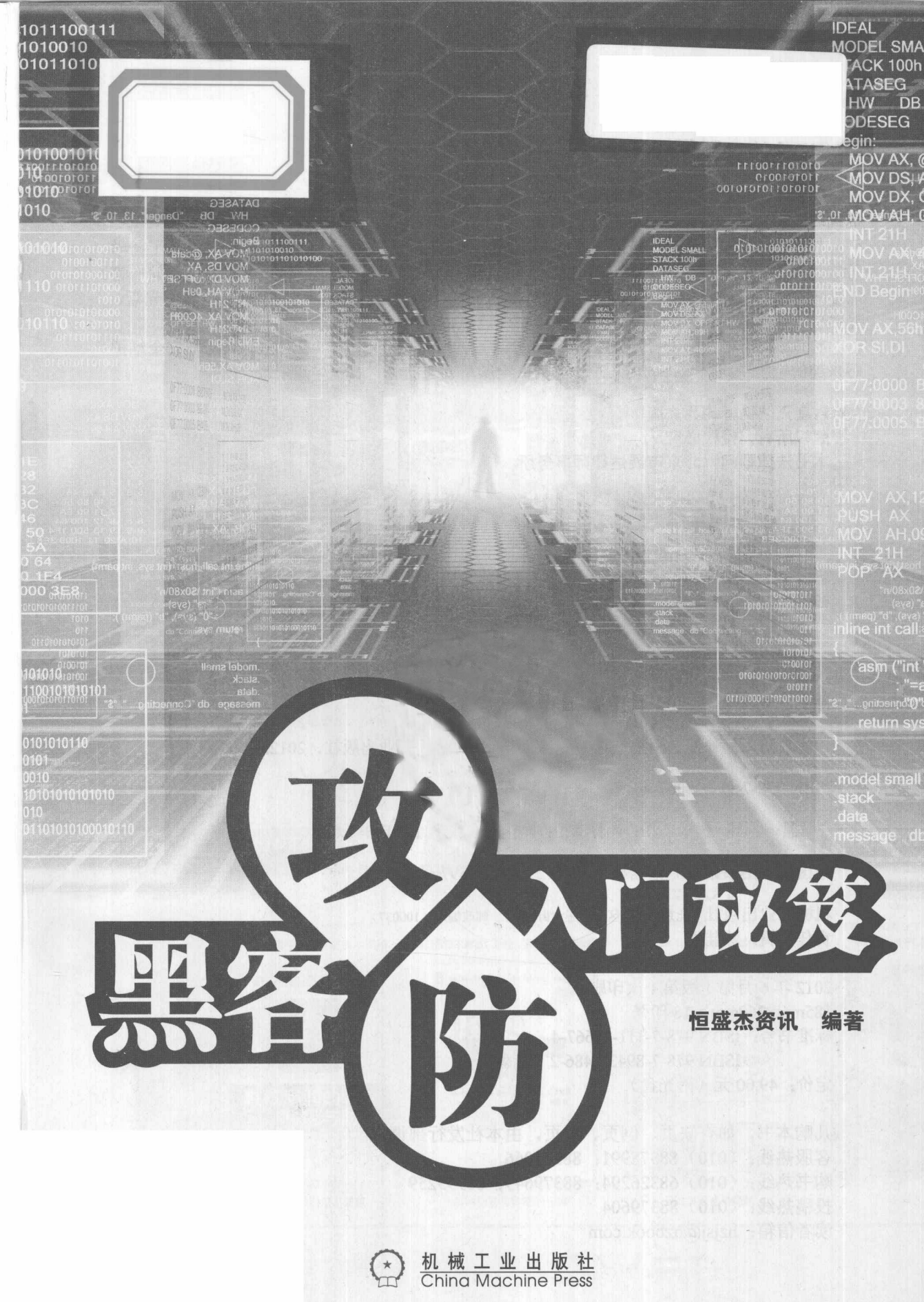

HZ BOOKS
华章科技
“知己知彼，百战不殆”，黑客入门实战揭秘
Hack Attacks and Defenses Unleashed
黑客攻防
入门秘笈
恒盛杰资讯 编著
机械工业出版社
China Machine Press



黑客攻防入门秘笈

恒盛杰资讯　编著

机械工业出版社
China Machine Press

本书全面且详细地介绍了计算机黑客攻防的基础知识，主要包括黑客的定义，黑客必须掌握的常用术语和命令，网络信息的扫描与嗅探，Windows 系统漏洞攻防，木马和病毒攻防，网页、QQ 和 E-mail 攻防，破解常用密码以及提升系统安全性能等，让读者在了解黑客攻击手段的同时，也知道如何采取有效的防范措施。

本书在安排知识点时，按照由易到难、循序渐进的顺序进行排列，最大限度地满足了初学者的学习要求。本书内容全面，图文对应，讲解深浅适宜，叙述条理清楚，并采用了一问一答的形式，让读者不仅能够知其然，而且还能知其所以然。此外，本书还配有多媒体教学光盘，光盘中提供了相关的视频教学演示，读者可通过观看视频来巩固所学的知识。

本书适用于电脑初学者，也适用于电脑维护人员、IT 从业人员以及对黑客攻防与安全维护感兴趣的电脑中级用户，同时还可作为各大电脑培训班的教材及辅导用书。

图书在版编目（CIP）数据

黑客攻防入门秘笈 / 恒盛杰资讯编著. —北京：机械工业出版社，2012.6

ISBN 978-7-111-38667-4

Ⅰ. 黑…　Ⅱ. 恒…　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（2012）第 117597 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）
责任编辑：陈佳媛
中国电影出版社印刷厂印刷
2012 年 6 月第 1 版第 1 次印刷
185mm×260mm • 18 印张
标准书号：ISBN 978-7-111-38667-4
　　ISBN 978-7-89433-486-2（光盘）
定价：49.00 元（附光盘）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

PREFACE
前　言

在由 Internet 组成的网络世界中，总有那么一批人喜欢利用自己的高超技术去控制别人的电脑、偷窥别人的信息。称呼这类人为黑客时，总觉得太高估他们了。因为想要成为一名黑客并非是一两天或者一两个月就能成功的，这需要持之以恒的毅力，不仅要掌握计算机的基础知识，而且还要掌握至少两门编程语言。

Internet 中关于偷窥隐私信息的制度还不完善，仅仅通过法律来约束他们还不够，只有普及黑客知识，让更多的人知晓这类人能够在 Internet 中偷些什么、怎样偷等，才能更好地防止黑客入侵。

本书就是为此而编写的。本书围绕“攻”、“防”两个不同的角度，在介绍黑客攻击手段的同时，也讲解了相应的防范措施，通过黑客常用的入侵工具和浅显易懂的操作步骤向用户展现了黑客入侵网络与防御的全过程。

本书主要内容

本书分为三篇，共 15 章，第一篇为新人入门篇，包括第 1~2 章；第二篇为攻防实战篇，包括第 3~13 章；第三篇为安全与预防篇，包括第 14~15 章。

第 1 章的内容是黑客的基础知识，主要介绍了黑客的定义、成为黑客必须满足的条件、查看 IP 地址和端口以及创建安全的 Windows 7 测试环境等内容。

第 2 章的内容为黑客必须掌握的基础知识，主要介绍了黑客必须知道的术语、网络应用技术以及 DOS 命令等内容。

第 3 章的内容为扫描与嗅探攻防，主要介绍了搜索目标主机信息、扫描主机端口、嗅探数据包以及如何防范端口扫描和嗅探等内容。

第 4 章的内容为 Windows 系统漏洞攻防，主要介绍了 Windows 系统漏洞产生的原因、Windows XP/7 系统中存在的安全漏洞以及如何修补系统漏洞等内容。

第 5 章的内容为木马攻防，主要介绍了木马的概念、自定义配置及捆绑木马以及如何防范木马入侵等内容。

第 6 章的内容为病毒攻防，主要介绍了病毒的概念、如何制作常见的病毒以及如何防范病毒入侵计算机等内容。

第 7 章的内容为密码攻防，主要介绍了加密与解密的概念、如何破解常用文件密码以及如何防范密码被轻易破解等内容。

第 8 章的内容为远程控制攻防，主要介绍了远程控制的概念，利用 IPC$、Telnet 以及注册表实现远程监控，如何有效防范远程监控等内容。

第 9 章的内容为局域网攻防，主要介绍了局域网攻击常见方式、攻击局域网和抵制局域网攻击等内容。

第 10 章的内容为网页攻防，主要介绍了恶意代码的概念、如何利用漏洞攻击网页、防范恶意代码攻击等内容。

第 11 章的内容为 E-mail 攻防，主要介绍了如何盗取邮箱密码、常见的邮件攻击方式与防范等内容。

第 12 章的内容为 QQ 攻防，主要介绍了如何盗取 QQ 密码、如何远程攻击 QQ，以及如何保护 QQ 密码和聊天记录等内容。

第 13 章的内容为隐匿入侵和痕迹清除，主要介绍了隐匿入侵技术、黑客追踪技术以及如何清除自己留下的痕迹等内容。

第 14 章的内容为提升系统安全性能，主要介绍了设置 BIOS 密码、设置开机密码、系统安全设置和清除流氓软件等内容。

第 15 章的内容为做好系统数据的备份措施，主要介绍了系统、数据的备份与还原以及恢复被误删除的数据等内容。

本书特色

本书采用一问一答的形式进行编写，首先利用简短的一句话对提出的问题进行总

结和概括，然后再利用简单易懂的操作步骤或示意图来进行详细的阐释，旨在让用户达到“不仅知其然，而且知其所以然”的目的。

本书既不是全部介绍攻击计算机和盗取用户隐私信息的方法和手段，也不是全部介绍防范黑客攻击采取的有效措施，而是将两者结合起来，让读者不仅知晓怎样攻，同时也知道怎样防。

本书为用户附赠了攻防实战演练的教学视频光盘，通过浏览光盘，可以增加对黑客主流攻击手法感性的认识，使读者提高防范技能，确保自己的系统安全。

由于笔者水平有限，在本书的编写过程中难免会存在一些疏漏之处，希望广大读者发现后批评指正，并提出宝贵的意见。

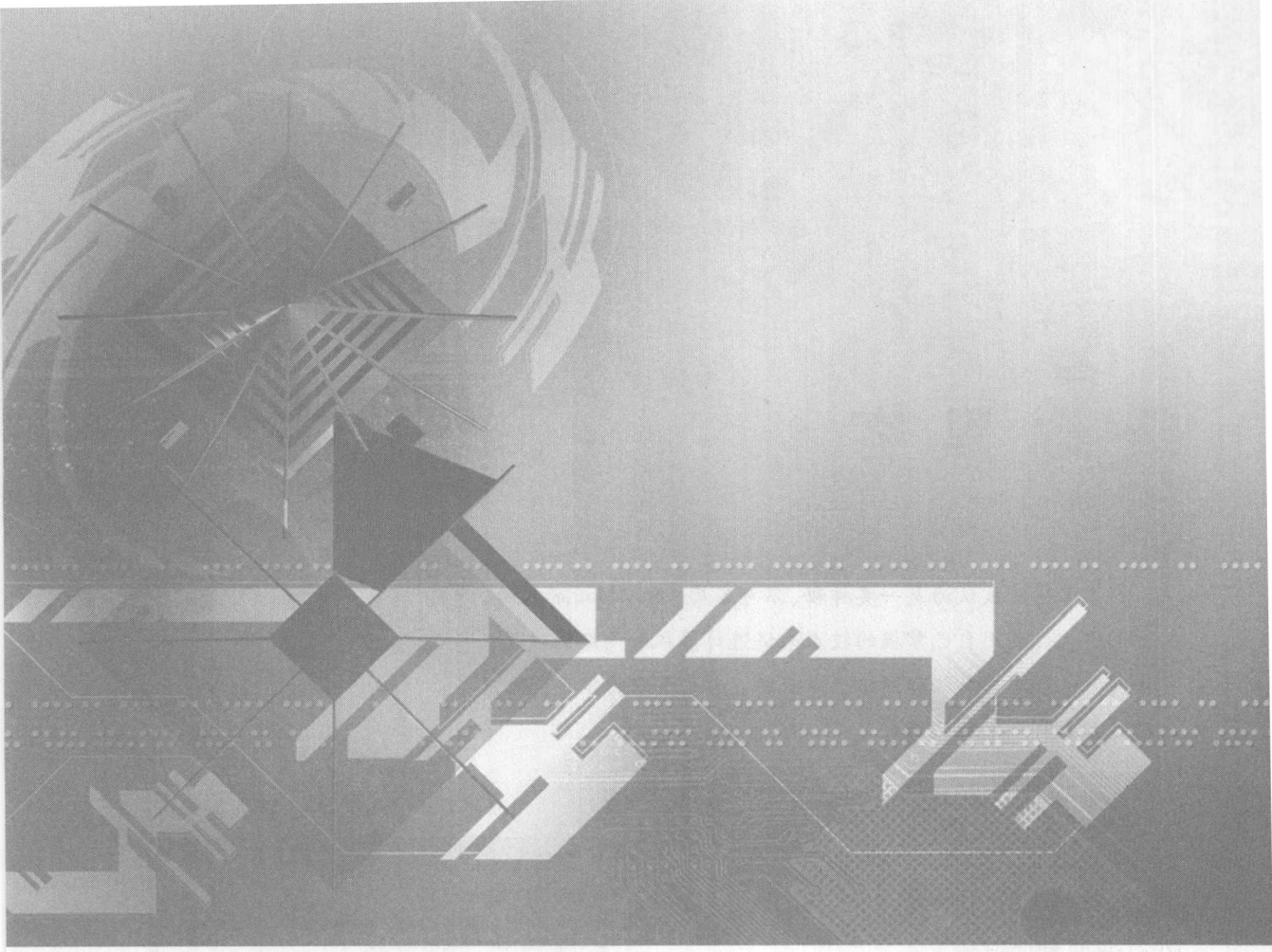
最后需要提醒读者的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，后果自负。

编 者

2012 年 3 月

CONTENTS

目　录



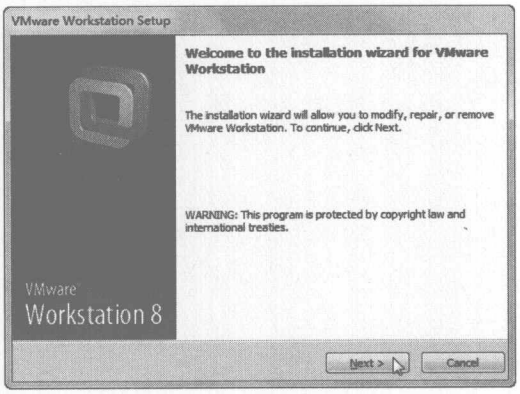
第一篇　新人入门篇

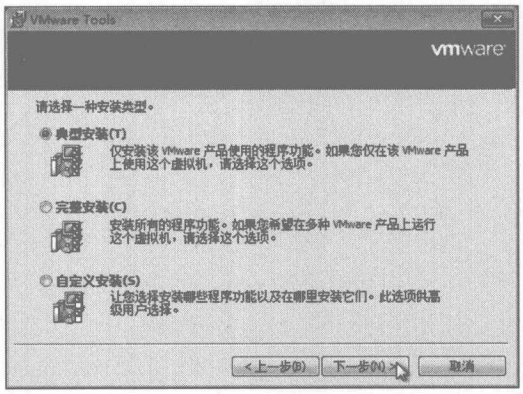
第 1 章
细 说 黑 客

黑客通常被认为是一类神秘、不可琢磨、难以接近的人群，他们通常会利用自己掌握的技术来促进计算机和网络的发展，但同时也会对计算机和网络造成威胁。通过本章的学习，用户对黑客会有一定的认识。

本章知识点：

- ☑ 认识黑客
- ☑ 认识 IP 地址和端口
- ☑ 创建 Windows 7 测试环境





1.1　认识黑客

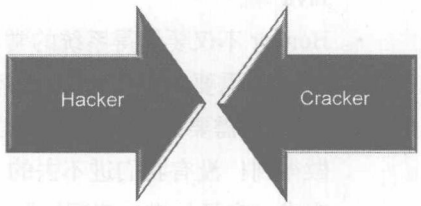
黑客总是给人一种神秘的色彩，仿佛他们不同于常人且难以接近。黑客与普通人有什么区别呢？他们可能是潜伏在网络中的“恐怖分子”或“小偷”，也可能是在进入他人系统后提醒管理员修复漏洞的“无名英雄”，也许是声名显赫的大人物，也可能是名不见经传的少年，下面就来简单介绍黑客是怎样的一类人以及成为黑客需要满足哪些条件。

001 Q 黑客是一类什么样的人？

A　黑客是掌握超高计算机技术的一群人，他们既可推动计算机和网络技术的发展，也可非法破坏或远程控制目标计算机。

黑客是英文单词 Hacker 的中文音译，原意是指热衷于计算机技术、水平高超的电脑专家或程序设计人员。但在今天，黑客则是泛指利用黑客工具或高超的计算机技术来入侵网络中其他的个人计算机、服务器并对其进行破坏的一类人，对这类人应该称之为 Cracker，音译为“骇客”。

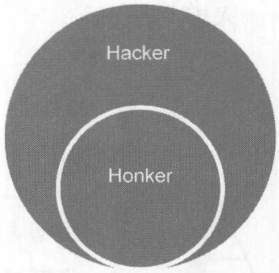
Hacker 热衷于研究和编写程序，他们精通各种计算机语言和系统，伴随着计算机和网络的发展而产生和成长。Hacker 对计算机有着狂热的兴趣和执著的追求，他们不断地学习计算机和网络知识，并运用这些知识来发现计算机和网络中存在的漏洞，然后向管理员提出解决和修补漏洞的方法，从而推动了计算机和网络的发展与完善。Hacker 不干涉政治，不受政治利用，所做的不是恶意破坏，他们是一群纵横于网络上的大侠，追求共享和免费。在黑客圈中，Hacker 一词带有褒义的色彩，例如熟悉操作系统的设计与维护的 System Hacker，精于找出使用者密码的 Password Hacker 以及通晓计算机并且让计算机“乖乖听话”的 Computer Hacker。



Cracker 同样包括含有超高计算机水平的一类人，他们的目的并非是推动计算机和网络的发展与完善，而是通过不正当的手段来破坏他人的电脑或盗取账号、密码等重要资料。Cracker 利用自己掌握的计算机技术或黑客工具来非法入侵网络中的其他个人计算机或服务器，例如将别人的计算机当做跳板来盗取其他计算机的银行账号、密码等资料，还可以在目标计算机中植入木马和病毒，起到随时监控和破坏目标计算机的作用。

002 Q 黑客与红客有什么区别和联系？

A 红客是指维护国家利益，利用自己掌握的网络技术来为自己国家争光的黑客。



红客是英文单词 Honker 的中文音译，它代表着一种精神，即热爱祖国、坚持正义和开拓进取的精神。因此只要具备这种精神并热衷于计算机技术的人都可以成为 Honker。Honker 是 Hacker 中的一部分人，这部分人维护国家利益，不利用掌握的计算机和网络技术入侵自己国家的计算机或服务器。他们维护正义，为自己国家争光。

在中国，由广大红客组成的红客联盟喜欢用《道德经》中的语言表达自己的观点，在红客联盟首页（http://www.cnhonkerarmy.com/）的顶部显示着《道德经》的第一句话——道，可道，非常道。名，可名，非常名。

作为一名 Honker，需要具备以下 9 方面特质。

- Honker 必须爱国。
- Honker 是不会随意炫耀自己掌握的攻防技术的。
- Honker 会将自己掌握的计算机和网络技术与他人一同分享。
- Honker 需要不断地学习，并不断地研究新的攻击技术和防护方法。
- Honker 需要熟练掌握 C 语言，同时还要掌握其他任一门面向对象的语言，例如 C++、Java 等。
- Honker 不仅要懂得系统的常用漏洞攻防之道，而且还要懂得如何去发掘系统的漏洞。
- Honker 需要懂得如何使用搜索引擎这个非常好的学习工具。
- Honker 需要打破常规的思维方式！“没有什么不可能，只要我们想得到，我们就能够做得到！没有我们进不去的‘房间’，只要‘房间’内能够进得去空气，我们就可以变成‘空气’进入房间！”
- Honker 必须懂得如何做人，即学技术先学做人。

003 Q 成为黑客需要满足哪些条件？

A 熟练掌握一定量的英文 + 理解与黑客相关的专用术语 + 熟练使用常用命令和黑客工具 + 掌握主流编程语言

黑客并非一两天就能练成的，这是一个日积月累的过程，需要丰富的知识为基础。仅仅掌

握了一两款黑客工具的使用是远远不够的，需要熟练掌握一定量的英文、理解黑客术语和网络安全术语、熟练使用常用命令和黑客工具以及掌握主流的编程语言和脚本。

熟练掌握一定量的英文

学习英文对黑客来说是非常重要的，仅仅依靠国内的资料和教程无法提高自己的技术，因此需要通过阅读国外的资料和教程来实现。而国外的资料和教程大多数为英文版本，因此需要熟练掌握一定的英文方可正常阅读这些资料。

理解黑客术语和网络安全术语

黑客们在相互交流时通常会使用黑客的相关术语，例如肉鸡、挂马、后门等，如果不理解这些术语，在网络中与其他黑客交流技术或经验时，往往会显得很吃力。由于黑客涉及的知识范围比较广，而最基础的就是网络的相关知识，了解网络的相关知识后，便可以在网络中查找有漏洞的计算机或服务器，并通知管理员及时修补。而网络安全术语则是网络知识的基础部分，包括 TCP/IP 协议、ARP 协议等。

熟练使用常用命令和黑客工具

黑客常用的命令是指日常使用的各种电脑命令，例如 ping、net、nbtstat 等，通过这些命令可以获取目标计算机的 IP 地址和 NetBIOS 等信息。而黑客工具则是在获取这些信息后扫描其端口和存在的漏洞，例如端口、漏洞扫描器以及嗅探器等。由于软件较多，功能各不相同，因此用户需要选择适合自己的工具。

掌握主流的编程语言和脚本

仅仅使用别人提供的黑客工具还不能称为黑客，黑客要有自己独立的思想，通过掌握主流的 C、C++或 Java 等编程语言来创建属于自己的工具，别人提供的工具可以为自己提供一种思路，启发灵感，从而利用掌握的编程语言制作出功能更强大的工具。

1.2 认识 IP 地址和端口

黑客在入侵 Internet 中的计算机之前都需要确定其 IP 地址，然后扫描指定计算机中有哪些开放着的端口，从而猜测出可能存在的漏洞。因此用户需要理解 IP 地址和端口这两个概念，并掌握查看本地计算机的 IP 地址以及打开、关闭端口的操作。