

- [Table of Contents](#)
- [Index](#)
- [Examples](#)

## **Maximum Security, Fourth Edition**

By Anonymous

Publisher: Que  
Date Published: December 16, 2002  
ISBN: 0-672-32459-8  
Pages: 976  
Slots: <sub>1</sub>

[Copyright](#)

[About the Lead Author](#)

[About the Contributing Authors](#)

[Acknowledgments](#)

[We Want to Hear from You!](#)

[Reader Services](#)

[Introduction](#)

[Why Did We Write This Book?](#)

[System Requirements](#)

[About Examples in This Book](#)

[A Final Note](#)

[Part I: Security Concepts](#)

[Chapter 1. Building a Roadmap for Securing Your Enterprise](#)

[Reactive Versus Proactive Models](#)

[Understanding Your Enterprise](#)

[Risk Assessment: Evaluating Your Enterprise's Security Posture](#)

[Identifying Digital Assets](#)

[Protecting Assets](#)

[Incident Response Policy](#)

[Training Users and Administrators](#)

[40,000-Foot Review](#)

[Summary](#)

[Chapter 2. The State of the Net: A World at War](#)

[Hacking, Cracking, and Other Malicious Behavior](#)

[Governments at War](#)  
[The State of the Government](#)  
[The State of the Corporate Sector](#)  
[A Warning](#)  
[Summary](#)  
[Additional Information](#)

[Chapter 3. Hackers and Crackers](#)  
[The Difference Between Hackers and Crackers](#)  
[Tools of the Trade](#)  
[Exploits and the SANS Top 20](#)  
[Summary](#)

[Chapter 4. Mining the Data Monster](#)  
[Information Overload](#)  
[How Much Security Do You Need?](#)  
[General Sources](#)  
[Mailing Lists](#)  
[Usenet Newsgroups](#)  
[Vendor Security Mailing Lists, Patch Depositories, and Resources](#)  
[Summary](#)

[Chapter 5. Internal Security](#)  
[Internal Security: The Red-Headed Stepchild](#)  
[Internal Risks: Types of Harm and Vectors](#)  
[Risk Mitigation Policies](#)  
[Products](#)  
[Resources](#)  
[Summary](#)

## [Part II: Hacking 101](#)

[Chapter 6. A Brief TCP/IP Primer](#)  
[What Is TCP/IP?](#)  
[How Does TCP/IP Work?](#)  
[The Individual Protocols](#)  
[IPsec, IPv6, VPNs, and Looking Ahead](#)  
[Summary](#)

[Chapter 7. Spoofing Attacks](#)  
[What Is Spoofing?](#)  
[Internet Security Fundamentals](#)  
[The Mechanics of a Spoofing Attack](#)  
[Documents Related Specifically to IP Spoofing](#)  
[How Do I Prevent IP Spoofing Attacks?](#)  
[Other Strange and Offbeat Spoofing Attacks](#)  
[Summary](#)

## [Chapter 8. Personal Privacy](#)

- [Degrees of Exposure](#)
- [Web Browsing and Invasion of Privacy](#)
- [Browser Security](#)
- [Your Email Address and Usenet](#)
- [At Work](#)
- [A Warning](#)

## [Chapter 9. Dispelling Some of the Myths](#)

- [When Can Attacks Occur?](#)
- [What Kinds of Attackers Exist?](#)
- [Operating Systems Used by Crackers](#)
- [Is There a Typical Attack?](#)
- [Who Gets Targeted Most Frequently?](#)
- [What Is the Motivation Behind Attacks?](#)
- [Summary](#)

## [Part III: A Defender's Toolkit](#)

### [Chapter 10. Firewalls](#)

- [What Is a Firewall?](#)
- [Other Features Found in Firewall Products](#)
- [Firewalls Are Not Bulletproof](#)
- [A Look Under the Hood of Firewalling Products](#)
- [Programmers Bypassing the Firewall](#)
- [Pitfalls of Firewalling](#)
- [Firewall Appliances](#)
- [Building Firewalls in the Real World](#)
- [Sample Failures of Firewall Technology](#)
- [Commercial Firewalls](#)
- [Summary](#)

### [Chapter 11. Vulnerability Assessment Tools \(Scanners\)](#)

- [The History of Vulnerability Scanners](#)
- [How Vulnerability Scanners Work](#)
- [What to Look For When Choosing a Scanner](#)
- [Fundamental Shortcomings](#)
- [Top Vulnerability Scanners](#)
- [Other Vulnerability Scanners](#)
- [Summary](#)

### [Chapter 12. Intrusion Detection Systems](#)

- [An Introduction to Intrusion Detection](#)
- [Network-Based IDSs](#)
- [Host-Based ID Systems](#)
- [Anomaly-Based IDSs](#)

[What to Look for When Choosing an IDS](#)  
[Snort and Other Open Source IDS Solutions](#)  
[Intrusion Detection Product Listing](#)  
[Summary](#)

#### [Chapter 13. Logging Tools](#)

[Why Log?](#)  
[Logs from a Cracking Perspective](#)  
[Forming a Logging Strategy](#)  
[Network Monitoring and Data Collection](#)  
[Tools for Analyzing Log Files](#)  
[Summary](#)

#### [Chapter 14. Password Security](#)

[An Introduction to Password Cracking](#)  
[The Password-Cracking Process](#)  
[The Password Crackers](#)  
[Password Crackers for Windows](#)  
[Unix Password Cracking](#)  
[Cracking Cisco, Application, and Other Password Types](#)  
[Improving Your Site's Passwords](#)  
[Other Resources](#)  
[Summary](#)

#### [Chapter 15. Sniffers](#)

[Sniffers as Security Risks](#)  
[What Level of Risk Do Sniffers Represent?](#)  
[Has Anyone Actually Seen a Sniffer Attack?](#)  
[What Information Do Sniffers Capture?](#)  
[Where Is One Likely to Find a Sniffer?](#)  
[Where Can I Get a Sniffer?](#)  
[Defeating Sniffer Attacks](#)  
[Summary](#)  
[Further Reading on Sniffers](#)

#### [Part IV: Weapons of Mass Destruction](#)

##### [Chapter 16. Denial-of-Service Attacks](#)

[What Is Denial of Service?](#)  
[Exploitation and Denial of Service](#)  
[Denial-of-Service Attack Index](#)  
[Summary](#)  
[Other DoS Resources](#)

##### [Chapter 17. Viruses and Worms](#)

[Understanding Viruses and Worms](#)  
[Objects at Risk of Virus Infection](#)

[Who Writes Viruses, and Why?](#)

[Antivirus Utilities](#)

[Future Trends in Viral Malware](#)

[Publications and Sites](#)

[Summary](#)

[Chapter 18. Trojans](#)

[What Is a Trojan?](#)

[Where Do Trojans Come From?](#)

[How Often Are Trojans Really Discovered?](#)

[What Level of Risk Do Trojans Represent?](#)

[How Do I Detect a Trojan?](#)

[Resources](#)

[Summary](#)

[Part V: Architecture, Platforms, and Security](#)

[Chapter 19. Network Architecture Considerations](#)

[Network Architecture](#)

[Protecting the Castle](#)

[Summary](#)

[Chapter 20. Microsoft](#)

[Windows 9x and Windows Me](#)

[Windows NT](#)

[Internal Windows NT Security](#)

[Windows 2000](#)

[Windows XP](#)

[Modern Vulnerabilities in Microsoft Applications](#)

[Summary](#)

[Chapter 21. Unix](#)

[A Whistle-Stop Tour of Unix History](#)

[Classifying Unix Distributions](#)

[Security Considerations in Choosing a Distribution](#)

[Unix Security Risks](#)

[Breaking set-uid Programs for Fun and Profit](#)

[Rootkits and Defenses](#)

[Host Network Security](#)

[Telnet](#)

[An Essential Tool: Secure Shell](#)

[FTP](#)

[The r Services](#)

[REXEC](#)

[SMTP](#)

[DNS](#)

[finger](#)

[SNMP](#)  
[Network File System](#)  
[The Caveats of chroot](#)  
[Better the Daemon You Know...](#)  
[Assessing Your Unix Systems for Vulnerabilities](#)  
[Summary](#)

#### [Chapter 22. Novell NetWare](#)

[The OS Facts of Life](#)  
[Watching the Big Three](#)  
[Further Reading](#)  
[Summary](#)

#### [Chapter 23. Routers, Switches, and Hubs](#)

[The Problems with Infrastructure Equipment](#)  
[Keeping Up with OS Revisions](#)  
[Securing Hubs](#)  
[Securing Switches](#)  
[Securing and Configuring Routers](#)  
[Network Management Considerations](#)  
[Preventing Spoofing and Other Packet Games](#)  
[Summary](#)  
[Further Reading and Reference](#)

#### [Chapter 24. Macintosh](#)

[Mac OS X—Apple's New Operating System](#)  
[Establishing the Macintosh as a Server](#)  
[Vulnerabilities on the Macintosh Platform](#)  
[About File Sharing and Security](#)  
[Server Management and Security](#)  
[Firewall Protection](#)  
[Internal Security](#)  
[Password Crackers and Related Utilities](#)  
[Anonymous Email and Mailbombing](#)  
[Macintosh Viruses, Worms, and Antivirus Solutions](#)  
[Spyware and Detection](#)  
[Resources](#)

#### [Chapter 25. Policies, Procedures, and Enforcement](#)

[The Importance of Security Policies](#)  
[Site and Infrastructure Security Policy](#)  
[Acceptable Use](#)  
[Enforcement of Policy](#)  
[Summary](#)

### [Part VI: Security and Integrated Services](#)

[Chapter 26. Secure Application Development, Languages, and Extensions](#)

[Security and Software](#)

[What Is a Secure Application?](#)

[A Security Architecture](#)

[Security-Aware Designs](#)

[Secure Coding Practices](#)

[Summary](#)

[Chapter 27. Wireless Security Auditing](#)

[Wireless LAN Topology](#)

[Access Points](#)

[Antennas](#)

[Wireless Networking Cards](#)

[Handheld Devices](#)

[Constructing a Wireless Test Lab](#)

[Wireless Attacks](#)

[Surveillance](#)

[War Driving](#)

[Client-to-Client Hacking](#)

[Rogue Access Points](#)

[Jamming \(Denial of Service\)](#)

[Practical WEP Cracking](#)

[Summary](#)

[Part VII: References](#)

[Appendix A. Security Bibliography—Further Reading](#)

[General Internet Security](#)

[TCP/IP](#)

[On NetWare](#)

[Appendix B. How to Get More Information](#)

[Establishment Resources](#)

[Underground Resources](#)

[Appendix C. Vendor Information and Security Standards](#)

[Vendor Security Information](#)

[RFC Documents Relevant to Security](#)

[Appendix D. What's on the CD-ROM](#)

[Glossary](#)

[Chapter 28. CD-ROM](#)

[Index](#)