电脑報 总策划

黑客攻防

最佳十一人

网络攻击、防御实例演练

前锋：进攻！一击致命
系统漏洞与网站漏洞攻击
暴力攻击与恶意绑架

中场：创意！制造杀机
远程控制与反控制
信息收集与行踪隐藏
网络嗅探与监控
木马植入与防范

后卫：防卫！转危为安
网络盗号与防范
病毒查杀与防范
网络提权与网吧攻防
数据的加密与解密

守门：不可逾越的防线
网络安全终极防范

黄国耀 李国良 编著

111招攻守博弈！
彻底破解黑客攻防之道！！
成就安全大师！！！

电脑报电子音像出版社
CHIP ELECTRONICS AUDIOVISUAL PRESS

黑客攻防

最佳十一人

网络攻击、防御实例演练

黄国耀 李国良 编著

电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容提要

本手册专为黑客技术与网络安全爱好者量身定制，以实例演练形式为读者详细剖析黑客攻防手段，并提供相应防护措施。手册内容共计11章，内容涵盖信息收集与行踪隐藏、网络嗅探与监听、木马植入与防范、远程控制与反控制、系统漏洞与网站漏洞攻击、暴力攻击与恶意绑架、网络盗号与防范、病毒查杀与防范、网络提权与网吧攻防、数据的加密与解密、网络安全终极防范。丰富的案例、 详尽的操作步骤将给读者提供最快捷的帮助，迅速掌握黑客与网络安全技术。

警告：本手册及光盘涉及到的黑客相关知识，仅供读者研究、学习参考，请勿用于非法用途，否则后果自负。

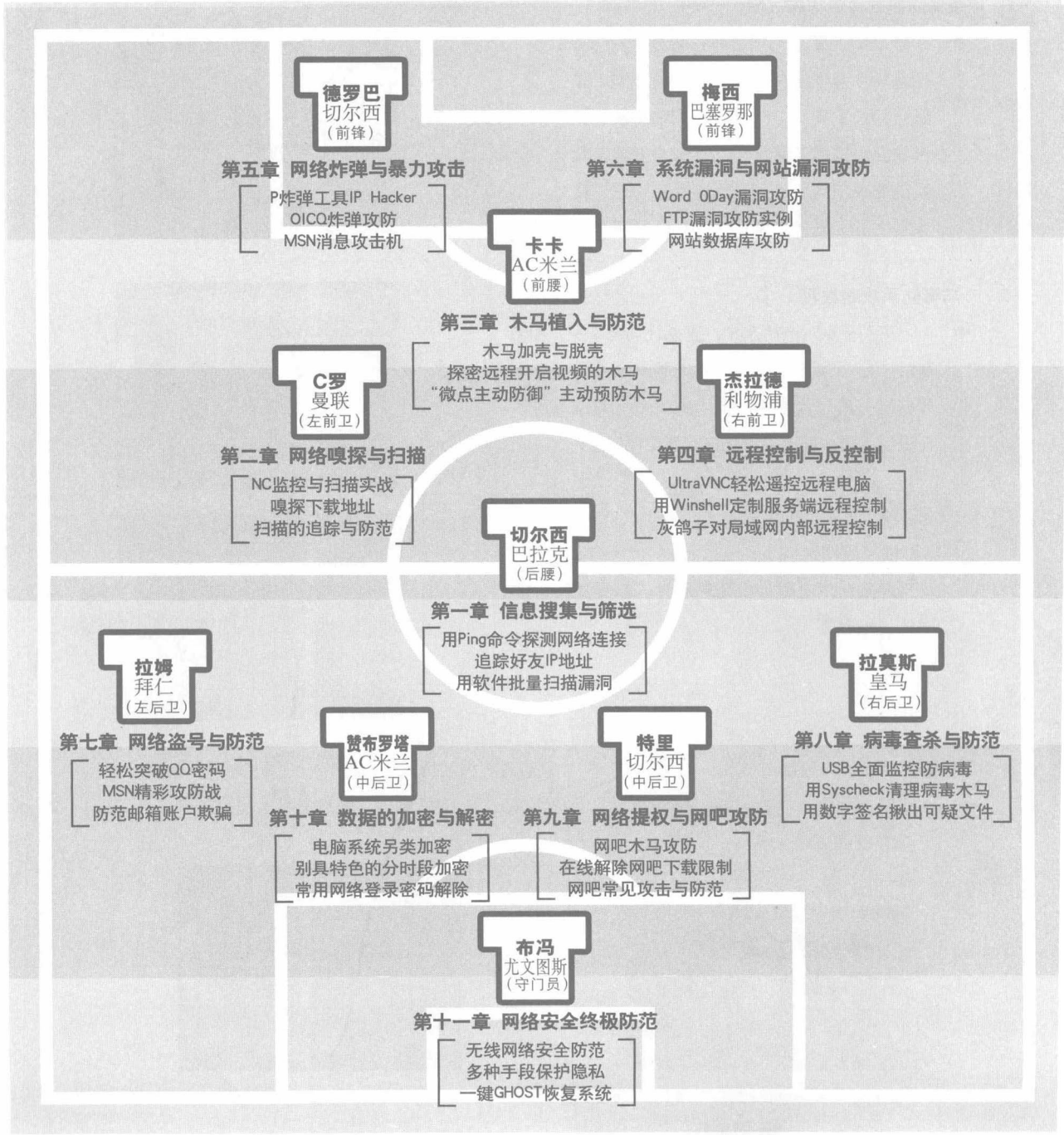
手　册　名：黑客攻防最佳十一人
编　　著：黄国耀　李国良
技术编辑：连　果　李　勇
封面设计：朱　姝
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
对外合作：(023)63658933
发　　行：电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD生产：苏州新海博数码科技有限公司
文本印刷：重庆科情印务有限公司
开本规格：787mm×1092mm 1/16　19印张　350千字
版　　号：ISBN 978-7-89476-128-6
版　　次：2009年4月第1版　2009年4月第1次印刷
定　　价：32.00元(1CD+1手册)

攻守兼备

黑客攻防最佳“十一人”

进攻，无坚不摧；防守，固若金汤。电光火石之间，他们亦能转危为安。这是一支攻守兼备、令人生畏的球队。十一人，或攻或防，进退自如，将足球运动的精髓演绎得如此完美。那么，你想拥有这样一支战无不胜的战队吗？你想拥有这样攻守兼备的“十一人”吗？

不可能？谁说不可能！在我们的电脑、网络生活中，我们同样可以雇佣这样的十一位“铁血硬汉”，打造一支攻守兼备的完美战队。攻，可如探囊取物般行走于网络； 防，可坚如磐石般抵御他人不轨侵袭。不同的十一人，同样的攻守兼备，你不想一试身手吗？现在，这“十一人”将一一亮剑，展示他们的能力和技巧，用好了他们，你将彻底玩转黑客攻防，成就安全大师。



光盘导航

全面、实用黑客攻防工具大全
光盘可自启动、可自动杀毒防黑

杀毒防黑软件精华库

杀毒反黑工具	漏洞检测修复工具
恶意插件清理工具	远程控制工具
账号保护工具	加密解密工具
系统安全辅助工具	浏览安全工具
系统监视工具	网吧管理工具
数据恢复工具	系统补丁程序

防毒防黑攻略教程

高手指点，亲历亲学，查杀现场全掌握。2008灰鸽子超级简单免杀、个人电脑安全设置、揭示局域网抓鸡过程演示、揭示另类木马躲避杀毒软件过程、清除被感染系统中的病毒代码。

黑客影视片段精选

经典谍战电影片段精彩欣赏，感受真实、震撼的现场氛围。

黑客影视海报与壁纸

超20幅谍战电影海报、壁纸欣赏，让精彩瞬间留住永恒。

黑客绚丽屏保

保护屏幕，酷炫桌面，质感体验。

CONTENTS 目录

中场：创意！制造杀机

第一章 巴拉克——信息搜集与筛选

第二章 C罗——网络嗅探与扫描

第四章 杰拉德——远程控制与反控制

前锋：进攻！一击致命

第五章 德罗巴——网络炸弹与暴力攻击

第六章 梅西——系统漏洞与网站漏洞攻防

后卫：防卫！转危为安

第七章 拉姆——网络盗号与防范

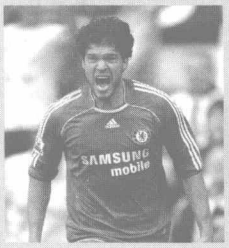
第八章 拉莫斯——病毒查杀与防范

第九章 特里——网络提权与网吧攻防

第十章 赞布罗塔——数据的加密与解密

守门：不可逾越的防线

第十一章 布冯——网络安全终极防范



球星小档案

姓名：巴拉克
国籍：德国（国家队队长、灵魂）
身高：189CM
生日：1976年9月26日
球员身价：1200万欧元
最擅长位置：后腰、中前卫
现效力俱乐部：英格兰超级联赛——切尔西

CHAPTER 01

巴拉克（收集对手信息，从容应对）信息搜集与筛选

巴拉克，德国国家队队长，标准的中场发动机。每次大战前总能精准地收集到对方球员的准确信息和特点，并告诫自己的队友根据对手的习性特点进行有针对性的防御与攻击。

在网络黑客攻防中更是如此，如果可以精准地收集到对方电脑的相关信息，查找和跟踪对方的电脑，则可以做到知己知彼，打有准备之仗。这样无论是攻击还是防御，都可以胜券在握。

第一招 巧用X-scan探测系统版本

每次足球比赛前，足球队员和教练组都要详细地收集对方队员的资料和信息。只有全面了解了对方的信息资料才可以有针对性的破解对方攻击，掌握球场上的主动。

黑客界同样如此：无论目标的规模有多大，安全防范有多严密，只要是人类参与设计及管理，那么人为因素产生的安全问题就一定存在。黑客在执行任务前的信息搜集，就是用于找出这些安全问题。在执行黑客任务之前，应尽量多收集一些关于目标电脑的信息，这些信息主要包括安装的是什么操作系统，提供了哪些服务，开放的端口有哪些，管理员入口是什么，系统或网络管理员的电话、生日、姓名等等。

黑客对一台电脑进行黑客攻击行为，首先要确定这台电脑使用的操作系统是什么。因为对于不同类型的操作系统，其上的系统漏洞有很大的区别，那么黑客使用的方法就会完全不同。甚至，同一类操作系统，安装的SP补丁包版本不同，也可能会导致黑客任务的失败。

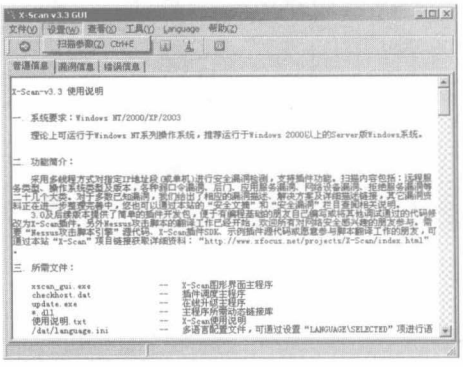
要确定目标电脑正在使用的操作系统是什么，对于初入安防之门的读者来说，推荐使用如下的探测方法来获知。

X-Scan是一款功能比较全面的扫描工具，扫描器是黑客兵器库中不可或缺的一部分，有了它的帮助，“黑客”们就会如虎添翼。扫描器不同于一些常见的攻击工具，它只能用来发现问题，而不能直接攻击目标机器，通过执行如下操作，可以完成远程电脑的操作系统探测。

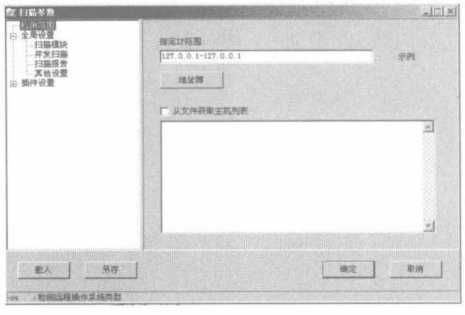
一、设置扫描参数

【第1步】 首先，至国内的著名安全网站“安全焦点”下载X-Scan 中文版。

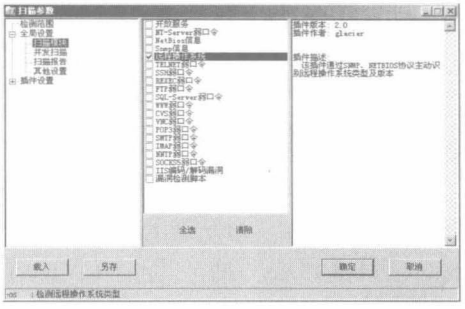
【第2步】 在完成下载并解压后，运行其中的“Xscan_gui.exe”打开如图所示的界面。



【第3步】 依次单击“设置”→“扫描参数”菜单，在弹出的下图所示对话框中，在“检测范围”设置面板的“指定IP范围”栏中输入要扫描的目标电脑的IP地址。



【第4步】 在“全局设置”→“扫描模块”设置界面中勾选“远程操作系统”项，通过右侧的说明，可以看出远程电脑的操作系统识别是通过“SNMP、NETBIOS协议主动识别远程操作系统类型及版本”插件来完成的。



二、开始扫描

单击“确定”按钮返回到“Xscan_gui.exe”主窗口后，单击“开始扫描”按钮后，耐心等待片刻就可以看到如图所示的扫描结果了。

三、查看操作系统版本

在左侧的扫描目标右侧可以看到“Windows 2003”的标识，这告诉我们这是一台正在使用Windows 2003的电脑，进而可以分析出这台电脑可能是台服务器，理由很简单：个人电脑一般是安装Windows XP或Vista。

第二招 用Ping命令探测网络连接

Ping命令是测试网络连接、信息发送和接收状况的实用型工具，这是一个系统内置的探测工具。

一、Ping命令参数介绍

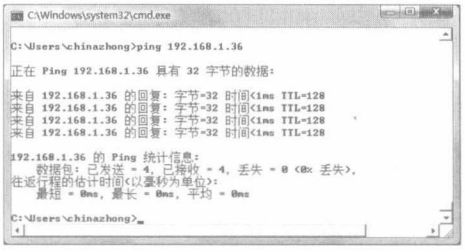
Ping命令的参数作用解释如下：

-t：不断使用Ping命令发送回响请求信息到目的地。要中断并退出Ping，只需按“Ctrl+C”键。初级黑客常喜欢使用这个参数对目标电脑进行攻击。

-a：指定对目的地IP地址进行反向名称解析。如果解析成功，Ping将显示相应的主机名。

-n Count：指定发送回响请求消息的次数，默认值为4。

-l Size：指定发送的回响请求消息中“数据”字段的长度（以字节表示）。默认值为32，如图所示。size的最大值是65,527。



-f：指定发送的回响请求消息带有“不要拆分”标志（所在的 IP 标题设为 1）。回响请求消息不能由目的地路径上的路由器进行拆分。该参数可用于检测并解决“路径最大传输单位（PMTU）”的故障。

-i TTL：指定发送回响请求消息的IP标题中的TTL字段值。其默认值是主机的默认TTL值。对于Windows XP主机，该值一般是128，TTL的

最大值是255。

-v TOS：指定发送回响请求消息的IP标题中的“服务类型（TOS）”字段值。默认值是0。TOS被指定为0到255的十进制数。

-r Count：指定IP标题中的“记录路由”选项用于记录由回响请求消息和相应的回响应答消息使用的路径。路径中的每个跃点都使用“记录路由”选项中的一个值。如果可能，可以指定一个等于或大于来源和目的地之间跃点数的Count。Count的最小值必须为1，最大值为9。

-s Count：指定IP标题中的“Internet时间戳”选项用于记录每个跃点的回响请求消息和相应的回响应答消息的到达时间。Count的最小值必须为1，最大值为4。

-j Path：指定回响请求消息，使用带有HostList指定的中间目的地集的IP标题中的“稀疏资源路由”选项。可以由一个或多个具有松散源路由的路由器分隔连续中间的目的地。主机列表中的地址或名称的最大数为9，主机列表是一系列由空格分开的IP地址（带点的十进制符号）。

-k HostList：指定回响请求消息，使用带有HostList指定的中间目的地集的IP标题中的“严格来源路由”选项。使用严格来源路由，下一个中间目的地必须是直接可达的（必须是路由器接口上的邻居）。主机列表中的地址或名称的最大数为9，主机列表是一系列由空格分开的IP地址（带点的十进制符号）。

-w Timeout：指定等待回响应答消息响应的时间（以微妙计），该回响应答消息响应接收到的指定回响请求消息。如果在超时时间内未接收到回响应答消息，将会显示“请求超时”的错误消息。默认的超时时间为4000（4秒）。

Target Name：指定目的端，它既可以是IP地址，也可以是主机名。

二、Ping命令探测实例

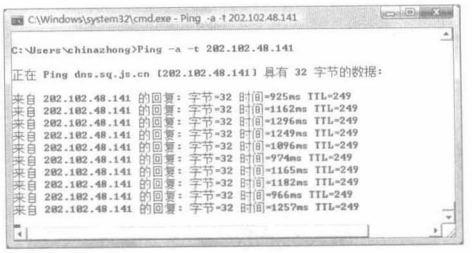
下面给出一些Ping命令的典型使用方法。

1.实例1：检测本机

要检测本机的网卡驱动程序及TCP/IP协议是否正常，只需在“命令提示符”窗口中输入“Ping 127.0.0.1”命令即可。由于127.0.0.1这个保留的IP地址指向到本机，所以能通过此命令来检查本机的网卡驱动。

2.实例2：多参数合用检测

假设，现在使用“Ping -a -t 202.102.48.141”命令对IP地址为202.102.48.141的计算机进行探测，可以得到如图所示的反馈信息。



通过反馈信息，可以得知上述命令中的参数“-a”检测出了该机的Net BIOS名为dns.sq.js.cn；参数“-t”在不断向该机发送数据包。

通常，Ping命令会反馈如下两种结果：

结果1：请求超时

这表示没有收到网络设备返回的响应数据包，也就是说网络不通。出现这个结果原因很复杂，通常有如下几种可能：

* 对方装有防火墙并禁止ICMP回显。

* 对方已经关机。

* 本机的IP设置不正确或网关设置错误。

* 网线不通。

结果2：来自 202.102.*.141 的回复: 字节=32 时间<1ms TTL=128

这表示网络畅通，探测使用的数据包大小为32Bytes，响应时间小于1ms。TTL这个值需要细说一下，TTL全称“Time To Live”，中文意思