ATTACK

在攻与防的对立统一中
寻求技术突破

黑客攻防
从入门到精通

全新升级版

明月工作室◎编著

附赠
大型视频教程光盘

以下人群请勿翻阅本书：

1.自以为很牛，对黑客不屑一顾的人
2.心存侥幸，认为黑客离自己很远的人
3.习惯黑客攻击，总是折腾他人的人
4.号太多，习惯被盗号的人
5.不差钱，不怕被盗刷的人
6.我不是Boss，对交易安全漠不关心的人

DEFENSE

北京大学出版社
PEKING UNIVERSITY PRESS

黑客攻防
从入门到精通
全新升级版

明月工作室◎编著

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 提 要

本书由浅入深、图文并茂地再现了计算机与手机安全相关的多方面知识。

全书共22章，分别为社会工程学、计算机与网络反黑基础、Windows 10系统防火墙与Windows Defender、Windows 10高级安全管理、系统和数据的备份与恢复、计算机与网络控制命令、扫描与嗅探：确定目标与探索网络资源、木马防范技术、病毒防范技术、Windows系统漏洞攻防技术、计算机后门技术、程序的加密与解密技术、局域网安全防范技术、计算机远程控制技术、Web站点安全防范技术、清理恶意插件和软件、网游与网吧安全防范技术、网络账号防黑实战、网络支付工具的安全、无线网络安全防范技术基础、Wi-Fi安全防范技术、蓝牙安全防范技术。

本书语言简洁、流畅，内容丰富全面，适用于计算机初、中级用户、计算机维护人员、IT从业人员及对黑客攻防与网络安全维护感兴趣的计算机中级用户，各大计算机培训班也可以将其作为辅导用书。

图书在版编目(CIP)数据

黑客攻防从入门到精通：全新升级版 / 明月工作室编著. — 北京：北京大学出版社，2017.4
ISBN 978-7-301-28031-7

Ⅰ. ①黑… Ⅱ. ①明… Ⅲ. ①黑客—网络防御 Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字(2017)第024334号

书　　名：黑客攻防从入门到精通（全新升级版）
HEIKE GONGFANG CONG RUMEN DAO JINGTONG

著作责任者：明月工作室　编著
责 任 编 辑：尹　毅
标 准 书 号：ISBN 978-7-301-28031-7
出 版 发 行：北京大学出版社
地　　址：北京市海淀区成府路205号　100871
网　　址：http://www.pup.cn　　新浪微博：@北京大学出版社
电 子 信 箱：pup7@pup.cn
电　　话：邮购部62752015　发行部62750672　编辑部62580653
印　刷　者：北京大学印刷厂
经　销　者：新华书店
787毫米×1092毫米　16开本　32.75印张　712千字
2017年4月第1版　2017年4月第1次印刷
印　　数：1-4000册
定　　价：69.00元

专家面对面

数码设备和网络是我们每天都离不开的，在互联网的大潮之中，无论是专业人士还是普通大众都需要有网络安全意识。在这里，我们特别邀请了来自《黑客防线》的作者以及百度、腾讯、360、趋势科技等公司的资深人士，为读者解答一系列大家最关心的问题。

问 作为一名普通的计算机用户，我可以抵御来自网络的攻击吗？如果可以，那么应该怎样做？

答 普通的计算机用户，一般可能遭受的网络攻击有钓鱼网站欺骗、网站挂马、邮件发马等形式，此外还可能会遭受弱口令扫描、密码嗅探等方式的攻击。因此要抵御来自网络的攻击时，可从以下 3 个方面来防范。

（1）针对钓鱼网站欺骗、网站挂马等方式的攻击，尽量做到只登录信任的网站，不要随便打开来路不明的网站地址；开启杀毒软件、防火墙，通过监控软件帮助防范这类网络攻击。

（2）针对邮件发马的攻击方式，一是要注意保护个人邮件地址的信息不要泄漏，二是不要打开陌生邮件中的链接、文件、应用程序等。

（3）自身相关账号密码要做好保护工作，防止泄露，各类账号不要使用同一密码或简单的弱口令密码，以防弱口令暴力扫描破解。

——360 公司冰河洗剑

问 计算机有哪些后门，如何发现和防范不法分子留下的后门？

答 系统后门是控制系统后，为了方便下一次进入采用的一种技术，一般是通过修改系统文件或者安装第三方工具来实现，有很大的隐蔽性和危害性。较常见的后门有以下2种。

（1）Rhosts+ + 后门：在联网的UNIX机器中,像Rsh和Rlogin这样的服务是基于rhosts文件里的主机名使用简单的认证方法。用户可以轻易地改变设置而不需口令就能进入。入侵者只要向可以访问的某用户的rhosts文件中输入“+ +”，就可以允许任何人、从任何地方无须口令便能进入这个账号。

（2）Login后门：在UNIX里,login程序通常用来对telnet来的用户进行口令验证。入侵者获取login.c的原代码并修改,使它在比较输入口令与存储口令时先检查后门口令。如果用户输入后门口令,它将忽视管理员设置的口令让你长驱直入。

防范和发现后门可以从以下3点入手。

（1）以自己的经验，结合特定的工具，手动做一些检测。

（2）使用Tripwire或md5校验来检查系统。

（3）借助IDS系统，检测目标的可疑网络连接。

——蒋勇

问 怎样防范电脑被远程控制？

答 如需防范电脑被远程控制，那么有以下几种方法。

（1）关闭远程桌面服务，即不允许连接到这台计算机。

（2）只允许指定用户连接到此台计算机。

（3）在远程连接时更改 3389 端口，防止随意接入。

（4）将远程连接账户权限降低，保障电脑权限安全。

（5）注意网络使用安全，不浏览不安全的网站，不下载来路不明的文档文件，不安装不正规的安装程序，防止计算机中病毒和木马。

——风清扬

问 我是一名企业网管，我们公司的网站经常被攻击而无法登录，有什么解决办法吗？

答 首先找到网站每次遭受攻击的原因，对漏洞进行封堵。常见的攻击方式是 DDOS 攻击，这种攻击方式使网站瘫痪而导致无法登录，这时可通过运营商让合法服务请求及流量通过的方式来解决。另外，网站本身应做好安全防御，下面分享 4 个基本的安全防御方法。

（1）开启 IP 禁 PING，可以防止被扫描。

（2）关闭不需要的端口。

（3）开启防火墙。

（4）通过 360 等网络安全服务公司推出的网站卫士进行正常的日常维护等。

——趋势科技 xysky

问 我是一名网店店主，我要怎样做好工作用电脑的安全防护？

答 网店店主最重要的是要做好网店登录的账号、密码保护及支付环境的信息保护。具体的防护操作如下。

（1）要保证上网环境的安全，在虚拟机内进行操作，本机开设影子系统，进行重启还原到初始状态。

（2）不打开来路不明的陌生应用程序或文件。

（3）日常操作开启杀毒软件、打开防火墙并时时更新。

（4）要保证账号、密码的安全，不要以任何方式泄露账号、密码，利用强口令密码、经常更换密码等方式来保障电脑安全。

——叶猛

问 我是一名网游玩家，从来没有登录过乱七八糟的网站，为什么账号还会被盗？

答 导致游戏账号被盗的原因主要有以下两种情况。

（1）由于自身原因，多类账号使用同一密码，其他账号泄露，导致游戏账号密码泄露被盗。

（2）账号被盗除自身原因以外，还可能来自网络游戏本身的数据库遭受攻击导致的泄密，以及一些不法分子利用漏洞扫描工具进行扫描，通过游戏漏洞获得账号、密码等。这一因素玩家自身较难控制，可通过经常更改密码、增设密码难度等降低被盗号的风险。

——腾讯公司花非花

问 我是一名网游玩家，偶尔会使用网络代理工具登录国外游戏服务器，这会有什么安全隐患吗？

答 代理服务器的工作模式正是典型的“中间人攻击”模型，代理服务器在其中充当了一个“中间人”的角色，通信双方计算机的数据都要通过它。代理工具中存在的恶意代码可能在执行代理程序时就悄悄收集了你的计算机信息进行服务器回传，这种方法最让人不设防，因为它利用的是人们对代理的无条件信任和贪便宜的想法，因此是存在一定的未知安全隐患。

——百度公司孤烟逐云

问 我是一名公司职员，网管能够监控我的 QQ 聊天记录吗？如果能，应怎样防范？

答 公司职员的 QQ 聊天记录是能被网管监控的。无论使用的是截屏监控，还是插件记录，或其他监控方式，都是网管合法的监控手段，一般很难避免。一般来说，可以通过拨加密 VPN 的方式使通信信息加密，即使通信信息被截到，也无法查看具体内容。但是，如果是截屏监控，那么就无法避免被监控了。

——楚茗

问 注册和登录一些网站，用假身份证号会通不过验证，用真实资料却面临着信息泄露，那么该怎么办？

答 首先，在注册网站时使用强密码，防止密码被破解，并且使用和其他账号不同的密码，防止其他账号、密码泄露后，影响该账号的正常使用，从而有效防范不法分子通过账号的方式获取个人信息。其次，尽量少留个人真实信息，但如必须使用真实信息，尽量做到使用完进行信息删除。另外，在公开渠道也应避免留下真实信息。

——百度公司 TTFCT

问 遇到真实网站一模一样的钓鱼网站时，如何识别？

答 识别钓鱼网站有以下几个途径。

（1）看域名。钓鱼网站的域名虽然有很大的欺骗性，但是和真实的网站域名还是有差别的，如果网页内容相同，但是域名不同，就可以断定访问了钓鱼网站。

（2）看协议。现在很多网站都采用 https 协议来增加安全性，但是一些钓鱼网站却采用的是 http 协议。如果发现协议发生了变化，也可以断定访问了钓鱼网站。

（3）使用 scamscanner 网站分析查询。

（4）若是简单的钓鱼网站欺骗，可通过输入错误的账号、密码来验证，若成功跳转就是钓鱼网站。

——刘寅

问 除了系统自带、360 卫士等常用安防软件以外，我需要下载一些木马及病毒专杀工具吗？

答 如果确定系统已经中毒，用现有的安防软件不能够彻底清除病毒，那么很可能是安防软件的病毒库缺少类似病毒的样本，可以到网上查找是否有关于该病毒的权威通告以及相应的清除办法和防御措施，然后按照给出的方法清理病毒。必要时可以使用该病毒专杀工具。如果不确定系统是否中毒，那么就没有必要使用病毒专杀工具。

——依然魔力邓欢

黑客攻防精彩视频展示

一、社会工程学

1. 防范用户浏览过的文件泄密
2. 缩略图泄密与防范
3. 查看软件的备份文件
4. 防范 Windows 生成的缩略图泄密
5. 防范网站 Cookies 泄密
6. Cookies 欺骗的防范措施与技术之一：删除 Cookies 记录
7. Cookies 欺骗的防范措施与技术之二：更改 Cookies 文件的保存位置
8. 利用 IECookiesView 获得目标计算机中的 Cookies 信息
9. 简单的人肉搜索玩法

二、黑客攻防入门

1. 查看计算机端口
2. 开启和关闭服务
3. 限制端口
4. 利用服务工具关闭端口
5. 安装 VMware 虚拟机
6. 配置 VMware 虚拟机
7. 在 Windows 系统中启动 Dos 命令的多种方式
8. 测试物理网络的 ping 命令

三、信息的扫描与嗅探

1. 用 SSS 扫描器扫描系统漏洞
2. 使用影音神探工具搜索图片或视频地址
3. 使用经典嗅探器 Iris 捕获数据
4. 使用“艾菲网页侦探”捕获网页内容
5. 流光软件的配置与使用

四、木马与病毒的防范

1. 在“Windows 进程管理器”中管理进程，清除木马
2. Windows Defender 的使用方法
3. 用木马清除专家清除木马
4. 使用“木马清道夫”清除木马
5. 使用 NOD32 查杀病毒
6. 使用瑞星杀毒软件查杀病毒
7. 使用 360 查杀病毒
7. 使用 IEscan 屏蔽恶意网站
9. 用 SpySweeper 清除间谍软件
10. 清除电脑中的恶意代码和恶意软件

五、系统漏洞防范

1. 使用 MBSA 检测单台计算机漏洞
2. 使用 MBSA 检测多台计算机漏洞
3. 关闭 Netbios 漏洞
4. 使用 Windows Update 修复系统漏洞
5. 如何使用 360 安全卫士修复漏洞
6. 内存补丁程序的制作
7. 文件补丁程序的制作

六、远程控制技术

1. Windows 系统的远程桌面连接
2. 利用任我行软件进行远程控制
3. 使用 QuickIP 进行多点控制

七、入侵检测与入侵痕迹清理技术

1. 学会使用萨客嘶入侵检测系统
2. 日志分析工具 WebTrends 的使用方法 1
3. 日志分析工具 WebTrends 的使用方法 2
4. 用 SocksCap32 设置动态代理
5. “代理猎手”代理工具的设置与使用

八、局域网的监控与安全

1. 路由器无线功能的安全设置
2. 解除 WiFi 安全权限
3. 使用 LanSee 查看局域网信息
4. 使用网络特工进行数据监控

九、浏览器安全与性能优化

1. 设置浏览器的安全级别
2. 修改默认主页
3. 清理浏览器插件
4. 强行修改 IE 标题栏
5. IE 的 ActiveX 控件设置

十、Web 安全技术实战

1. 在本地主机配置网站环境与数据库
2. 熟悉高效代码审查工具 bitbucket
3. Code Blocks 的安装
4. 网站重置密码
5. 啊 D 注入工具原理揭秘

十一、加密与解密

1. 对 Excel 表格进行加密
2. 对 Word 文档进行加密
3. 使用 WinZip 加密文件
4. 使用 WinRAR 加密文件
5. 为 EXE 文件添加运行密码
6. 文件夹加密精灵的使用方法
7. 光盘加密软件 (GiliSoft Secure Disc Creator) 的使用
8. 对文件夹进行加密设定
9. 分割文件进行加密
10. Hiew 的简要使用技巧
11. RAR 压缩包密码破解工具 (RAR Password Recovery) 的使用方法
12. Zip 解密软件 (ARCHPR) 的使用方法
13. Windows 开机加密狗的制作方法

十二、系统安全设置

1. 计算机安全的系统设定
2. 本地安全策略的设定
3. IP 安全策略的自动优化
4. 设置系统组策略
5. 注册表的安全设定
6. 开启和关闭防火墙
7. Windows 防火墙入站规则的设置
8. 限制他人访问不良站点
9. 系统优化工具 CCleaner 的使用方法

十三、数据备份与还原

1. 系统还原点的创建与使用
2. 使用驱动精灵备份与还原驱动程序
3. Windows PE 启动盘的制作
4. 使用 Windows PE 修复注册表故障
5. 使用 Recuva 向导恢复数据

十四、网络应用及理财安全

1. 增强 QQ 安全性的方法
2. 备份和还原 QQ 聊天记录
3. 加密 QQ 聊天记录
4. 加强支付宝账户的安全防护
5. 加强支付宝手机端安全
6. 加强财付通账户的安全防护
7. 360 安全卫士防范网络钓鱼

十五、移动网络安全

1. 使用 360 手机卫士清理手机
2. 使用 360 手机助手备份 Android 手机数据
3. 使用 91 助手备份和还原用户数据
4. 使用腾讯手机管家优化手机性能
5. Android 手机刷机（仅供参考，慎用）
6. 获取 Android Root 权限
7. 更新平板操作系统
8. 使用 iTunes 备份和还原用户数据
9. 将手机游戏移动到内存卡
10. 蓝牙设备的配对
11. 利用蓝牙在两台设备传递文件
12. 手机短信与照片加密
13. 手机开机密码设置
14. 屏幕锁定
15. PIN 锁屏设置

前言 INTRODUCTION · 全新升级版

从 2003 年起，我国互联网逐渐找到了适合国情的商业模式和发展道路，互联网应用呈现多元化局面，电子商务、网络游戏、视频网站、社交娱乐等百花齐放。计算机技术及通信技术的进一步发展，持续推动我国互联网新一轮的高速增长，到 2008 年，我国当前网民数量已经达到 2.53 亿人，首次大幅度超过美国，跃居世界首位。

2009 年左右开始，移动互联网兴起；互联网与移动互联网共同营造了当前双网互联的盛世。网络已经成为个人生活与工作中获取信息的重要手段，网络购物也已经成为了民众重要的消费渠道。当前，“互联网 +”的战略布局与工业 4.0 的深度发展，使得国家经济发展、民众工作生活都与网络安全休戚相关，一个安全的网络环境是必不可少的。

当前最大的一个问题是广大用户对网络相关软硬件技术的掌握程度远远不够，这就为不法分子提供了大量的机会，借助于计算机网络滋生的各种网络病毒、木马、流氓软件、间谍软件，给广大网络用户的个人信息及财产带来了非常大的威胁。

为提升广大民众对于计算机网络安全知识的掌握程度，做好个人信息财产安全的防护，我们做了这套“黑客攻防从入门到精通”丛书，本书为其中的《黑客攻防从入门到精通（全新升级版）》分册。

丛书书目

黑客攻防从入门到精通（全新升级版）

黑客攻防从入门到精通（Web 技术实战篇）

黑客攻防从入门到精通（Web 脚本编程篇・全新升级版）

黑客攻防从入门到精通（黑客与反黑工具篇・全新升级版）

黑客攻防从入门到精通（加密与解密篇）

黑客攻防从入门到精通（手机安全篇・全新升级版）

黑客攻防从入门到精通（应用大全篇・全新升级版）

黑客攻防从入门到精通（命令实战篇・全新升级版）

黑客攻防从入门到精通（社会工程学篇）

本书特点

- 内容全面：涵盖了从计算机安全攻防的社会工程学，到计算机安全攻防入门，再到专业级的 Web 技术安全知识，适合各个层面、不同基础的读者阅读。此外，本书对当前移动端应用较多的 Wi-Fi、移动支付等新知识进行了重点介绍和剖析。
- 与时俱进：本书主要适用于 Windows 7、Windows 10 的操作系统用户阅读。尽管本书中的许多工具、案例等可以在 Windows XP 等系统下运行或使用，但为了能够顺利学习本书全部的内容，强烈建议广大读者安装 Windows 7 及更高版本的操作系统。
- 任务驱动：本书理论和实例相结合，在介绍完相关知识点以后，即以案例的形式对该知识点进行介绍，加深读者对该知识点的理解和认知能力，力争彻底掌握该知识点。
- 适合阅读：本书摈弃了大量枯燥文字叙述的编写方式，采用图文并茂的方式进行编排，以大量的插图进行讲解，可以让读者的学习过程更加轻松。
- 深入浅出：本书内容从零起步，步步深入，通俗易懂，由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高。
- 赠送超值光盘：针对本书的重点章节，我们录制了视频教学光盘，帮助读者更好地理解和学习本书内容。此外，本书还赠送 140 个 Windows 系统常用快捷键大全、157 个 Linux 基础命令手册、136 个 Linux 系统管理与维护命令手册、58 个 Linux 网络与服务器命令手册、Windows 系统安全与维护手册、计算机硬件管理超级手册、Windows 文件管理高级手册和黑客攻防命令手册等资源。
- 技巧与问答：本书在每章的最后整理了本章相关的练习题，以巩固读者所学知识与技能。相关习题答案请在光盘文件中查阅。

读者对象

- 计算机初、中级用户。
- 网店店主、网店管理及开发人员。
- 计算机爱好者、提高者。
- 各行各业需要网络防护的人员、中小企业的网络管理员。
- Web 前、后端的开发及管理人员。
- 无线网络相关行业的从业人员。
- 计算机及网络相关的培训机构。
- 大中专院校相关学生。

本书结构及内容

全书共 22 章，内容由浅入深，循序渐进，前后衔接紧密，逻辑性较强。

第 1 章　社会工程学

第 2 章　计算机与网络反黑基础

第 3 章　Windows 10 系统防火墙与 Windows Defender

第 4 章　Windows 10 高级安全管理

第 5 章　系统和数据的备份与恢复

第 6 章　计算机与网络控制命令

第 7 章　扫描与嗅探：确定目标与探索网络资源

第 8 章　木马防范技术

第 9 章　病毒防范技术

第 10 章　Windows 系统漏洞攻防技术

第 11 章　计算机后门技术

第 12 章　程序的加密与解密技术

第 13 章　局域网安全防范技术

第 14 章　计算机远程控制技术

第 15 章　Web 站点安全防范技术

第 16 章　清理恶意插件和软件

第 17 章　网游与网吧安全防范技术

第 18 章　网络账号反黑实战

第 19 章　网络支付工具的安全

第 20 章　无线网络安全防范技术基础

第 21 章　Wi-Fi 安全防范技术

第 22 章　蓝牙安全防范技术

后续服务

本书由明月工作室编著，高翔、胡华、闫珊珊、王栋、宗立波、马琳、赵玉萍、栾铭斌等老师也参加了本书部分内容的编写和统稿工作，在此一并表示感谢！在本书的编写过程中，我们竭尽所能地为您呈现最好、最全的实用功能，但仍难免有疏漏和不妥之处，敬请广大读者不吝指正。若您在学习过程中产生疑问或有任何建议，可以通过 E-mail 或 QQ 群与我们联系。

投稿信箱：pup7@pup.cn

读者信箱：2751801073@qq.com

读者交流群：218192911（办公之家）、99839857

郑重声明

本书对大量计算机及移动端的攻击行为进行了曝光，为广大读者做好了安全防范工作。请本书广大读者注意：据国家有关法律规定，任何利用黑客技术攻击他人的行为都是违法的！

目录 CONTENTS