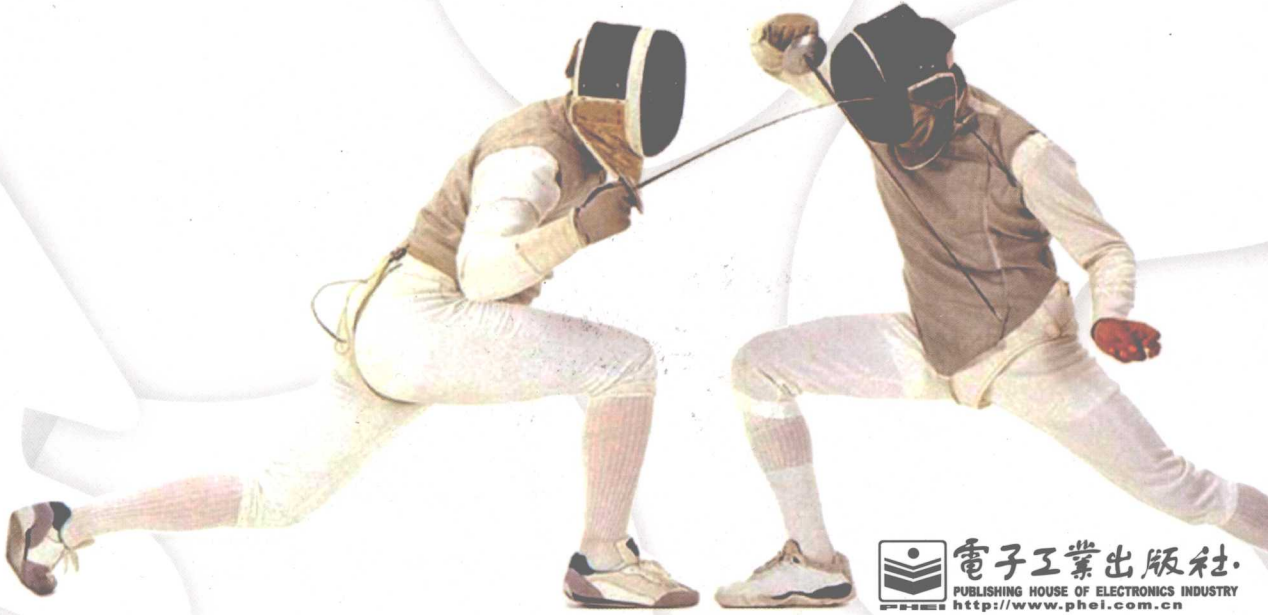
Broadview
www.broadview.com.cn

安全技术大系

黑客攻防
实战案例解析

陈小兵　张艺宝　编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

黑客攻防
实战案例解析

陈小兵　张艺宝　编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书从“攻”与“防”两个不同的角度，结合网络安全中的实际案例，图文并茂地再现网络入侵和防御的全过程。全书共分八章，给出了100多个实际案例，由浅入深地介绍了目前网络流行的攻防方法和手段，并结合作者多年的网络安全实践经验给出了相应的安全防范措施。本书的最大特点是实用性和实战性强，即通过实际案例来对每一个攻防手段进行介绍，使读者对网络攻防技术有较为深入的感性认识；而且本书还列出了许多图文解释步骤，按照书中的操作步骤可以还原当时的攻防情景，便于读者掌握网络攻防的流程、最新的方法和技术。

本书适合对网络安全和黑客攻防感兴趣的读者，也适合作为计算机应用专业本科生和研究生的网络安全课程实践参考资料。

图书在版编目（CIP）数据

黑客攻防实战案例解析 / 陈小兵，张艺宝编著. —北京：电子工业出版社，2008.10
（安全技术大系）
ISBN 978-7-121-07311-3

I. 黑… II. ①陈… ②张… III. 计算机网络－安全技术 IV. TP393.08

中国版本图书馆CIP数据核字（2008）第133946号

责任编辑：顾慧芳
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编100036
开　　本：787×980　1/16　印张：28.75　字数：690千字
印　　次：2008年10月第1次印刷
印　　数：5000册　定价：49.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

本书是我从事写作以来最难写的书，因为书中的案例都来自真实的网络环境。为了让每一个案例都要具有一定的代表性，尽量做到不重复，我和本书的另一位作者张艺宝对案例进行了精选、分析、比较和测试，最后终于完成了使命，将我们的许多研究成果放在本书中与大家分享。

网络安全是一个涵盖较多领域的一门学科，它包括密码学、社会工程学、计算机应用技术等诸多学科；网络安全还跟大家的工作和生活息息相关，例如网页木马、网站挂马、盗号、QQ 密码破解、网银大盗、公司机密资料的窃取等都是造成网络不安全的一些症状，网络安全的目的是预防和治疗这些症状，为广大群众提供更好的服务。相对而言，我国的网络安全工作起步较晚，目前网络安全的核心技术大多数被西方国家所掌握。我们是从 2000 年开始接触网络安全问题的，从很多网络不安全的案例中深切感到有一种使命感在催促我们在国内传播网络安全的知识。起初我们在学习过程中购买了大量有关网络安全的书籍，但这些书籍中的理论较多，实践较少，并且技术相对滞后，有些技术在目前已经不能使用。鉴于这种情况，我们决定将多年的实践经验和研究成果按照网络攻击的流程进行整理，用生动、典型的实际案例来分析网络的攻击与防御，让更多的朋友来了解、推动和探讨网络安全问题，提升我国网络安全的整体水平。

本书以网络的攻击与防御为主线，以实际案例的形式来对每一个攻防手段进行介绍，使读者能够对网络攻防技术有比较深入的感性认识。并且本书还列出了许多通俗易懂的图文解释步骤，按照书中的步骤即可还原当时的攻防情景。这样一来，通过阅读本书，初学者便可以很快地掌握网络攻防的流程、最新的技术和方法；有经验的读者则可以在技术上更上一层楼，对网络攻防技术的认识从理论到实践更加系统化，同时还可以使用本书介绍的一些防御方法加固自己的计算机系统。

本书的内容

本书共分为八章，由浅入深，依照网络攻击的流程来安排内容，每一小节一个案例，在每一个案例中列出了相关的知识要点。

第 1 章　网络安全基本知识

本章介绍网络的一些基本知识，有关网络安全的一些基本术语和常见的一些 DOS 命令等。

第 2 章　信息收集案例

信息收集是网络攻击的主要步骤之一，在本章中介绍了如何利用 Google、电驴、Foxy、网站、BBS、Blog 等来收集信息，以及使用扫描软件来收集被攻击目标的信息，通过对收集信息的分析和处理，可以直接控制被攻击的目标。

第 3 章　网络攻击案例

本章介绍网络攻击案例中一些典型的攻击方法和手段。

第 4 章　网络控守案例

本章介绍利用目前一些主流的控制技术来对目标计算机进行控制，以及如何在被控制计算机上获取更多有用的信息。

第 5 章　网络渗透

本章介绍如何利用已有的信息来进行内网渗透，入侵者如何实现远程控制。

第 6 章　隐藏技术与痕迹清除

本章通过一些实际案例来介绍网络入侵过程中的隐藏技术与痕迹清除技术。

第 7 章　常用工具

本章介绍目前黑客使用的一些常用工具。

第 8 章　安全检查工具

本章介绍如何使用一些工具软件来扫描网络计算机中存在的安全漏洞、如何修补系统中存在的安全漏洞、如何检查网络端口和进程等，通过这些工具来对系统进行安全加固。

网络安全问题涉及面积广，尽管我们在这方面做了很多的研究，但仍然无法涵盖所有的黑客攻防问题。因此，本书打算通过一个一个的实际案例来探讨网络安全的问题，与读者分享我们的实践经验和研究成果，以提高对网络安全问题的认识和远离黑客威胁的能力。

反馈与提问

读者在阅读本书过程中遇到任何问题或者意见，可直接发邮件至 simeon2008@gmail.com，也可去我个人的 Blog 地址（http://simeon.blog.51cto.com）留言。

致谢

感谢电子工业出版社对本书的大力支持，尤其是策划编辑毕宁和责任编辑顾慧芳为本书出版所做的大量工作。借此机会，我还要感谢多年来在信息安全领域给我教诲的所有良师益友，感谢网友非安全·后生、暮云飞、逍遥复仇、Lenk、大馄饨等对本书的支持。最后感谢我的家人，是他们的支持和鼓励使本书得以顺利完成。

陈小兵
2008 年 6 月于北京

特别声明：

本书的目的决不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任；本书的目的在于最大限度地提醒大家对网络安全的重视，并采取相应的安全措施，以减少由于网络安全问题而带来的经济损失。

目　录

CHAPTER 1

第 1 章　网络安全基本知识

网络安全的范围很广，涵盖的内容很多，涉及的技术也很多。对一个新手来说：如何了解网络安全，如何防范入侵，如何加固自己的操作系统，就显得尤为重要；这一切都离不开最基本的一些网络安全知识和一些术语，了解这些基本知识和术语有助于了解本书后面章节中的案例。

本章介绍的网络安全知识和术语是一些常见的 DOS 入侵用的命令以及一些常用的工具。这些基本知识是网络攻防的基础，而这些知识的综合运用在进行网络的大型攻防实战中是必不可少的。通常，网络攻防中有这样一个理念："网络安全高手要进行一次次的试验和尝试，就跟武林高手一样，一个简单的动作都要做无数遍，这样才能深得其方法、技巧和精髓！"

本章主要内容：

- 常见的网络安全术语
- 常用 DOS 基本命令
- 端口和服务
- 常用工具

1.1　常见的网络安全术语

在网络安全的攻防过程中，将一些操作或者某一类跟网络安全相关的知识称为安全术语，这些术语有的是国际通用的，有的是"圈内"说法，也有通俗叫法。在本节中收集整理了一些网络安全以及与网络安全相关的术语，这些术语有些是书面的，有些是网络上流行的，因此在名称和叫法上可能会不一样，但其本质都是一样的，读者只须了解这些术语的意义即可。

1.1.1　常见的网络基本术语

1. 协议

网络是一个信息交换的场所，所有接入网络的计算机都可以通过彼此之间的物理连接设备来进行信息交换，这种物理设备包括最常见的电缆、光缆、无线 WAP 和微波等。但是单纯拥有这些物理设备并不能实现信息的交换，这就好像人类的身体不能缺少大脑的支配一样，信息交换还要具备

软件环境，这种“软件环境”是人类事先规定好的和必须遵守的规则，被称之为“协议”，有了协议，不同的计算机可以遵照相同的协议使用物理设备，不会造成相互之间的“不理解”，常见的协议有 TCP/IP 协议、UDP 协议、HTTP 协议以及 POP3 协议等。

这种协议类似于“摩尔斯电码”，简单的一点一横，经过排列可以有千变万化，但是假如没有“对照表”，谁也无法理解一份杂乱无章的电码所表述的内容是什么；计算机也是一样，它们通过各种预先规定的协议完成不同的使命，例如 RFC1459 协议可以实现 IRC 服务器与客户端计算机的通信。因此无论是黑客还是网络管理员，都必须通过学习协议才能了解网络运作的机理。

每一个协议都是经过多年修改延续使用至今的，新产生的协议大多也是在基层协议基础上建立的，因而协议相对来说具有较高的安全机制，黑客很难发现协议中存在的安全问题而直接进行网络攻击。但是对于某些新型协议，因为出现时间短、考虑欠周到，也可能会因安全问题而被黑客利用。

2．网络服务器与网络客户端

最简单的网络服务形式是：若干台计算机作为客户端，使用一台计算机作为服务器，每一个客户端都具有向服务器提出请求的能力，然后由服务器应答并完成请求的动作，最后服务器会将执行结果返回给客户端计算机。很多服务器都是按照这种方式来运行的，例如电子邮件服务器、网站服务器、聊天室服务器等。另外还有一种连接方式，它不需要服务器的支持，而是直接将两个客户端计算机进行连接，也就是说每一台计算机都既是服务器、又是客户端，它们之间具有相同的功能，对等地完成连接和信息交换工作，例如 DCC 传输协议即属于此种类型。

客户端和服务器分别是各种协议中规定的请求计算机和应答计算机。作为一般的上网用户，都是操作自己的计算机（客户端），向网络服务器发出常规请求完成诸如浏览网页、收发电子邮件等的动作，而对于黑客来说则是通过自己的计算机（客户端）对其他计算机（有可能是客户端，也有可能是服务器）进行攻击，以达到入侵、破坏、窃取信息的目的。

3．操作系统与系统环境

计算机要正常运行必须安装操作系统，目前操作系统的类型主要有 UNIX、Linux、Mac、BSD、Windows 系列等。这些操作系统各自独立运行，它们有自己的文件管理、内存管理、进程管理等机制；在网络上，这些不同的操作系统既可以在服务器、也可以在客户端被使用者操作，它们之间通过“协议”来完成信息的交换工作。

不同的操作系统配合不同的应用程序就构成了系统环境，例如 Linux 系统配合 Apache 软件可以将计算机构设成一台网站服务器，其他使用客户端的计算机可以使用浏览器来获得网站服务器上供浏览者阅读的文本信息；再如 Windows 2000 Server 配合 Serv-U 等 Ftp 软件可以构建一台文件服务器，通过远程 Ftp 客户端程序登录可以获得系统上的各种文件资源，普通用户使用 Windows 2000 Professional、Windows XP 或者 Windows Vista 等系统，通过安装一些常用的应用软件就构成了普通的计算机环境，入侵者如果攻击或者控制的是这类计算机，则习惯于称之为“肉鸡”。

4．IP 地址和端口

上网时可能会同时浏览网页、收发电子邮件、进行语音聊天等，不同的网络服务项目都是通过不同协议完成的。计算机主要通过 IP 地址来寻找提供所需服务项目的服务器或者客户端。

每一台上网的计算机都具有独一无二的 IP 地址，这个地址类似于生活中人们的家庭地址，每一家都有不同门牌号码。通过网络路由器等多种物理设备，网络可以完成从一个计算机到另一个计

算机之间的信息交换工作，因为他们的 IP 地址不同，所以不会出现找不到目标的混乱局面。

不同的协议体现在不同的网络服务上，而不同的网络服务则会在客户端计算机上开辟不同的端口来完成它的信息传送工作。当然，如果一台网络服务器同时开放了多种网络服务，那么它也要开放多个不同的端口来接纳不同的客户端请求。

网络上经常听到的“后门”就是这个意思，黑客通过软件或者脚本在服务器上开辟了一个网络服务，这个服务主要是完成黑客的指定命令或者其他特别目的，那么该服务器上就会被打开一个新的端口用来完成这种服务，因为这个端口是供黑客使用的，因而轻易不会被一般上网用户和网络管理员发现，即“隐藏的端口”，也称之为“后门”。

从理论上来说，每一台计算机都可以打开 65535 个端口，因而我们可以开发出至少 65535 种不同的网络服务。虽然这个数字非常大，但是网络上经常用到的服务协议不过几十种，例如浏览网页客户端和服务端使用的都是 80 号端口；传输文件的是 20 和 21 端口；telent 使用的是 23 端口；发送邮件使用的是 110 端口；进行 IRC 聊天则在服务端使用 6667 端口、客户端使用 1026 端口等。

1.1.2　网络安全基本术语

1．特洛伊木马（木马）

特洛伊木马，一般简称为木马，是一个程序，该程序可以做程序设计者有意设计的未出现过的事情，它一般是“偷偷地”执行的。但是对于特洛伊木马所做的操作，不论用户是否了解，都是不被赞同的。目前关于病毒和木马的界限还并不是很清楚，很多杀毒软件都将木马程序列为病毒，甚至一些功能强大的网管软件都将其作为有“威胁”的病毒进行处理。因此，目前很多远程控制软件也习惯上被称之为木马；还有一些具有执行命令、操作文件等功能的网页程序也被称之为木马（网页木马），例如海洋顶端等。

2．黑客与骇客

只要涉及网络安全问题，就离不开黑客（Hacker）这个话题。1998 年出版的《新黑客字典》中对黑客的定义是“喜欢探索软件程序奥秘、并从中增长其个人才干的人”。黑客一词，源于英文“Hacker”，愿意是指热心于计算机技术，水平高超的电脑专家，尤其是程序设计人员，他们出现的真正原因是网络先天存在的安全漏洞。但今天黑客一词已被用于泛指那些专门利用电脑搞破坏或者恶作剧的人，尤其是目前利用黑客技术来牟利的人，其英文称之为 Cracker，翻译成中文称之为“骇客”。黑客与骇客的区别是：黑客建设，骇客破坏！目前对黑客比较确切的定义是：在数据安全领域，一种未经授权又企图躲过系统访问控制程序的检查而侵入计算机网络或者个人计算机的用户。

当然无论是黑客还是骇客，其入侵行为都是违法的。但目前黑客已经成为一个特殊的社会群体，在欧美以及亚洲等国都有一些合法的黑客组织，一些安全公司中的“安全”高手，其前身就可能是其组织中的著名“黑客”。在我国，黑客的活动也逐渐呈组织化、集团化和利益化的特点。

3．漏洞

漏洞是在硬件、软件以及协议等的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未经授权的情况下访问或者破坏系统。例如最简单的“弱密码”漏洞是指系统管理员忘记屏蔽某些网络应用程序中的账号；Perl 程序漏洞则可能是由于程序员在设计程序的时候考虑情况不完善而出现的“让程序执行起来不知所措”的代码段；“溢出”漏洞则属于当初设计系统或者程序

的时候，没有预先保留出足够的资源（内存空间等），而在日后使用程序时造成的资源不足；特殊 IP 包炸弹是程序在分析某些特殊数据的时候出现错误等；黑客等入侵者一般都是利用漏洞来进行网络攻击。网络上未公开的漏洞，常被称为“oday”。

4．安全漏洞与系统攻击

安全漏洞是在系统具体实现和具体使用中产生的错误，但并不是系统中存在的所有错误都是安全漏洞，只有能够威胁到系统安全的错误才是漏洞。普通用户在使用应用软件等过程中，有时候出现的错误就是漏洞，而将这些漏洞挖掘出来并加以利用（如能让用户执行特定的程序），则该漏洞就是系统安全漏洞或者应用程序安全漏洞。

系统攻击者往往是安全漏洞的发现者和使用者，要攻击一个系统，如果不能发现和使用系统中存在的安全漏洞是很少能够成功的，这对于安全级别越高的计算机网络系统来说尤其如此。目前有很多安全扫描软件，其主要功能之一就是查找并发现系统中存在的安全漏洞。因此，系统攻击往往就是发现和利用安全漏洞的过程。

5．网页后门与网页木马

网页后门是随着脚本漏洞的出现而出现的，它是在系统漏洞越来越难利用的情况下网络安全发展的一个新阶段。网页后门就是先利用某种脚本程序漏洞上传脚本后门，然后在该服务器上上传、安装和执行程序，找到提升权限的突破口，进而拿到服务器的系统权限，对服务器实施全面控制。目前的网页后门主要有 ASP、ASP.net、PHP、JSP、CGI 等类型，网页后门也称为 Webshell，目前比较有名的 Webshell 有海洋顶端、evil 的一句话后门、桂林老兵等。

网页木马是指借助网页脚本、IE 浏览器等应用程序漏洞或者操作系统漏洞等，在浏览者访问网页或者打开攻击者所构造的特殊格式文件时，会自动“偷偷”地下载并执行攻击者指定地址的木马程序。这些木马程序可能是游戏盗号程序，也可能是远程控制软件，例如灰鸽子等。

6．挂马

挂马是指将网页木马地址插入到被控制的网站文件中、用户在访问这些网站文件时，如果系统以及应用程序未安装相应的补丁程序，则会下载并执行网页木马中的木马程序。攻击者通过木马客户端（控制端）可获取已执行木马程序计算机中的游戏账号等信息，并通过这些信息来牟取利益。

7．跨站攻击（旁注）

跨站攻击（旁注）是指在 SQL 注入过程中无法对正在入侵的某个网站有所突破时，转而向被入侵网站所在的服务器的其他网站进行攻击。在获得 Webshell 的情况下，采取 Cookies 以及 Session 欺骗等方式来获取入侵目标网站的 Webshell。也就是说，正路不行走旁路。目前由于经济成本等原因，多个用户共用一台服务器，每一个网站只是使用服务器上一个单独的文件夹，因此控制某一个网站以后，可以提升服务器权限达到完全控制或者通过 Webshell 来读取其他网站的文件，从而获得 Webshell。

8．Shell

在网络安全中 Shell 其实也是一个后门，只是触发方式不一样而已。一般状态下的 Shell 是指通过控制端打开远端（被控制计算机）的一个端口，并出现一个类似 DOS 提示符的窗口，可以在该窗口中执行各种 DOS 命令。

9．Rootkit

Rootkit 出现于 20 世纪 90 年代，在 1994 年 2 月的一篇安全咨询报告中首次使用了 Rootkit 这个名词。从出现至今，Rootkit 的技术发展非常迅速，应用也越来越广泛，检测难度也越来越大，其中针对 SunOS、Linux 和 Windows 系统的 Rootkit 较多。Rootkit 是用来隐蔽入侵者的踪迹和保留 Root 访问权限的工具，Rootkit 最早出现在 Linux 和 UNIX 系统中。通常，攻击者通过远程攻击获得 Root（Administrator）访问权限，进去系统后，攻击者会在控制的计算机中安装 Rootkit，然后通过 Rootkit 的后门来检查系统、嗅探用户的密码等。

Windows 下的 Rootkit 大多是内核级后门程序，目前也有驱动级的 Rootkit。安装这些 Rootkit 后，入侵者可以隐藏文件、进程、系统驱动、注册表和键值、打开的端口和网络连接、虚设可用磁盘空间等。系统中如果安装了 Rootkit，被安装者通过普通的查杀途径很难检测这些 Rootkit 程序，故 Rootkit 的危害性非常大。在本书的后门章节中，单独介绍了如何利用目前网络上的一些 Rootkit 检测工具来检查系统中是否被安装了 Rootkit 程序。

10．网络监听

网络监听是入侵者常用的一种方法。在入侵成功并控制一台计算机后，往往要继续扩大战果，尝试登录或者夺取网络中其他主机的控制权，这时就需要获取用户使用这些网络或者资源的用户名称和密码。获取这些途径的方式主要有键盘记录和网络监听两种。在网络上，监听效果最好的地方是网关、路由器、防火墙一类的设备，通常由网络管理员来进行操作，入侵者在网络管理员的计算机或者附近服务器计算机中安装嗅探软件来进行嗅探。

11．键盘记录

键盘记录通常是指将键盘记录软件安装在已控制计算机中，通过键盘记录文件来分析被安装键盘记录的计算机用户的一些操作行为和有关密码等敏感信息。通过分析键盘记录可以获取有关用户邮件、QQ 号码、MSN、FTP 等账号和密码，通过获取的信息进行信息收集和再次渗透攻击等。

12．加密与解密

加密与解密是网络安全中一个最重要的课题，网络上最常使用的是设置个人密码、使用 DES 加密锁等。这些加密方式分别可以完成用户登录系统、网站、电子邮件信箱和保护信息包的工作，而黑客所要进行的工作，就是通过漏洞、暴力猜测、加密算法反向应用等方式获得加密档案的明文。加密和解密都跟密码相关，加密中最关键的一点就是采用哪一种算法进行加密，例如在网页脚本中最常见的就是 Md5、DES 加密。

13．浏览器劫持

从软件方面来说，浏览器劫持是一种恶意程序，通过 DLL 插件、BHO、Winsock LSP 等形式对用户的浏览器进行篡改，使用户浏览器出现访问正常网站时被转向到恶意网页、IE 浏览器主页/搜索页等被修改为劫持软件指定的网站地址等异常情况。

从技术方面来说，浏览器劫持是一种常见的在线攻击类型，黑客可通过这种方式控制计算机的浏览器，并更改网上冲浪的方式和冲浪时所显示的内容。

浏览器劫持有多种不同的方式，从最简单的修改 IE 默认搜索页到最复杂的通过病毒修改系统设置并设置病毒守护进程、劫持浏览器，等等。

14. 网络钓鱼

网络钓鱼（Phishing）一词，是“Fishing”和“Phone”的综合体，是常见的网络欺诈行为。自1996 年以来，黑客便开始利用电子邮件作为诱饵，盗用美国在线的账号和密码。后来鉴于最早的黑客是用电话线作案的，所以黑客们常常用 Ph 来取代 f，就形成了今天的 Phishing 一词。

“网络钓鱼”攻击是利用欺骗性的电子邮件和伪造的 Web 站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、账户用户名、密码和社保编号等内容。而诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信的品牌，所以在所有接触诈骗信息的用户中，有高达 5%的人都会对这些骗局做出响应。

15. 攻击分析和响应

攻击分析和响应是实时监控行为，即识别攻击特征和其他包括病毒、探测行为和未授权修改系统存取控制机制的可疑行为。实时监控提供了迅速检测未授权黑客行为并以反击手段响应的能力，响应的方式有简单的通知安全管理员和向技术专家提供检测报告等。

16. 审核

审核是由安全或系统支持部门所采取的行为，用来评估已定义的策略和实际履行之间的不同。这些部门会找出在策略和计划方面需要的更正行为，以及评价该企业支持策略的能力。

17. 误操作分析及响应

误操作分析是对内部网络资源的误操作实行实时监控。误操作通常不会影响操作性能，但却违反企业的有关规定、使用了企业的某些资源（如，用企业网看色情小说）。自动响应包括拒绝服务、警告信息、给相应管理员发送电子邮件，等等。

18. 策略

策略是指对网络和安全系统的设置、实施、操作的正式和强迫的组织要求。这些要求建立在正式的操作危险评估基础上，考虑了网络要求（功能、表现和成本）、威胁和弱点情况等。

19. 攻击评估

攻击评估是指由一组高水平的操作和攻击分析员所采取的，针对与特定企业和地理区域有关的人为和环境攻击活动的评估行为。他们的基本意图是建立特殊攻击种类的相似性或可能性，这些数据支持最终的危险评估（攻击、漏洞、企业资产分析）。

1.1.3 常见的黑客软件类型

在网络攻击中有很多工具软件，这些软件一般被称为黑客软件，黑客软件按照用途可以分为以下几类：

1. 防范类黑客软件

这是从安全防范的角度出发涉及的一类软件，例如防火墙、查杀病毒软件、系统进程监视器、端口管理程序、日志分析软件、系统入侵软件等都属于此类软件。这类软件可以帮助管理员（用户）维护和管理服务器（个人计算机）的安全，并对入侵者进行追踪。

2. 信息搜集类黑客软件

信息搜集软件种类比较多，包括端口扫描、漏洞扫描、弱密码扫描等扫描类软件，以及监听、截获信息包等间谍类软件。它们大多数属于亦正亦邪的软件，也就是说无论正派黑客、邪派黑客、

系统管理员还是一般的计算机使用者，都可以使用这类软件达到各自不同的目的。该类软件是攻击过程中不可缺少的软件，也是入侵者或者管理员用得较多的一类软件。

3．木马与蠕虫类黑客软件

木马与蠕虫类黑客软件是两种不同类型的软件，但它们的工作原理大致相同，都具有病毒的隐藏性和破坏性。另外，此类软件还可以由拥有控制权的人进行操作，或由事先精心设计的程序完成一定的工作。当然这类软件也可以被系统管理员利用，作为远程管理服务器的工具。

4．洪水类黑客软件

所谓“洪水”类黑客软件即信息垃圾炸弹，通过大量的垃圾请求可以导致目标服务器负载超负荷而崩溃。洪水软件还可以用做邮件炸弹或者聊天式炸弹，这些都是经过简化并由网络安全爱好者程序化的“傻瓜式”软件，对网络具有较大的破坏力。

5．密码破解类黑客软件

网络安全最核心的内容就是依靠各种加密算法的密码系统，入侵者也许可以很容易地获得一份暗文密码文件，但是如果没有解密算法，它仍然无法获得真正的密码。在很多情况下，应用软件会采取一些安全措施来保证文件的安全，例如 PDF 文件加密、Word 文件加密、Rar 文件加密等，为了获取这些文件的原始内容，需要进行解密。破解这些文件以及破解系统密码的软件就是密码破解类黑客软件。

6．欺骗和伪装类黑客软件

当通过正面的攻击无法达到目的时就需要通过发送文件等方式来进行欺骗，让被攻击目标主动执行木马或者指定程序，例如 Arp 软件、邮件木马等，这类软件被称为欺骗类软件。在网络攻击过程中，入侵者在网络上进行的各种操作都会被 ISP、服务器记录下来，因此需要通过软件或者代理等技术来掩藏入侵者的 IP 地址等信息、达到伪装的目的，这类软件称为伪装类黑客软件。

1.1.4　黑客分类和黑客行为

“黑客”大体上分为“正派”和“邪派”两类：“正派”黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善，在网络上也被称为“红客”；而“邪派”黑客则是通过各种黑客技术对系统进行攻击、入侵或者做其他一些有害于网络的事情，并常常以牟取商业利益为主要目的。由于“邪派”黑客所从事的事情违背了《黑客守则》，所以也被称为“骇客”（Cracker）。

网络安全只是黑客界的一种好听称呼，网络安全爱好者和黑客从本质上来说都差不多。实际上，最好的攻击就是最好的防御，如果自己部署的系统没有人能够攻陷，这种系统能不安全吗？所以无论黑客还是网络安全爱好者，其网络安全的技术都是一样的，用之正道，则正之；用之邪道，则邪之。通常，黑客要具备以下几种能力。

1．学习能力

网络安全以及计算机技术的发展日新月异，对于黑客来说，需要不断地学习，了解和掌握最前沿的技术；特别是进入 21 世纪以来，随着互联网技术的不断发展，可以从网上很方便地学习和获取世界各地的知识和技术，因此高手的知识都是靠平时一点一点积累起来的，还要通过无数次的试验和尝试才能练就系统的“铜墙铁壁”和掌握战无不胜的攻击工具——“矛”。