网络攻防技术

实训教程

赖小卿　杨育斌　主　编
李　强　黎权友　冯斌斌　副主编

清华大学出版社

网络攻防技术

实训教程

赖小卿　杨育斌　主　编
李　强　黎权友　冯斌斌　副主编

清华大学出版社
北京

内 容 简 介

本教材基于蓝盾信息安全攻防平台系统进行网络攻防实验，是校企合作的成功典范。教材中每个实验通过背景描述和工作原理对我们所处网络的信息安全现状和实验原理进行分析，以使读者更好地理解网络攻防技术；然后用基于虚拟靶机的实验方法，通过详细的实验步骤，对攻防技术的实现进行实际操作，并在实验后通过问题答辩温习、巩固攻防技术的知识。

本教材分为三部分，共 18 章，分别从主机安全、网络攻防、病毒攻防三个方面讲解了网络攻防技术，涵盖了目前流行的各种实用技术和常用工具。

本教材适于讲授网络攻防课程的老师、学习网络攻防技术的学生，以及其他想学习黑客基础知识的人员学习使用。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

网络攻防技术实训教程/赖小卿，杨育斌主编. —北京：清华大学出版社，2014
ISBN 978-7-302-35909-6

Ⅰ. ①网… Ⅱ. ①赖… ②杨… Ⅲ. ①计算机网络—安全技术—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 061897 号

安徽大学图书馆 藏书 www.lib.ahu.edu.cn

责任编辑：陈砺川
封面设计：傅瑞学
责任校对：袁　芳
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：20　　**字　　数**：484 千字
版　　次：2014 年 7 月第 1 版　　**印　　次**：2014 年 7 月第 1 次印刷
印　　数：1～2000
定　　价：39.00 元

产品编号：057682-01

前言

FOREWORD

一、教材编写背景

Internet是一种开放和标准的面向所有用户的技术，其资源通过网络共享。资源共享和信息安全是一对矛盾。计算机网络资源共享的进一步加强所带来的信息安全问题日益突出，各种计算机病毒和网上黑客（Hackers）对Internet的攻击越来越激烈，许多网站遭受破坏的事例不胜枚举。

目前社会上介绍网络安全攻防技术的教材并不少，但针对高职院校教学特点而量身定做的网络攻防技术教材并不多，能够真正指导学生实际动手做的网络攻防的实训教材更是少之又少。本教材正弥补了这个缺口，最大的特点是，所有的案例均由在高职院校从事网络安全教学的两位专职教师，在信息安全技术行业的上市企业多位一线工程师的帮助下共同整理完成的。

二、教材主要内容

第一部分（第1～5章）主机安全

本部分主要通过系统安全、口令破解、Apache安全配置、数据库安全、安全协议这5个章节讲解。系统安全分为Windows 2003系统安全和Linux系统安全；口令破解分为Windows密码破解、Linux口令破解；Apache安全配置分为Apache安全配置的实现和Apache日志审计；数据库安全分为SQL注入和防范SQL注入；安全协议分为TCP/IP协议分析、IPSec-IP安全协议、SSL安全套接层实现网络安全通信。

第二部分（第6～14章）网络攻防

本部分主要通过信息搜集、漏洞扫描、网络嗅探、缓冲区溢出、拒绝服务攻击、欺骗攻击、特洛伊木马、防火墙、蜜罐技术这9个章节讲解。信息搜集分为主机发现、端口扫描；漏洞扫描分为Web漏洞扫描器、FTP弱口令扫描器、综合扫描与安全评估；网络嗅探分为明文嗅探、原始套接字；缓冲区溢出分为本地缓冲区溢出、远程溢出；拒绝服务攻击分为洪泛攻击、DDoS攻击；欺骗攻击为ARP欺骗；特洛伊木马分为网页木马和木马免杀；防火墙为iptables应用；蜜罐技术为蜜罐（HoneyPot）捕获。

第三部分（第15～18章）病毒攻防

本部分主要通过引导区病毒、脚本病毒、宏病毒、蠕虫病毒这4个章节讲解。引导区病毒为BMW病毒；脚本病毒为脚本及恶意网页病毒；宏病毒为

Word 宏病毒；蠕虫病毒为“暴风一号”蠕虫病毒。

三、本教材的特点

该教材的出版得到高职骨干院校广东科学技术职业学院的计算机工程技术学院以及蓝盾信息安全技术股份有限公司大力支持，可以说，该教材是校企合作的一个成功典范。教材结构清晰，通俗易懂，每个实验通过背景描述和工作原理对我们所处网络的信息安全现状和实验原理进行分析，以使读者更好地理解网络攻防技术；然后用基于虚拟靶机的实验方法，通过详细的实验步骤，对攻防技术的实现进行实际操作，并在实验后通过问题答辩温习、巩固攻防技术的知识。

教材里面涉及的很多内容都来源于真实的企业案例，使得本教材的内容具有很强的实践性和真实性，教材中介绍的案例操作步骤描述清楚、讲解透彻并附有相关的截图，这样不仅最大限度地保证了案例的直观性，也保证了学生能够按照教材提供的每个真实场景，亲自动手完成一系列网络安全攻防的实训任务。

四、教材的读者对象

本教材适用于教授网络攻防课程的老师、学习网络攻防技术的学生以及其他想学习黑客基础知识的人员。

五、编者感言

除本教材主创人员之外，编者还要特别感谢梁琦、石龙兴、龙志强等人为此书付出的心血和努力，他们在资料的整理、环境的搭建与测试方面为这本教材的最后完成提供了很大的帮助和支持。由于编者水平有限，加上本书涉及的内容较广泛，理论点讲解的过程中难免存在一些疏漏之处，恳请广大读者和专家批评、指正。

编　者

2014 年 2 月

试读结束：需要全本请在线购买： www.ertongbook.com

目录

CONTENTS

第一部分 主机安全

第二部分 网络攻防

第三部分 病毒攻防

试读结束：需要全本请在线购买： www.ertongbook.com

第一部分　主机安全

第1章 系统安全

Chapter 1

1.1 Windows 2003 系统安全

1.1.1 背景描述

Windows Server 2003 包含了基于 Windows 2000 Server 构建的核心技术，是经济划算的优质服务器操作系统。Windows Server 2003 在任意规模的企业里都能成为理想的服务器平台，它所具有的可靠性、可用性、可伸缩性和安全性使其成为高度可靠的平台，同时也成为广大用户所青睐的产品。

随着网络应用的不断深入，处于网络中的敏感信息被集中保存在服务器或存储设备中，甚至在网络客户端也往往保存着大量的敏感数据。当这些数据由于硬件或系统故障导致丢失或者被恶意用户非法访问时，将对网络用户造成难以估量的巨大损失。而在技术的时代，不可能有完美无缺的操作系统，由于 Windows 系统存在大量高度危险的漏洞，而服务器又都是通过各种方式接入 Internet，因此这些漏洞又往往被恶意用户作为远程攻击的手段。另外，层出不穷的蠕虫类病毒借助 Internet 和局域网广泛传播，不仅会严重影响网络的传输性能，而且将直接导致网络服务故障，造成潜在的安全隐患。因此，加强系统安全，保护系统不受入侵显得尤为重要。

1.1.2 工作原理

多年以来，许多客户都使用 Windows Server 2003 作为服务器操作系统，随着技术的发展以及网络的普及，服务器安全问题层出不穷，这就对 Windows Server 2003 的安全提出了更高的要求。加强 Windows Server 2003 系统的安全可以从以下几个方面入手。

1. 目录权限的配置

(1) 除系统所在分区之外的所有分区都赋予 Administrators 和 SYSTEM 有完全控制权，之后再对其下的子目录作单独的目录权限，如果 Web 站点目录，要为其目录权限分配一个与之对应的匿名访问账号并赋予它有修改权限，如果想使网站更加安全，可以分配只读权限并对特殊的目录作可写权限。

(2) 系统所在分区下的根目录都要设置为不继承父权限，之后为该分区只赋予 Administrators 和 SYSTEM 有完全控制权。

(3) 因为服务器只有管理员有本地登录权限，所在要配置 Documents and Settings 这个目录权限只保留 Administrators 和 SYSTEM 有完全控制权，其下的子目录做同样处理。另外还有一个隐藏目录也需要同样设置。因为如果安装有 PCAnyWhere，那么它的配置信息都保存在其下，使用 webshell 或 FSO 可以轻松地调取这个配置文件。

(4) 配置 Program Files 目录，为 Common Files 目录之外的所有目录赋予 Administrators 和 SYSTEM 有完全控制权。

(5) 配置 Windows 目录，其实这一块主要是根据自身的情况配置，如果使用默认的安全设置也是可行的，不过还是应该进入 system32 目录下，将 cmd. exe、ftp. exe、net. exe、scrrun. dll、shell. dll 这些杀手锏程序赋予匿名账号拒绝访问。

(6) 审核 MetBase. bin，C:\WINNT\system32\inetsrv 目录只有 Administrator，只允许 Administrator 用户读写。

2. 组策略配置

(1) 在用户权利指派下，从通过网络访问此计算机中删除 Power Users 和 Backup Operators。

(2) 启用不允许匿名访问 SAM 账号和共享。

(3) 启用不允许为网络验证存储凭据或 Passport。

(4) 从文件共享中删除允许匿名登录的 DFS $ 和 COMCFG。

(5) 启用交互登录：不显示上次的用户名。

(6) 启用在下一次密码变更时不存储 LANMAN 哈希值。

(7) 禁止 IIS 匿名用户在本地登录。

3. 本地安全策略设置

执行“开始”菜单→“管理工具”→“本地安全策略”命令。

(1) 本地策略→审核策略

审核策略更改　成功　失败

审核登录事件　成功　失败

审核对象访问失败

审核过程跟踪　无审核

审核目录服务访问失败

审核特权使用失败

审核系统事件　成功　失败

审核账户登录事件　成功　失败

审核账户管理　成功　失败

注意：在设置审核登录事件时选择记录失败，这样在事件查看器里的安全日志就会记录登录失败的信息。

(2) 本地策略→用户权限分配

关闭系统：只有 Administrators 组，将其他全部删除。

通过终端服务拒绝登录：加入 Guests、User 组。

通过终端服务允许登录：只加入 Administrators 组，将其他全部删除。

(3) 本地策略→安全选项

交互式登录：不显示上次的用户名 启用

网络访问：不允许 SAM 账户和共享的匿名枚举 启用

网络访问：不允许为网络身份验证储存凭证 启用

网络访问：可匿名访问的共享 全部删除

网络访问：可匿名访问的命令 全部删除

网络访问：可远程访问的注册表路径全部删除

网络访问：可远程访问的注册表路径和子路径全部删除

账户：重命名来宾账户 重命名一个账户

账户：重命名系统管理员账户 重命名一个账户

4. 本地账户策略

(1) 在“账户策略”→“密码策略”选项中设定以下内容。

① 密码复杂性要求启用。

② 密码长度最小值 6 位。

③ 强制密码历史 5 次。

④ 最长存留期 30 天。

(2) 在“账户策略”→“账户锁定策略”选项中设定以下内容。

① 账户锁定 3 次错误登录。

② 锁定时间 20min。

③ 复位锁定计数 20min。

5. 修改注册表配置

(1) 更改注册表

通过更改 local_machine\system\currentcontrolset\control\lsa-restrictanonymous＝1 来禁止 139 空连接。

(2) 修改数据包的生存时间(TTL)值

```
hkey_local_machine\system\currentcontrolset\services\tcpip\parameters
defaultttl reg_dword 0-0xff(0~255,十进制,默认值为 128)
```

(3) 防止 SYN 洪水攻击

```
hkey_local_machine\system\currentcontrolset\services\tcpip\parameters
synattackprotect reg_dword 0x2(默认值为 0x0)
```

(4) 禁止响应 ICMP 路由通告报文

```
hkey_local_machine\system\currentcontrolset
\services\tcpip\parameters\interfaces\interface
performrouterdiscovery reg_dword 0x0(默认值为 0x2)
```

(5) 防止 ICMP 重定向报文的攻击

```
hkey_local_machine\system\currentcontrolset\services\tcpip\parameters
enableicmpredirects reg_dword 0x0(默认值为 0x1)
```

(6) 不支持 IGMP 协议

```
hkey_local_machine\system\currentcontrolset\services\tcpip\parameters
```

(7) 修改 3389 默认端口

运行 Regedt32 并转到此项：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations
\RDP-Tcp
```

找到 PortNumber 子项，用户会看到值 00000D3D，它是 3389 的十六进制表示形式。使用十六进制数值修改此端口号，并保存新值。

禁用不必要的服务，不但可以降低服务器的资源占用减轻负担，而且可以增强安全性。例如：

```
igmplevel reg_dword 0x0(默认值为 0x2)
```

(8) 设置 ARP 缓存老化时间设置

```
hkey_local_machine\system\currentcontrolset\services:\tcpip\parameters
arpcachelife reg_dword 0-0xffffffff(秒数,默认值为 120s)
arpcacheminreferencedlife reg_dword 0-0xffffffff(秒数,默认值为 600)
```

(9) 禁止死网关监测技术

```
hkey_local_machine\system\currentcontrolset\services:\tcpip\parameters
enabledeadgwdetect reg_dword 0x0(默认值为 0x1)
```

(10) 不支持路由功能

```
hkey_local_machine\system\currentcontrolset\services:\tcpip\parameters
ipenablerouter reg_dword 0x0(默认值为 0x0)
```

6. 禁用服务

- Application Experience Lookup Service
- Automatic Updates
- BITS
- Computer Browser
- DHCP Client
- Error Reporting Service
- Help and Support
- Network Location Awareness
- Print Spooler
- Remote Registry
- Secondary Logon
- Server
- Smartcard
- TCP/IP NetBIOS Helper

试读结束：需要全本请在线购买： www.ertongbook.com