

<<黑客任务实战>>

图书基本信息

书名：<<黑客任务实战>>

13位ISBN编号：9787894980816

10位ISBN编号：7894980811

出版时间：2003-2-1

出版时间：北京希望电

作者：程秉辉,JOHN HAWKE

页数：478

字数：552000

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>

## &lt;&lt;黑客任务实战&gt;&gt;

## 内容概要

网站服务器的黑客攻防一直是网络安全中重要的一部分。本书作者在经过数月的努力之后，终于将网站服务器的黑客攻防以深入浅出、简单易懂的方式呈现在您的眼前，让您不必具有高深的网络知识和经验，只要依照本书的操作说明来按图索骥的进行，就可以完成许多看似不能的黑客任务，让您充分了解与感受到黑客高手的技巧和行为，如此网管人员才可对症下药，防止黑客的入侵与破坏。

本书中详细的讨论了Unicode、IIS错误解码、CGI解译错误等漏洞的详细攻防操作，同时针对最近几年黑客最流行的远程缓冲区溢出漏洞入侵（Remote Buffer Overflow）进行完整研究，包含.ida/idq、.printer、FrontPage 2K Extension Server等漏洞的攻略操作；另外如更换网页、服务器瘫痪攻击与死机、清理服务器中的日志让黑客全身而退等内容在本书中都有详尽的讨论，再加上本书作者精心设计的漏洞扫描程序、远程溢出入侵程序和IIS瘫痪工具，更让黑客任务平易近人，而同时，网络管理员也将从本书中找到如何防护自己的网站的绝佳思路。

本书适合于所有上网用户增强网络安全意识，同时对网络管理员和致力于网络安全的开发人员有很大参考价值。

本书CD包含端口列表、各地IP地址详细列表、NetBrute Scanner、Clearlogs、N-Stealth等多项黑客必备软件。

## &lt;&lt;黑客任务实战&gt;&gt;

## 书籍目录

- 第1章 服务器的攻防观念与准备工作 ( Basic Concept and Preparing for Hacking Web Server ) Q1 : 入侵或攻击网站或服务器 ( 如 : WebServer、PTP Server ) 的原理与观念是什么 ?
- Q2 : 对Internet上的各类服务器进行黑客任务有哪些方法可使用 ? 各有何优缺点 ?
- Q3 : 什么是服务器漏洞 ?
- 如何找出服务器漏洞 ?
- 哪些服务器系统有漏洞 ?
- Q4 : 如何利用漏洞方式来入侵或攻击Internet上的各类服务器 ?
- Q5 : 利用漏洞入侵或攻击Internet服务器有哪些标准步骤与操作 ?
- Q6 : 利用漏洞可以进行哪些黑客任务 ?
- Q7 : 入侵或攻击Internet上的各类服务器需要隐藏自己的上网IP吗 ?
- Q8 : 如何判断与决定对Internet服务器进行黑客任务时需要隐藏IP ?
- Q9 : 隐藏上网IP有哪些方法 ?
- 如何做到 ?
- Q10 : 如何判断与决定是否要清除进行黑客任务时留在服务器中的各种记录 ?
- Q11 : 进行黑客任务时可能留在服务器中的各种记录要如何清理 ?
- Q12 : 如何从各种记录中查看找出可能的黑客入侵 ?
- Q13 : 有哪些方法可以尽可能防止各种日志文件被黑客更改或删除 ?
- 第2章 IIS服务器攻防战 ( Hacking and Defense for IIS Server ) Q14 : 有哪些方法可以进入IIS服务器中 ?
- Q15 : 如何进入IIS服务器来更换网页、植入木马程序、复制文件...等工作 ?
- Q16 : 如何利用FrontPage的远程管理功能来更改网页 ?
- Q17 : 如何找出或猜测FrontPage远程管理功能的用户名称与密码 ?
- Q18 : 如何彻底防止黑客利用FrontPage的远程管理功能来更改网页 ?
- Q19 : 什么是Unicode漏洞 ?
- 如何利用它来发展出各种不同的黑客任务 ?
- Q20 : 如何利用Unicode漏洞来获得最高权限帐户、修改网页、上传文件、植入木马程序或偷取各种文件 ?
- Q21 : 如何利用Unicode漏洞来打开资源管理器连接目标服务器的大门 ?
- Q22 : 如何对Unicode漏洞彻底修补以防止黑客入侵 ?
- Q23 : 什么是IIS错误解码漏洞 ?
- 如何利用它 ?
- Q24 : IIS错误解码漏洞到底有多少种 ?
- 如何找出所有的IIS解码漏洞 ?
- Q25 : 如何将IIS错误解码漏洞彻底修补 ?
- Q26 : 什么是CGI解译错误漏洞 ?
- 对黑客的价值有多高 ?
- Q27 : 为何CGI解译错误漏洞不易使用 ?
- Q28 : 如何对CGI解译错误漏洞进行修补 ?
- Q29 : 什么是.ida/.ida缓冲区溢出漏洞?如何使用 ?
- Q30 : 如何利用.ida/.ida缓冲区溢出漏洞来入侵网站服务器与创建最高权限帐户 ?
- Q31 : 如何修补.ida/.ida缓冲区溢出漏洞 ?
- Q32 : 什么是.printer缓冲区溢出漏洞 ?
- 如何使用 ?
- Q33 : 如何利用.printer缓冲区溢出漏洞来入侵网站服务器与创建最高权限帐户 ?

<<黑客任务实战>>

Q34：如何修补.printer缓冲区溢出漏洞？

Q35：什么是Frontpage 2000服务器扩展缓冲区溢出漏洞？

如何使用？

Q36：如何利用Frontpage 2000服务器扩展缓冲区溢出漏洞来入侵网站服务器与创建最高权限帐户？

Q37：如何修补Frontpage 2000服务器扩展缓冲区溢出漏洞？

第3章 拒绝服务攻击与防护 ( Hacking and Patch the Exploits for Denial of Service ) Q38：什么是拒绝服务攻击？

它会造成哪些影响？

Q39：拒绝服务攻击 ( DOS , DenialofService ) 通常有哪些方式？

各有何优缺点？

基本原理为何？

Q40：什么是分布式攻击 ( DDOS ) ？

它与一般拒绝服务攻击 ( DoS ) 有何不同？

Q41：什么是.ida/ida缓冲区溢出漏洞宁如何利用它来进行拒绝服务攻击？

Q42：如何修补.ida/ida缓冲区溢出漏洞？

Q43：什么是.asp缓冲区溢出漏洞？

如何利用它来进行拒绝服务攻击？

Q44：如何让ASP网站或局域网 ( 或Intranet ) 中的网站严重瘫痪？

Q45：如何修补.asp缓冲区溢出漏洞？

Q46：什么是.printer缓冲区溢出漏洞？

如何利用它来进行拒绝服务攻击？

Q47：如何修补.printer缓冲区溢出漏洞？

Q48：什么是Frontpage Web页面处理漏洞？

如何利用它进行拒绝服务攻击？

Q49：如何修补Frontpage Web页面处理漏洞？

Q50：什么是SMB缓冲区溢出漏洞？

它有多可怕？

如何使用它？

Q51：如何彻底修补SMB缓冲区溢出漏洞？

附录A 各地IP地址详细列表附录B NetBrute Scanner附录C Claerlogs附录D N-Stealth附录E X-Scan

附录F Tftpd32附录G IIS SYSTEM Privilege Client附录H OFScan附录I Hackfp2k附录J IIS\_DoS附

录K Angry IP Scanner附录L TaskInfo附录M SMBdie附录N Cacheman附录O GetRight附录P 流光 ( Fluxay ) 附录Q CleanIISLog附录R idshack与iis5hack

#### 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>