网络攻防原理与实践

主编 邓 涛 单广荣

非外借

科学出版社

基金项目：甘肃省重点学科计算机科学与技术

网络攻防原理与实践

主编　邓　涛　单广荣
参编　郝玉胜　李　娜

科学出版社
北京

内 容 简 介

本书内容涵盖网络原理、组网技术、网络应用和网络攻防等几个方面，实践项目既包含了对网络原理的理解和运用，又融合了当今网络工程的某些主流技术，适应了基础与验证性、综合和设计性两种不同层次的要求。全书共 10 章，第 1 章介绍网络扫描与嗅探；第 2 章介绍密码破解技术；第 3 章介绍数据库攻击技术；第 4 章介绍网络欺骗技术；第 5 章介绍日志清除技术；第 6 章介绍操作系统安全策略配置技术；第 7 章介绍缓冲区溢出技术；第 8 章介绍恶意代码技术；第 9 章介绍逆向工程技术；第 10 章介绍网络设备攻击技术。

本书可作为高等学校软件工程和计算机科学与技术本科专业、高职高专计算机及相关专业的辅导教材，也可作为全国计算机等级考试的辅导教材，还可供从事软件开发以及相关领域的工程技术人员参考使用。

图书在版编目(CIP)数据

网络攻防原理与实践 / 邓涛，单广荣主编. —北京：科学出版社，2017.11
ISBN 978-7-03-055368-3

Ⅰ. ①网… Ⅱ. ①邓… ②单… Ⅲ. ①计算机网络－网络安全 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 277240 号

责任编辑：于海云 / 责任校对：郭瑞芝
责任印制：吴兆东 / 封面设计：迷底书装

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京京华虎彩印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2017 年 11 月第 一 版 开本：787×1092 1/16
2018 年 1 月第二次印刷 印张：18 1/2
字数：420 000

定价：65.00 元

(如有印装质量问题，我社负责调换)

前　言

21 世纪信息成为一种重要的战略资源。信息安全牵涉到国家安全、社会稳定，必须采取措施确保信息安全。信息安全人才培养是我国国家信息安全保障体系建设的基础和先决条件。在信息安全领域中，网络安全问题尤为突出。目前，信息安全的主要威胁来自基于网络的攻击。随着网络安全问题的层出不穷，网络安全人才短缺的问题亟待解决。在我国，高校是培养网络安全人才的核心力量。网络攻击与防护是网络安全的核心内容，也是国内外各个高校信息安全相关专业的重点教学内容。网络攻击与防护具有工程性、实践性的特点，对实验室环境提出了更高的要求。

目前，我国大部分高校开设的网络安全课程(或相关课程)的主要内容包括：网络应用服务安全、防火墙、入侵检测、虚拟专用网、网络攻击与防护等，其中网络攻击与防护是应用性、实践性、综合性最强的一部分核心内容。学生要很好地掌握这些内容，除了课堂学习，主要通过实验的实际操作来加深理解和掌握工程性技能。当前国内高校的信息安全实验室中涉及网络攻防的内容较少且较为松散，无法满足我国高校越来越注重网络安全和相关实践的需求。因此，引入专业的网络攻防实验原理是十分重要和必要的。

网络技术的特点是理论性与实践性都很强，涉及的知识面较广，概念繁多，并且比较抽象，仅靠课堂教学，学生难以理解和掌握。在学习网络攻防的一般性原理和技术的基础上，必须通过一定的实践训练，才能真正掌握其内在机理。然而，在课时有限的情况下如何组织网络攻防原理与实践实施的手段，使之既能配合课堂教学，加深对所学内容的理解，又能紧跟网络技术的发展，培养和提高学生的实际操作技能，却不是件容易的事。为了进一步提高学生计算机网络技术的综合应用和设计创新能力，西北民族大学数学与计算机科学学院联合西普科技于 2011 年共同建立了计算机网络与信息安全实验室。西普科技一直专注于实验教学系统，以专业、卓越、优质的服务博得了众多高校客户的信任。目前，全国已有超过 500 家单位在使用西普科技所提供的产品和服务。

本书正是在西普科技提供的产品和服务基础上，针对网络扫描与嗅探、密码破解、数据库攻击、网络欺骗、日志清除、操作系统安全、缓冲区溢出、恶意代码、逆向工程及网络设备攻击等常见网络攻击技术进行原理与实践的介绍。同时，该系统提供实验管理及实验工具等多种扩展接口，方便学校添加新实验，并提供校企合作模式进行实验课程的开发。

本书由西北民族大学数学与计算机科学学院邓涛(负责全书统筹及策划，提纲撰写，撰写并且修改第 1～3 章，全书校对)、单广荣(负责策划和全书校对)主编，郝玉胜(负责撰

写并且修改第 4～7 章)、李娜(负责撰写并且修改第 8～10 章)参编。作者均为多年从事计算机网络教学、科研的一线教师，有丰富的教学、实践经验，本书力求做到结构严谨、概念准确、内容组织合理、语言使用规范。

本书在写作的过程中，得到诸多专家和领导的热情支持与指导，在此一并表示衷心感谢。由于作者水平有限，加之时间仓促，书中不足之处在所难免，恳请读者批评指正。

编　者

2017 年 8 月

目　录

第 1 章　网络扫描与嗅探

1.1　网络连通探测实验

实验目的

(1) 了解网络连通测试的方法和工作原理。
(2) 掌握 ping 命令的用法。

实验原理

1. ping 原理

ping 命令用来探测主机到主机之间是否可通信，如果不能 ping 到某台主机，则表明不能和这台主机建立连接。ping 使用的是 ICMP，它发送 ICMP 回送请求消息给目的主机。ICMP 规定：目的主机必须返回 ICMP 回送应答消息给源主机。如果源主机在一定时间内收到应答，则认为主机可达。ICMP 通过 IP 发送，IP 是一种无连接的、不可靠的数据包协议。ping 不通一个地址，并不一定表示这个 IP 不存在或者没有连接在网络上，因为对方主机可能作了限制，如安装了防火墙，因此 ping 不通并不表示不能使用 FTP 或者 Telnet 连接。

2. ping 工作过程

假定主机 A 的 IP 地址是 192.168.1.1，主机 B 的 IP 地址是 192.168.1.2，在同一子网内，则当在主机 A 上运行“ping 192.168.1.2”后，会发生些什么呢?

首先，ping 命令会构建一个固定格式的 ICMP 请求数据包，然后由 ICMP 将这个数据包连同地址 192.168.1.2 一起交给 IP 层协议(和 ICMP 一样，实际上是一组后台运行的进程)，IP 层协议将以地址 192.168.1.2 作为目的地址，本机 IP 地址作为源地址，加上一些其他的控制信息，构建一个 IP 数据包，并在一个映射表中查找出 IP 地址 192.168.1.2 所对应的物理地址(也叫 MAC 地址，这是数据链路层协议构建数据链路层的传输单元——帧所必需的)，一并交给数据链路层。后者构建一个数据帧，目的地址是 IP 层传过来的物理地址，源地址则是本机的物理地址，还要附加上一些控制信息，依据以太网的介质访问规则，将它们传送出去。

主机 B 收到这个数据帧后，先检查它的目的地址，并和本机的物理地址对比，如果符合，则接收，否则丢弃。接收后检查该数据帧，将 IP 数据包从帧中提取出来，交给本机的 IP 层协议。同样，IP 层检查后，将有用的信息提取后交给 ICMP，后者处理后，马上构建一个 ICMP 应答包，发送给主机 A，其过程和主机 A 发送 ICMP 请求包到主机 B 一模一样。

3. ping 命令详解

ping 命令格式如下：

```
ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count]
     [-s count] [[-j computer-list] | [-k computer-list]]
     [-w timeout]destination-list
```

参数说明如下。

-t：ping 指定的计算机直到中断，按 Ctrl+键停止。

-a：将地址解析为计算机名。例如，c:\>ping -a 127.0.0.1。

```
pinging china-hacker [127.0.0.1] with 32 bytes of data:(china-hacker
就是他的计算机名)
reply from 127.0.0.1: bytes=32 time<10ms ttl=128
reply from 127.0.0.1: bytes=32 time<10ms ttl=128
reply from 127.0.0.1: bytes=32 time<10ms ttl=128
reply from 127.0.0.1: bytes=32 time<10ms ttl=128
ping statistics for 127.0.0.1:packets: sent = 4, received = 4,
  lost = 0(0% loss),approximate
round trip times in milli-seconds:minimum = 0ms, maximum = 0ms,
  average = 0ms
```

-n count：发送 count 指定的 echo 数据包数，默认值为 4。

-l length：发送包含由 length 指定的数据量的 echo 数据包，默认为 32 字节，最大值是 65527。

-f：在数据包中发送“不要分段”标志。数据包就不会被路由上的网关分段。

-i ttl：将“生存时间”字段设置为 ttl 指定的值。

-v tos：将“服务类型”字段设置为 tos 指定的值。

-r count：在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少 1 台，最多 9 台计算机。

-s count：指定 count 指定的跃点数的时间戳。

-j computer-list：利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔(路由稀疏源)IP 允许的最大数量为 9。

-k computer-list：利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔(路由严格源)IP 允许的最大数量为 9。

-w timeout：指定超时间隔，单位为毫秒。

destination-list：指定要 ping 的远程计算机。

```
c:\>ping ds.internic.net
pinging ds.internic.net [192.20.239.132] with 32 bytes of data:
   (192.20.239.132 是他的 IP 地址)
reply from 192.20.239.132:bytes=32 time=101ms ttl=243
reply from 192.20.239.132:bytes=32 time=100ms ttl=243
```

```
reply from 192.20.239.132:bytes=32 time=120ms ttl=243
reply from 192.20.239.132:bytes=32 time=120ms ttl=243
```

实验要求

(1) 认真阅读和掌握本实验相关的知识点。

(2) 上机实现软件的基本操作。

(3) 得到实验结果，并加以分析生成实验报告。

注：因为实验所选取的软件版本不同，学生要有举一反三的能力，通过对该软件的使用能掌握运行其他版本或类似软件的方法。

实验步骤

ping 命令是一种 TCP/IP 实用工具，在 DOS 和 UNIX 系统下都有此命令。它在用户的计算机与目标服务器间传输一个数据包，再要求对方返回一个同样大小的数据包来确定两台网络机器是否连接相通。

(1) 在命令提示符窗口中输入 ping 以了解该命令的详细参数说明，如图 1-1 所示。

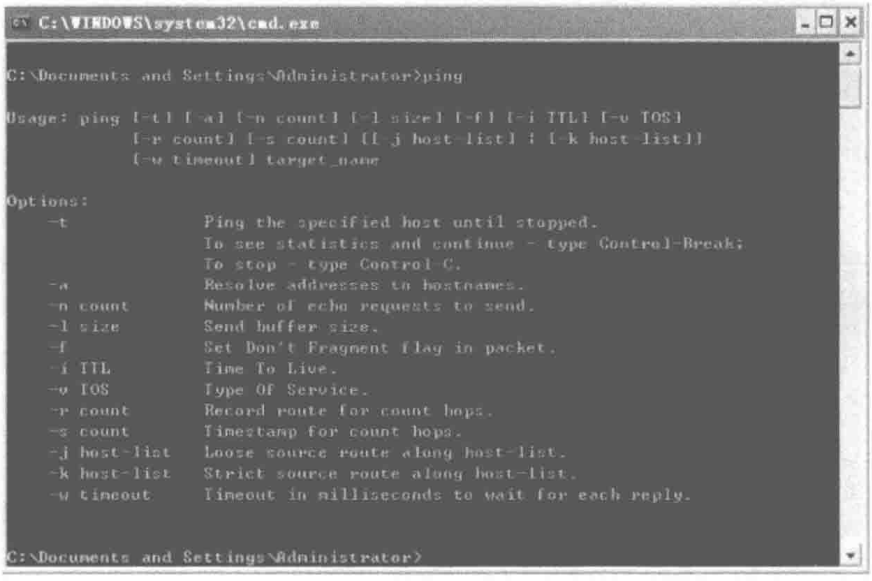

图 1-1　ping 命令参数帮助

(2) 输入 ping www.cuit.edu.cn，查看目标主机是否在线(需要配置 DNS)，如图 1-2 所示。

从返回的结果可以得到，目标主机可能不在线，或者开启了防火墙。

(3) 输入 ping 192.168.100.1，查看主机能否到达网关，如图 1-3 所示。

从返回结果可以得到，本主机能到达网关，说明网络是通的。

实验总结

通过 ping 命令查看主机网络的连通性是否正常。