

Contents

| | |
|---|------------|
| Preface | xi |
| I Getting Started | 1 |
| 1 Introduction | 3 |
| 1.1 Why Security? | 3 |
| 1.2 Picking a Security Policy | 4 |
| 1.3 Strategies for a Secure Network | 8 |
| 1.4 The Ethics of Computer Security | 15 |
| 1.5 WARNING | 17 |
| 2 An Overview of TCP/IP | 19 |
| 2.1 The Different Layers | 19 |
| 2.2 Routers and Routing Protocols | 26 |
| 2.3 The Domain Name System | 27 |
| 2.4 Standard Services | 29 |
| 2.5 RPC-based Protocols | 34 |
| 2.6 File Transfer Protocols | 39 |
| 2.7 The “r” Commands | 42 |
| 2.8 Information Services | 44 |
| 2.9 The X11 System | 47 |
| 2.10 Patterns of Trust | 48 |
| II Building Your Own Firewall | 49 |
| 3 Firewall Gateways | 51 |
| 3.1 Firewall Philosophy | 51 |
| 3.2 Situating Firewalls | 53 |
| 3.3 Packet-Filtering Gateways | 54 |
| 3.4 Application-Level Gateways | 75 |
| | vii |

| | | |
|----------|---|------------|
| 3.5 | Circuit-Level Gateways | 76 |
| 3.6 | Supporting Inbound Services | 78 |
| 3.7 | Tunnels Good and Bad | 79 |
| 3.8 | Joint Ventures | 80 |
| 3.9 | What Firewalls Can't Do | 82 |
| 4 | How to Build an Application-Level Gateway | 85 |
| 4.1 | Policy | 85 |
| 4.2 | Hardware Configuration Options | 86 |
| 4.3 | Initial Installation | 89 |
| 4.4 | Gateway Tools | 91 |
| 4.5 | Installing Services | 94 |
| 4.6 | Protecting the Protectors | 109 |
| 4.7 | Gateway Administration | 110 |
| 4.8 | Safety Analysis—Why Our Setup Is Secure and Fail-Safe | 113 |
| 4.9 | Performance | 115 |
| 4.10 | The TIS Firewall Toolkit | 115 |
| 4.11 | Evaluating Firewalls | 116 |
| 4.12 | Living Without a Firewall | 118 |
| 5 | Authentication | 119 |
| 5.1 | User Authentication | 120 |
| 5.2 | Host-to-Host Authentication | 123 |
| 6 | Gateway Tools | 125 |
| 6.1 | Proxylib | 125 |
| 6.2 | Syslog | 127 |
| 6.3 | Watching the Network: Tcpdump and Friends | 128 |
| 6.4 | Adding Logging to Standard Daemons | 130 |
| 7 | Traps, Lures, and Honey Pots | 133 |
| 7.1 | What to Log | 133 |
| 7.2 | Dummy Accounts | 140 |
| 7.3 | Tracing the Connection | 141 |
| 8 | The Hacker's Workbench | 143 |
| 8.1 | Introduction | 143 |
| 8.2 | Discovery | 145 |
| 8.3 | Probing Hosts | 148 |
| 8.4 | Connection Tools | 150 |
| 8.5 | Routing Games | 150 |
| 8.6 | Network Monitors | 152 |
| 8.7 | Metastasis | 152 |
| 8.8 | Tiger Teams | 155 |

| | |
|---|------------|
| 8.9 Further Reading | 156 |
| III A Look Back | 157 |
| 9 Classes of Attacks | 159 |
| 9.1 Stealing Passwords | 159 |
| 9.2 Social Engineering | 160 |
| 9.3 Bugs and Backdoors | 161 |
| 9.4 Authentication Failures | 163 |
| 9.5 Protocol Failures | 164 |
| 9.6 Information Leakage | 165 |
| 9.7 Denial-of-Service | 165 |
| 10 An Evening with Berferd | 167 |
| 10.1 Introduction | 167 |
| 10.2 Unfriendly Acts | 167 |
| 10.3 An Evening with Berferd | 169 |
| 10.4 The Day After | 174 |
| 10.5 The Jail | 175 |
| 10.6 Tracing Berferd | 177 |
| 10.7 Berferd Comes Home | 178 |
| 11 Where the Wild Things Are: A Look at the Logs | 181 |
| 11.1 A Year of Hacking | 183 |
| 11.2 Proxy Use | 189 |
| 11.3 Attack Sources | 190 |
| 11.4 Noise on the Line | 192 |
| IV Odds and Ends | 195 |
| 12 Legal Considerations | 197 |
| 12.1 Computer Crime Statutes | 198 |
| 12.2 Log Files as Evidence | 200 |
| 12.3 Is Monitoring Legal? | 202 |
| 12.4 Tort Liability Considerations | 206 |
| 13 Secure Communications over Insecure Networks | 211 |
| 13.1 An Introduction to Cryptography | 211 |
| 13.2 The Kerberos Authentication System | 223 |
| 13.3 Link-Level Encryption | 226 |
| 13.4 Network- and Transport-Level Encryption | 227 |
| 13.5 Application-Level Encryption | 229 |

| | |
|---|------------|
| 14 Where Do We Go from Here? | 235 |
| A Useful Free Stuff | 239 |
| A.1 Building Firewalls | 240 |
| A.2 Network Management and Monitoring Tools | 243 |
| A.3 Auditing Packages | 244 |
| A.4 Cryptographic Software | 246 |
| A.5 Information Sources | 247 |
| B TCP and UDP Ports | 249 |
| B.1 Fixed Ports | 249 |
| B.2 MBone Usage | 252 |
| C Recommendations to Vendors | 253 |
| C.1 Everyone | 253 |
| C.2 Hosts | 253 |
| C.3 Routers | 254 |
| C.4 Protocols | 254 |
| C.5 Firewalls | 255 |
| Bibliography | 257 |
| List of ●s | 277 |
| Index | 279 |