技的声音和压力感应器，一旦有任何人入侵导致的异常都会触发警报。

主人公通过假扮成消防员混进大楼，通过房间上层的通道入侵，在同伴的帮助下支开管理员，成功地绕开了身份验证。

主人公就在被悬空吊在空中，接着破解计算机的口令后成功获取了NOC名单。

另外，实施技巧型物理攻击的主角还可能包括一些“犯罪分子”，《偷天陷阱》中肖恩·康纳利饰演的艺术大盗、《偷天换日》中的盗金三人组、《越狱》团队等。

在《越狱》中，闯入Company总部偷取Scylla是一个典型的技巧型物理攻击场景：Michael一行人为了获得异常珍贵的资源Scylla，必须潜入Company内部。

他们面临的是两堵墙，一堵混凝土墙，一堵玻璃墙，而且期间不能发出声音，不能触碰地面，甚至不能发出任何多余的热量。

他们利用强大的电磁场来破坏结实的混凝土墙，根据建筑和力学工程原理挖出一个洞；利用液氮的冷却技术防止人体发出的热量能发热传感器的安全警报；巧妙地搭建一个空桥越过障碍；最终突破了玻璃墙成功穿越，并故意引诱监护者来帮助“保护”他们成功逃脱。

## <<网络攻防技术与实践>>

### 编辑推荐

作为一本面向网络安全技术初学者和相关专业学生的基础书籍，诸葛建伟的《网络攻防技术与实践》内容上更多的是在笔者个人教学、科研和实践经验的基础之上，对网络攻防的基本理论知识、技术方法、工具软件进行的系统性整理与组织，同时结合了笔者在北大开设的相关课程授课经验，在介绍每一部分网络攻防技术之后，通过一些自主设计和从社区借鉴的实践挑战，来引导读者在具体实践解决挑战过程中，更加深入地去理解所讲解的网络攻防理论知识与技术原理，并培养起核心的安全攻防实战技能。

<<网络攻防技术与实践>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>