计算机安全实验手册

Vincent J. Nestler　Wm. Arthur Conklin
Gregory B. White　Matthew P. Hirsch　著
汪青青　译

清华大学出版社

计算机安全实验手册

Vincent J. Nestler
Wm. Arthur Conklin
Gregory B. White
Matthew P. Hirsch
著

汪青青 译

清华大学出版社
北 京

Vincent J. Nestler, Wm. Arthur Conklin, Gregory B. White, Matthew P. Hirsch
Computer Security Lab Manual
EISBN: 0-07-225508-0

北京市版权局著作权合同登记号　图字：01-2006-3577 号

图书在版编目（CIP）数据

计算机安全实验手册 /（美）内思特（Nestler. V. J.）等著；汪青青译. —北京：清华大学出版社，2006.12
书名原文：Computer Security Lab Manual
ISBN 7-302-14123-1

Ⅰ. 计…　Ⅱ. ①内…　②汪…　Ⅲ. 电子计算机–安全技术–手册　Ⅳ. TP309-62

中国版本图书馆 CIP 数据核字（2006）第 134536 号

责任编辑：常晓波
责任校对：张　俭
责任印制：何　芊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 刷 者：北京密云胶印厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：26.5　**字　数**：641 千字
版　　次：2006 年 12 月第 1 版　　**印　　次**：2006 年 12 月第1 次印刷
书　　号：ISBN 7-302-14123-1/TP·8484
印　　数：1～3000
定　　价：49.00 元

关 于 作 者

Vincent Nestler，Capitol College 和 M.A.T. Education、Columbia University 的网络安全硕士，是一位有着超过 15 年网络管理和安全方面经验的网络工程顾问和技术教练员。曾在美国海军陆战预备队担任数据通信维护军官。设计并实施了针对国防情报系统机构（DISA）计算机紧急响应小组的海军训练。在其调任 DISA 期间，为联合广播系统担任助理操作员（训练）。他开发了计算机网络操作程序的课程。他是 Capitol College、DeVry Institute of Technology 以及 The Katharine Gibbs School 的网络和安全方面的副教授。专业认证包括 Red Hat 认证工程师、Microsoft 认证培训师、Microsoft 认证系统工程师、Cisco 认证网络工程师、以及 Security+。

Wm. Arthur Conklin，是德州大学 San Antonio 分校（UTSA）的 Center for Infrastructure Assurance and Security 的助理教授研究员。他是工商管理博士后，专攻信息系统和信息保障。Conklin 先生拥有 Washington University 的 B.A.，UTSA 的 M.B.A，以及加州 U.S. Naval Postgraduate School in Monterey 的电子工程双学位。他所感兴趣的研究领域是分布式系统的安全问题。Conklin 先生是 U.S. Navy 有着 10 年经验的老手，曾担任外部战争军官和工程值勤官，有超过 10 年的软件工程和项目管理经验。他是 McGraw-Hill 出版的 *Security+ Certification All-in-One Exam Guide* and *Principles of Computer Security: Security+ and Beyond* 的合著者。

Gregory White 博士自 1986 年以来就涉足计算机和网络安全工作。他在空军呆了 19 年，目前就职于空军预备队。1995 年从 Texas A&M University 获得计算机科学哲学博士。目前他担任 Center for Infrastructure Assurance and Security 的临时指导和技术指导，并且是 UTSA 计算机系的助理教授。目前他正发起多项研究，包括对影响计算机安全的组织问题的考察、高速入侵检测、基础设施保护，以及从安全性来计算投资收益的方法。他是几本计算机安全方面书籍的合著者，并发表了大量的文章和报告出版物。

Matthew Hirsch，Capitol College 的网络安全硕士，NEW Paltz 纽约州立大学（SUNY）物理学 B.A.，Katharine Gibbs School 计算机网络专业的副教授。有超过 15 年的系统和网络管理员经验。Deutsche Bank 的系统管理者，Sanwa Securities 和 Market Arts Software 的系统/网络管理员。纽约市一家非盈利性 ISP——Dorsar 的志愿管理员。在 1994 年为 Market Arts 建立了一个几乎完全安全，或者说极度安全的防火墙。

关于技术编辑

Mike Casper 的主要角色是财政服务行业的信息安全管理者，负责服务供应商的合规

性和监督。他对于估算全球厂商的安全状态有着广博的知识和经验。Mike 也曾在宾夕法尼亚州和北卡罗莱那州有着 9 年的高校讲师经历。Mike 的成就之一是合著了 *CompTIA Security + Examination*。他获得的认证包括：CompTIA Security+、安全认证网络专家（SCNP），以及认证的信息系统安全专家（CISSP）。

前　言

听过的会忘记
看见的会记住
做过的会理解　——孔子

对于学生来说，努力学习的成功与否依赖于几个因素，包括资料的复杂度和直接接触的程度。学习最复杂的科目不能只是在讲稿上被动地参与。真正学会并理解一个复杂问题的所有要素，需要更密切地探索素材。

计算机安全是个综合性科目，有许多复合领域、交迭规则以及非常特殊、错综复杂的技术现状。开发计算机安全方面熟练的专业人员需要定位几个部分，即技术和基于原理的知识，外加在操作中使用那个知识的实践经验。这本书的目的是协助模拟计算机安全知识库的实践体验部分。

这本书不是设计来涵盖计算机安全方面的所有特征的独立参考书。它旨在与基于原理的课本相结合，比如 McGraw-Hill 出版的 *Principles of Computer Security: Security + and Beyond*。这两种课程完美的结合提供了理解基本的计算机安全概念和技能的基础。

教学设计

安全方面的四个问题

本书安排了四个部分，每一部分都对应与网络和计算机安全相关联的问题。这些问题作为结构化的框架，建立在前一部分的基础之上，据此我们努力来开发对计算机安全原理连贯的理解。那些部分和问题是：

第 1 部分——网络如何工作？

第 2 部分——网络是怎样易受攻击的？威胁是什么？

第 3 部分——怎样防止对网络的伤害？

第 4 部分——在网络上怎样检测并响应攻击？

这四个问题建立在彼此的基础上。首先，在我们能看到存在的漏洞之前，理解网络是怎样工作的非常重要。研究了基于网络的漏洞和威胁之后，一定会期待着防止伤害网络的方法。最后，即使是在最安全的环境中，我们也必须做最坏的打算，并询问我们能怎样检测和应该怎样响应攻击。

实验习题设计

这本实验手册是特别设计的，允许教师灵活运用。关于设备和设置是相当灵活的，因此它们可以在 Windows、Linux 或使用虚拟机的 Mac 平台上实施。设备数量也相当灵活，

因此独立的网络和虚拟的网络都可用来部署。最后，实验的选择很灵活，因此并不期望每一个实验都被用到，而是选择合适的实验，用来支持在课程作业的原理部分中特定的概念。

这些实验习题的目的在于传授计算机和网络安全方面的技巧和概念。每个实验都有几个特征，允许在不会偏离重要概念的情况下灵活运用。

为 Windows 和 Linux 而准备的实验

大部分的实验练习都是针对 Windows 和 Linux 操作系统的。这不仅使学生们可以在自己所熟悉的操作系统上操作，而且可以用来在理解每个操作系统如何运作之间架起桥梁。

实验彼此独立

尽管这些实验根据所涵盖的内容和技巧而相互关联，但相对于配置和设置来说它们是独立的。这样就使得在实验的次序和重复方面有最大的灵活性。

实验以步进式来介绍

在本实验手册分成四个部分的同时，每一部分又进一步分成多章，把内容划分成多个逻辑组。这有助于对网络安全很陌生的学生循序渐进地开发他的知识并了解技巧和概念。

实验可以以主题的次序完成

不但实验练习根据那四个问题按内容分成了不同的组，而且针对当前实验之后的实验的参考也被分了不同的组。例如，可能想要执行一个与 FTP 相关的实验练习。可以从第 1 部分做 FTP 实验，它演示了 FTP 的用法；从第 2 部分做嗅探实验，它演示了 FTP 的漏洞；从第 3 部分做 SCP 实验，它演示了通过加密文件的传输来加固；以及从第 4 部分做日志分析实验，它可以揭露 FTP 服务器上的攻击。

大部分实验都有进一步学习的建议

在每一个实验的结尾都有进一步研究的建议。这些部分为学生指出正确的方向来探索更多内容。对于那些超前和提早完成了实验的学生而言，这些建议的实验提供了挑战，然而它们不必作为其它学生的要求。

虚拟机的使用

尽管所有的实验都可以在按配套 Web 站点上的说明所配置的计算机上执行，但强烈建议在诸如 Microsoft Virtual PC 或 VMWare 那样的虚拟机上执行那些实验。使用虚拟机有若干好处。

易于部署

一旦创建了虚拟机，就可以复制到所有的实验计算机上。

可以在 Linux 或 Mac 平台的 PC 上完成

只要满足了最低资源和软件需求，就可以在两种 PC（Linux 或 Mac）上完成实验。

一名学生，一台 PC，多台机器

如果用实际的 PC 机去建立实验，将至少需要 3 台 PC 机来创建完成所有实验所必需的网络。这意味着在拥有 30 台计算机的教室中，仅有 10 个实验能同时进行。通过使用虚拟机，全部的 30 台计算机都可以用来同时运行 30 个实验。

实验是可移动的——笔记本电脑

使用虚拟机的额外好处是在笔记本电脑上建立网络安全实验。这意味着学生不必非要去实验室做练习；他可以随时随地进行实验。

易于回滚

如果正确地配置，则每个实验练习结束后都不需要卸载或重新镜像计算机。所要做的只是退出虚拟机而不保存改变。如果虚拟硬盘驱动器被修改了，将原始文件复制回来只是个很简单的过程。

进一步实验的无限潜能

不像模拟器，每个虚拟机都使用实际的操作系统，这样就可以用来开发新的技术和/或考查其它的安全概念和软件，而只有相对很少的麻烦。

安全实验设置

所有的实验练习都有 a、b、c 或 d 的字母标记。“a”实验是基于 Windows 的练习，“b”实验是基于 Linux 的练习，而“c”实验是 Windows 和 Linux 的混合练习。带有 a、b、或 c 标记的实验规定在封闭的网络或虚拟 PC 上执行。“d”实验则需要在带有 Internet 访问的计算机上执行。

“a”实验

这些实验涉及一台 Windows XP Professional PC 机和一台 Windows 2000 Server。通常 XP PC 机将是攻击者，而服务器是防御者。

“b”实验

这些实验涉及 Linux 的 Red Hat 9 版本。一个将被配置为客户端，一个配置为服务器。通常 Linux 客户端将是攻击者，而服务器是防御者。

“c”实验

这些实验涉及 Windows 和 Linux PC 机的组合。Linux PC 机用作 SSH 和邮件服务器。

“d”实验

这些实验涉及带有 Internet 访问的主 PC 机。尽管大多数练习设计为没有 Internet 访问就能完成，但少数需要连接。Internet 连接允许学生进行搜索并看看现实世界所存在的间谍软件的影响。

注意，所有的计算机都有意配置了不坚固的密码。这是为了易于实验使用，并演示了不坚固密码的危险。第 3 部分中涵盖了更多坚固密码的创建和使用。

安全性实验需求和使用说明

安全性实验设置的详细需求和使用说明可以在 www.securitylabmanual.com 上找到。需求和使用说明因所要使用的平台和基本 OS 而异。

注意

由于许多厂商改善了他们的软件，本手册中所使用的有效版本可能不再可用了。同样，少数实验练习可能不完全按所写的那样工作，但通常仍然应该工作。请访问 www.securitylabmanual.com 查找更新和其他信息。

目　录

第 1 部分　网络基础——网络如何工作

第 2 部分　漏洞和威胁——网络能怎样被损坏

第 3 部分 预防——怎样防止对网络的伤害

第 4 部分 检测与响应——如何检测并响应攻击

第 1 部分　网络基础——网络如何工作

了解你自己。——Oracle at Delphi

保护网络的安全可能是件棘手的事情。有诸多问题要考虑。必须知道已知的弱点、可能的威胁以及检测攻击的方法，并开发方案来处理可能的威胁。然而在能真正保护网络免遭攻击之前，必须首先了解网络，并且应该比攻击者更了解自己的网络。我们必须研究并了解自己的能力和限制、网络做些什么以及如何去做。只有这样才能真正地看到弱点并采取必要的措施来防护。假如不知道其工作方式，就不能保护网络的安全。

第一部分将展示一些概念来说明设备如何在局域连接上通信、IP寻址、路由、三向握手，并介绍了网络应用的基础。同时也将介绍贯穿全书所使用的工具，诸如ping、arp、nslookup，以及协议分析器之类的工具。

这一部分分为三章，涵盖了 TCP/IP 协议栈的不同方面的概念。第 1 章将包含涉及访问和网络层的习题，第 2 章将安排传输层，第 3 章是应用层。在实施该节中的实验时应该不断地问自己一个问题，该漏洞如何被攻击？怎样被利用？当正在学习某事物是怎样工作的时候就去考虑它怎样能被破坏，这或许看来好像很空洞，但这是个开始像攻击者那样进行思考的好机会。也是为第 2 部分中将要提到的实验做好准备。

第 1 章　工作站网络配置与连接

下面列出了这一章中的实验，以内容难易程度递增的顺序排列：

实验 1：网络工作站客户端配置

实验 1a：Windows 客户端配置（ipconfig/ping/arp）

实验 1b：Linux 客户端配置（ifconfig/ping/arp）

实验回顾

关键术语

关键术语提问

实验分析问题

实验 2：计算机名的解决

实验 2a：Windows（nslookup）

实验 2b：Linux（nslookup）

实验回顾

关键术语

关键术语提问

实验分析问题

实验 3：网络路由基础（路由）

实验 3c：网络路由基础

实验回顾

关键术语

关键术语提问

实验分析问题

实验 4：网络通信分析

实验 4a：Windows 网络通信分析（Ethereal）

实验 4b：Linux 网络配置分析（Ethereal）

实验回顾

关键术语

关键术语提问

实验问题分析

本章包含实验习题来阐明用于在基于传输控制协议/网际协议（TCP/IP）的网络中建立工作站连接的各种命令和方法。本章包含了在使用 Windows PC 机和基于 Linux 的 PC 机的网络环境中实现和监视连接的基本需求。本章将会引入一些基本的命令和工具，以便能够在工作站上操作和监视网络设置。这是迈向建立安全连接的必要的第一步。

实验 1：网络工作站客户端配置

为了让两台计算机在 **TCP/IP 网络**中通信，两台计算机都必须有唯一的**网际协议（IP）地址**。一个 IP 地址有四个八位组。IP 地址将被分为**网络地址**和**主机地址**。**子网掩码**标识网络 IP 地址的一部分，这部分是与主机地址相联系的。在局域网（LAN）上，每台计算机必须有相同的网络地址和不同的主机地址。利用不同的网络 IP 地址与 LAN 外部通信，使用默认网关是必需的。连接到 TCP/IP 网络，通常有四项要配置：IP 地址（包括网络部分和主机部分）、子网掩码、域名系统（DNS）服务器的 IP 地址，以及网关的 IP 地址。如果是单独在局域网上通信，则只需要 IP 地址和子网掩码。要想和其他网络通信，就需要默认网关。如果希望能够使用域名来连接到不同的站点和网络，那么还需要一个 DNS 地址。

当不同网络上的机器之间互相通信时，数据包通过默认网关发送，进出 LAN。路由选择要使用第三层或 IP 地址。如果计算机在同一个网络上，则 IP 地址转化到第二层，或者由**介质访问控制（MAC）地址**与计算机通信。MAC 地址由生产网卡的公司硬编码到网卡中。

计算机利用 MAC 和 IP 地址跨网络互相通信。在这个实验中，两台计算机将通过 ping 消息相互“交谈”。然后将会修改一台计算机的**地址解析协议（ARP）**表，来表明机器的 IP 和 MAC 地址之间的关系。

ping（网际数据包探测器）程序是用于测试两台计算机之间连接的基本实用程序。该名称来源于潜水艇上的声纳产生的声音，并以同样的方式使用。一个“信号”或请求被发送出去，沿着一个固定的“间隔”去探测目标是否存在。两台计算机之间的距离可以利用**生存时间（TTL）**测出。ping 操作利用**网际控制信息协议（ICMP）**测试连接；因此万一 ICMP 受到限制，ping 实用程序可能不可用。尽管有其他可供选择的方法存在，ping 通常还是利用 ICMP 回显消息实现的。

在该实验中使用 ping 命令时，大家将会看到尽管是使用 IP 地址作为 ping 的目标，但实际上是 MAC 地址被用来与那台计算机进行通信。IP 地址用于在网络之间传输数据。反之，MAC 地址用于在同一个网络上设备之间发送信息。这是由 ARP 将 IP 地址解析为相关联的 MAC 地址。ARP 是一个用于修改 **ARP 高速缓冲存储器的传输控制协议/网际协议（TCP/IP）**工具。ARP 缓存包含了最近解析的网络 IP 主机的 MAC 地址。

当沿着实验继续学习时，同学们将会看到计算机如何为了通信去获得 MAC 地址和 IP 地址。应该思考的问题是：“计算机怎样知道正在获得的信息是正确的？”

在该实验习题中将会使用 Windows 的 **ipconfig** 命令以及 Linux 中的 **ifconfig** 命令来查看配置信息。然后会利用 Windows 中的本地连接属性页（Local Area Connection Properties）以及 Linux 中的 ifconfig 来更改 IP 地址。

学习目标

完成该实验后，大家将能够：

- 通过命令行得到 IP 地址配置信息。

- 列举 ipconfig（Windows）/ifconfig（Linux）命令的功能性开关。
- 利用 Windows 图形用户界面（GUI）来配置网卡以使用给定的 IP 地址。
- 确定机器的 MAC 地址。
- 确定机器被分配的网络资源，包括 DNS 地址和网关地址。
- 利用 ifconfig（Linux）命令以给定的 IP 地址配置网卡。
- 理解怎样测试两台计算机之间的网络连接。
- 列举 ping 命令的功能性选项。
- 利用 arp 命令查看和管理计算机上的 ARP 缓存。