

<<黑客攻防入门与实战详解>>

图书基本信息

书名：<<黑客攻防入门与实战详解>>

13位ISBN编号：9787113132439

10位ISBN编号：711313243X

出版时间：2011-9

出版时间：中国铁道

作者：至诚文化

页数：268

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<黑客攻防入门与实战详解>>

内容概要

由至诚文化编著的《黑客攻防入门与实战详解》秉承“知己知彼”的理念。

《黑客攻防入门与实战详解》详细阐述了在网络安全的具体实践中所用到的各类原理、技巧和工具，例如：了解黑客、命令行、端口扫描、漏洞扫描、网络嗅探、局域网干扰防御、木马攻防、痕迹清除与加密破解等，旨在帮助读者清晰地了解入侵者的攻击方式，进而能制作出完善的防御方案，同时从另一个完全不同的角度全面解读系统安全，从而洞察防御的死角，组织更为严密防御体系以应对层出不穷的入侵挑战。

<<黑客攻防入门与实战详解>>

书籍目录

第1章 走近黑客

- 1.1 认识真正的黑客
 - 1.1.1 黑客发展简介
 - 1.1.2 白帽黑客与黑帽黑客
 - 1.1.3 他们是怎样成为黑客的
- 1.2 黑客与程序
 - 1.2.1 黑客攻防与程序
 - 1.2.2 黑客“兵器”分类
- 1.3 黑客“兵器”背后的故事
 - 1.3.1 为何黑客总是偏爱打造神兵利刃
 - 1.3.2 计算机病毒与木马的黑色产业链
 - 1.3.3 流氓软件的生财之道
 - 1.3.4 新兴的手机病毒产业链
- 1.4 善用手中的“兵器”

第2章 黑客与命令行

- 2.1 认识命令行
 - 2.1.1 黑客偏爱命令行的原因
 - 2.1.2 在windows环境下运行命令行程程序
 - 2.1.3 命令行环境的基本操作
- 2.2 网络检测命令
 - 2.2.1 连接测试命令Ping
 - 2.2.2 跃点追踪命令Tracerl
 - 2.2.3 网络连接状态命令Netstat
 - 2.2.4 路由表管理命令Route
 - 2.2.5 硬件地址查询管理命令ARP
- 2.3 命令行窗口下使用Telnet操控远程主机
 - 2.3.1 Telnet登录远程主机
 - 2.3.2 Telnet实战1——远程关机及重启
 - 2.3.3 Telnet实战2——远程进程终止
 - 2.3.4 Telnet实战3——加插管理员账户
 - 2.3.5 Telnet实战4——停用Windows防火墙
 - 2.3.6 Telnet实战5——允许程序通过防火墙
- 2.4 批处理
 - 2.4.1 什么是批处理
 - 2.4.2 一键完成多项黑客任务
 - 2.4.3 让批处理隐藏执行的技巧

第3章 端口扫描

- 3.1 端口扫描基础
 - 3.1.1 什么是端口
 - 3.1.2 获得开放端口的作用与意义
 - 3.1.3 认识常见端口
 - 3.1.4 端口扫描原理简介
- 3.2 局域网扫描实战
 - 3.2.1 共享资源发掘器Netsuper
 - 3.2.2 局域网扫描专家LanSee

<<黑客攻防入门与实战详解>>

3.3 因特网扫描实战

- 3.3.1 Linux / WindOWS两栖扫描软件nmap
- 3.3.2 图形界面的扫描入侵一体化工具X.Scan
- 3.3.3 二级代理隐藏扫描软件x, wAY

3.4 利用端口扫描战果

- 3.5 防御端口扫描
- 3.5.1 停用不必要的服务
- 3.5.2 利用防火墙保护计算机

第4章 漏洞扫描

4.1 漏洞扫描基础

- 4.1.1 漏洞扫描的意义
- 4.1.2 漏洞扫描原理简介

4.2 多平台漏洞扫描工具Nessus

- 4.2.1 注册Nessus
- 4.2.2 添加账户
- 4.2.3 创建扫描策略
- 4.2.4 扫描目标主机

4.3 利用漏洞扫描战果

4.4 修补漏洞

- 4.4.1 通过windows update修补操作系统漏洞
- 4.4.2 修补服务程序漏洞
- 4.4.3 通过漏洞扫描程序修复漏洞

第5章 网络嗅探

5.1 局域网通信基础

- 5.1.1 共享式局域网通信
- 5.1.2 交换式局域网通信

5.2 网络嗅探入门

- 5.2.1 什么是网络嗅探
- 5.2.2 局域网嗅探原理
- 5.2.3 远程嗅探原理
- 5.2.4 认识嗅探的危害

5.3 共享式局域网嗅探实战

- 5.3.1 轻易获得web登录密码——密码监听器
- 5.3.2 ICQ / MSN杀手——Shadow IM sniffer

5.4 交换式局域网嗅探实战

- 5.4.1 全能嗅探器cain简介
- 5.4.2 配置Cain
- 5.4.3 Cain基本应用

5.5 防御嗅探

- 5.5.1 安全登录网站
- 5.5.2 善用Messenger保护盾
- 5.5.3 利用VLAN降低嗅探危害
- 5.5.4 使用IPsec加密通信信息

第6章 局域网干扰与防御

6.1.局域网常见干扰类型

- 6.1.1 广播风暴
- 6.1.2 ARP欺骗及攻击

<<黑客攻防入门与实战详解>>

- 6.1.3 IP地址大规模冲突
- 6.1.4 网关 / 主机拒绝服务
- 6.2 干扰实战
 - 6.2.1 局域网环路干扰
 - 6.2.2 ARP攻击
 - 6.2.3 IP冲突攻击
 - 6.2.4 SYN洪泛攻击
- 6.3 压制及消除广播风暴
 - 6.3.1 检测广播风暴
 - 6.3.2 检查硬件环路
 - 6.3.3 在可管理交换机中使用STP
 - 6.3.4 可管理交换机抑制广播风暴设置
 - 6.3.5 使用VLAN隔绝广播域
- 6.4 防御ARP欺骗及IP冲突攻击
 - 6.4.1 ARP欺骗原理分析
 - 6.4.2 使用静态ARP列表防御
 - 6.4.3 使用ARP防火墙防护
 - 6.4.4 可管理交换机端口绑定MAC
- 6.5 防范SYN洪泛攻击
 - 6.5.1 SYN洪泛攻击原理分析
 - 6.5.2 SYN洪泛防御策略
 - 6.5.3 修改注册表应对小型sYN洪泛
 - 6.5.4 应用冰盾防火墙
- 第7章 无线网络破解
 - 7.1 无线局域网通信基础
 - 7.1.1 Ad.hoc对等无线局域网
 - 7.1.2 AP基础架构无线局域网
 - 7.1.3 无线入侵原理分析
 - 7.1.4 通信距离与定向增幅天线
 - 7.2 入侵wEP加密的无线局域网实战
 - 7.2.1 安装和配置BT3
 - 7.2.2 破解无线网络的wEP认证密码
 - 7.3 防御无线入侵
 - 7.3.1 隐藏或定期修改SSID标识
 - 7.3.2 使用更安全的WPA2—PSK验证
 - 7.3.3 使用不规律的多位密码
 - 7.3.4 使用MAC地址过滤功能
- 第8章 本地入侵
 - 8.1 本地入侵常见手段
 - 8.2 B10S解锁
 - 8.3 光盘启动入侵
 - 8.3.1 窃取硬盘中的资料
 - 8.3.2 修改Windows密码
 - 8.4 MS DaRT密码爆破
 - 8.4.1 安装MS DaRT
 - 8.4.2 制作密码破解光盘
 - 8.4.3 破解windox~rs登录密码

<<黑客攻防入门与实战详解>>

- 8.5 笔记本电脑强化BIOS锁定
- 8.6 防范光盘启动入侵
- 8.7 加密保护重要文件资料
 - 8.7.1 EFS加密
 - 8.7.2 压缩文件加密
- 第9章 网络远程控制
 - 9.1 远程控制入门
 - 9.1.1 了解远程控制
 - 9.1.2 远程控制原理简介
 - 9.1.3 常见远程控制手法
 - 9.2 正向远程控制实战
 - 9.2.1 使用网络工具包Telnet肉鸡
 - 9.2.2 连接3389肉鸡
 - 9.2.3 远程编辑注册表
 - 9.3 穿透内网远程控制
 - 9.3.1 网关端口映射简介
 - 9.3.2 宽带路由器端口映射设置
 - 9.3.3 TeamViewer反弹连接实战
 - 9.4 防御非法远程控制
- 第10章 木马攻防
 - 10.1 认识特洛伊木马
 - 10.1.1 木马与病毒的区别
 - 10.1.2 木马常见功能简介
 - 10.1.3 木马的分类
 - 10.1.4 木马植入受害者计算机的方法
 - 10.2 自定义及配置木马
 - 10.2.1 配置灰鸽子木马
 - 10.2.2 解决无固定IP时使用灰鸽子的问题
 - 10.2.3 控制灰鸽子服务端
 - 10.3 木马防杀
 - 10.3.1 花指令木马防杀
 - 10.3.2 木马加壳防杀
 - 10.4 网页挂马
 - 10.4.1 将木马程序构造成网页木马
 - 10.4.2 入侵服务器后添加挂站代码
 - 10.5 个人用户封杀木马
 - 10.5.1 使用杀毒软件
 - 10.5.2 使用网络防火墙
 - 10.5.3 开启系统自动更新功能
 - 10.6 网站防挂马指南
 - 10.6.1 及时更新网站程序补丁
 - 10.6.2 检测网页挂马
 - 10.6.3 使用web应用防火墙
- 第11章 跳板与痕迹清除
 - 11.1 黑客是如何自保的
 - 11.1.1 利用跳板阻断追踪
 - 11.1.2 获取优质代理跳板

<<黑客攻防入门与实战详解>>

- 11.1.3 设置代理跳板
- 11.1.4 实现多层代理
- 11.1.5 使用CCProxy转换通信协议
- 11.1.6 Tor路由隐匿术
- 11.2 清除日志
 - 11.2.1 清除Windows默认日志
 - 11.2.2 清除IIS日志
 - 11.2.3 清除防火墙日志
- 11.3 反追踪自检
 - 11.3.1 COFEE简介
 - 11.3.2 使用COFEE检查取证
- 第12章 加密破解
 - 12.1 加密解密基础
 - 12.1.1 加密与电子签名
 - 12.1.2 算法与密钥
 - 12.1.3 PKI架构
 - 12.2 破解windows EFS加密
 - 12.3 破解压缩文档密码
 - 12.4 破解Office加密文件
 - 12.5 破解加密的PDF电子文档
 - 12.6 修改Office加密算法及密钥长度
 - 12.7 使用Bitlocker强化windows加密安全
 - 12.7.1 让未配置TPM的计算机也能使用Bitlocker
 - 12.7.2 使用Bitlocker加密系统分区
 - 12.7.3 加密移动存储启动器
 - 12.7.4 解除Bitlocker加密
- 附录A：相关法律法规
- 附录B：端口、服务及说明
- 附录C：BackTrack3支持的网卡芯片

章节摘录

版权页：插图：虽然反弹连接可穿透内网，并利用防火墙开放的端口连接外网的客户端，但它也有不足的地方，那就是要求客户端必须拥有固定的IP地址（或域名）和通信端口。

如果管理员察觉到隐藏于主机的。

服务器端，很容易顺藤摸瓜，通过服务器端的连接请求找到黑客。

3. 中继连接 中继连接是反弹连接的加强，它在服务器端和客户端连接的过程中添加了一个代理服务器作为跳板，服务器端不再需要指定客户端的IP地址和端口，从而增强了客户端的隐蔽性。

中继连接有半反弹端口技术和全反弹端口技术两种。

半反弹技术是指客户端将自己的IP地址、监听端口，以及连接命令上传到充当跳板的代理服务器，而服务器端则每隔一段时间会自动查看代理服务器上有没有来自客户端的连接指令。

如果发现有，则会向客户端上传到代理服务器的IP地址和监听端口发送连接请求，当客户端回复请求后，客户端和服务器端就可以开始建立连接了，如图9-3所示。

全反弹技术是指客户端将对服务器端的控制指令（如破坏指令）上传到代理服务器，服务器端则每隔一段时间查看代理服务器上有没有控制指令。

如果发现有，则按照指令执行，并将执行结果上传到代理服务器，而客户端也会每隔一段时间查看代理服务器上有没有来自服务器端的执行结果。

与半反弹技术相比较，全反弹技术显然更具隐蔽性，如图9-4所示。

<<黑客攻防入门与实战详解>>

编辑推荐

《黑客攻防入门与实战详解》所谓“知己知彼，百战不殆”，要应对这类黑客入侵，最切实可行的方法就是了解广泛流传的各类黑客“兵器”，从它们的攻击特性着手，有的放矢进行针对性的拦截及防御。

<<黑客攻防入门与实战详解>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>