Tell Us What You Think

Introduction

1. Introduction
   The Golden Age of Hacking
   How Bad Is the Problem?
   What Are Companies Doing?
   What Should Companies Be Doing?
   Defense in Depth
   Purpose of This Book
   Legal Stuff
   What's Covered In This Book
   Summary

2. How and Why Hackers Do It
   What Is an Exploit?
   The Attacker's Process
   The Types of Attacks
   Categories of Exploits
   Routes Attackers Use to Get In
   Goals Attackers Try to Achieve
   Summary

3. Information Gathering
   Steps for Gathering Information
   Information Gathering Summary
   Red Teaming
   Summary

4. Spoofing
   Why Spoof?
   Types of Spoofing
   Summary

5. Session Hijacking
   Spoofing versus Hijacking
   Types of Session Hijacking
   TCP/IP Concepts
   Detailed Description of Session Hijacking
   ACK Storms
   Programs That Perform Hijacking
   Dangers Posed by Hijacking
   Protecting Against Session Hijacking
   Summary

6. Denial of Service Attacks
   What Is a Denial of Service Attack?
   What Is a Distributed Denial of Service Attack?
   Why Are They Difficult to Protect Against?
   Types of Denial of Service Attacks
   Tools for Running DOS Attacks
   Tools for Running DDOS Attacks
   Preventing Denial of Service Attacks
   Preventing Distributed Denial of Service Attacks
   Summary

7. Buffer Overflow Attacks
What Is a Buffer Overflow?
How Do Buffer Overflows Work?
Types of Buffer Overflow Attacks
Why Are So Many Programs Vulnerable?
Sample Buffer Overflow
Protecting Our Sample Application
Ten Buffer Overflow Attacks
Protection Against Buffer Overflow Attacks
Summary

8. Password Security
Typical Attack
The Current State of Passwords
History of Passwords
Future of Passwords
Password Management
Password Attacks
Summary

9. Microsoft NT Password Crackers
Where Are Passwords Stored in NT?
How Does NT Encrypt Passwords?
All Passwords Can Be Cracked (NT Just Makes It Easier)
NT Password-Cracking Programs
Comparison
Extracting Password Hashes
Protecting Against NT Password Crackers
Summary

10. UNIX Password Crackers
Where Are the Passwords Stored in UNIX?
How Does UNIX Encrypt Passwords?
UNIX Password-Cracking Programs
Comparison
Protecting Against UNIX Password Crackers
Summary

11. Fundamentals of Microsoft NT
Overview of NT Security
Availability of Source Code
NT Fundamentals
Summary

12. Specific Exploits for NT
Exploits for NT
Summary

13. Fundamentals of UNIX
Linux
Vulnerable Areas of UNIX
UNIX Fundamentals
Summary

14. Specific Exploits for UNIX

UNIX Exploits
Summary

15. Preserving Access
Backdoors and Trojans
Rootkits
NT Backdoors
Summary

16. Covering the Tracks
How To Cover One's Tracks
Summary

17. Other Types of Attacks
Bind 8.2 NXT Exploit
Cookies Exploit
SNMP Community Strings
Sniffing and Dsniff
PGP ADK Exploit
Cisco IOS Password Vulnerability
Man-in-the-Middle Attack Against Key Exchange
HTTP Tunnel Exploit
Summary

18. SANS Top 10
The SANS Top 10 Exploits
Commonly Probed Ports
Determining Vulnerabilities Against the SANS Top 10
Summary

19. Putting It All Together
Attack Scenarios
Summary

20. Summary
Security Cannot Be Ignored
General Tips for Protecting a Site
Things Will Get Worse Before They Get Better
What Does the Future Hold?
Conclusion

A. References
Hacker/Security Related URLs
Hacker/Security Tools
General Security Related Sites