

Table of Contents

| | |
|--|-----------|
| 1: UNDERSTANDING THE RISKS: AN INTRODUCTION TO INTERNET-ENABLED NETWORKS..... | 1 |
| <i>THE 1988 INTERNET WORM</i> | 2 |
| <i>UNDERSTANDING HOW MULTI-TASKING OPERATING SYSTEMS WORK</i> | 3 |
| <i>THE INTERNET WORM'S EXECUTION</i> | 4 |
| <i>THE INTERNET WORM'S EFFECTS</i> | 5 |
| <i>INCREASING RISKS</i> | 5 |
| <i>UNDERSTANDING THE INTERNET</i> | 8 |
| <i>UNDERSTANDING DOMAINS</i> | 10 |
| <i>PACKET SWITCHING: THE BUILDING BLOCK OF MOST NETWORKS</i> | 12 |
| <i>TRANSMITTING DATA WITH PACKET SWITCHING</i> | 12 |
| <i>THE INTERNET'S FORERUNNER: ARPANET</i> | 14 |
| <i>EXTENDING THE COMMUNICATIONS CAPABILITY OF ARPANET: TCP/IP</i> | 15 |
| <i>INTRODUCING THE WORLD WIDE WEB</i> | 16 |
| <i>THE WEB AS A BUSINESS OPPORTUNITY AND NECESSITY</i> | 18 |
| <i>CONSIDERING THE RISKS</i> | 19 |
| <i>THE DEBATE OVER THE TERM HACKER</i> | 20 |
| <i>THE TYPES OF THREATS: AN OVERVIEW</i> | 21 |
| <i>THE INTERNET'S BUSINESS-SAVVY COUSIN: THE CORPORATE INTRANET</i> | 25 |
| <i>REVISITING THE TYPES OF HACKERS, AND WHERE TO FIND OUT MORE</i> | 26 |
| <i>SECURITY-RELATED MAILING LISTS AND NEWSGROUPS</i> | 27 |
| <i>PUTTING IT ALL TOGETHER</i> | 30 |
| <i>ADDITIONAL INTERNET RESOURCES</i> | 31 |
| 2: UNDERSTANDING NETWORKS & TCP/IP | 33 |
| <i>BASIC NETWORKING AND TCP/IP IN A NUTSHELL</i> | 34 |
| <i>DEFINING THE COMPONENTS OF THE TCP/IP PROTOCOL SUITE</i> | 34 |
| <i>UNDERSTANDING THE ISO/OSI NETWORK MODEL</i> | 35 |
| <i>DEFINING THE PROTOCOL STACK</i> | 36 |
| <i>UNDERSTANDING HOW DATA FLOWS BETWEEN THE LAYERS</i> | 36 |
| <i>EXPLORING TCP/IP'S IMPLEMENTATION OF THE ISO/OSI MODEL</i> | 38 |
| <i>END-TO-END VERSUS HOP-BY-HOP SERVICES</i> | 39 |
| <i>UNDERSTANDING THE PHYSICAL LAYER</i> | 40 |
| <i>UNDERSTANDING THE DATA-LINK LAYER</i> | 40 |
| <i>UNDERSTANDING THE NETWORK LAYER</i> | 41 |
| <i>UNDERSTANDING ENCAPSULATION</i> | 41 |
| <i>UNDERSTANDING THE TRANSPORT LAYER</i> | 42 |
| <i>BYTE-STREAM SERVICE VERSUS DATAGRAM SERVICE</i> | 42 |
| <i>UNDERSTANDING THE APPLICATION LAYER</i> | 43 |
| <i>UNDERSTANDING THE CLIENT-SERVER MODEL</i> | 43 |
| <i>UNDERSTANDING THE TCP/IP ADDRESSING SCHEME</i> | 44 |
| <i>UNDERSTANDING ADDRESS CLASSES</i> | 45 |
| <i>DEFINING THE ADDRESS TYPES</i> | 45 |
| <i>REVISITING OCTETS</i> | 46 |
| <i>UNDERSTANDING THE TRANSPORT CONTROL PROTOCOL</i> | 46 |
| <i>ENSURING RELIABILITY</i> | 47 |
| <i>UNDERSTANDING A SIMPLE ACK HANDSHAKE</i> | 48 |
| <i>UNDERSTANDING A SLIDING WINDOW</i> | 48 |
| <i>DEFINING A TCP MESSAGE</i> | 50 |

| | |
|---|-----------|
| <i>ESTABLISHING A TCP CONNECTION</i> | 51 |
| <i>UNDERSTANDING THE INITIAL SEQUENCE NUMBER</i> | 52 |
| <i>ACKNOWLEDGING DATA TRANSMISSIONS</i> | 53 |
| <i>OFFICIALLY ESTABLISHING A CONNECTION</i> | 53 |
| <i>UNDERSTANDING SEQUENCE NUMBERS</i> | 54 |
| <i>USING FULL-DUPLEX SERVICES</i> | 55 |
| <i>CLOSING A TCP CONNECTION</i> | 55 |
| <i>UNDERSTANDING THE TCP HEADER</i> | 56 |
| <i>SOURCE AND DESTINATION PORT</i> | 56 |
| <i>SEQUENCE NUMBER</i> | 56 |
| <i>ACKNOWLEDGMENT NUMBER</i> | 57 |
| <i>HEADER LENGTH</i> | 57 |
| <i>FLAGS</i> | 57 |
| <i>WINDOW SIZE</i> | 58 |
| <i>TCP CHECKSUM</i> | 58 |
| <i>URGENT POINTER</i> | 58 |
| <i>OPTIONS</i> | 59 |
| <i>MOVING FROM CONCEPT TO DESIGN</i> | 60 |
| <i>UNDERSTANDING NETWORK TOPOLOGIES</i> | 60 |
| <i>THE STAR TOPOLOGY</i> | 60 |
| <i>THE RING TOPOLOGY</i> | 61 |
| <i>THE BUS TOPOLOGY</i> | 61 |
| <i>UNDERSTANDING BUS ARBITRATION</i> | 62 |
| <i>LEARNING MORE ABOUT BUS ARBITRATION</i> | 62 |
| <i>UNDERSTANDING TOKEN PASSING</i> | 63 |
| <i>VARIOUS NETWORK TECHNOLOGIES DEFINED</i> | 63 |
| <i>DEFINING ETHERNET</i> | 63 |
| <i>DEFINING ARCNET</i> | 64 |
| <i>DEFINING IBM TOKEN RING</i> | 64 |
| <i>DEFINING ASYNCHRONOUS TRANSFER MODE NETWORKING</i> | 65 |
| <i>CONNECTING COMPUTER NETWORKS</i> | 65 |
| <i>ATTENUATION AND REPEATERS</i> | 66 |
| <i>ERROR CONTROL AND CHECKSUMS</i> | 66 |
| <i>USING BRIDGES TO IMPROVE NETWORKS</i> | 67 |
| <i>UNDERSTANDING AND USING ROUTERS</i> | 68 |
| <i>UNDERSTANDING AND USING GATEWAYS</i> | 69 |
| <i>THE PHYSICAL STRUCTURE OF NETWORKS</i> | 70 |
| <i>UNDERSTANDING THE DIFFERENT TYPES OF BROADCAST CHANNELS</i> | 71 |
| <i>PUTTING IT ALL TOGETHER</i> | 71 |
| <i>INTERNET RESOURCES RELATED TO THE ISO/OSI MODEL AND TCP/IP</i> | 72 |
| 3: <i>UNDERSTANDING AND USING FIREWALLS</i> | 75 |
| <i>THE DIFFERENT FORMS OF SECURITY</i> | 75 |
| <i>UNDERSTANDING BASTION HOSTS</i> | 76 |
| <i>PROTECTING YOUR NETWORK AGAINST EXTERNAL INTRUSION</i> | 76 |
| <i>UNDERSTANDING SCREENING ROUTERS</i> | 77 |
| <i>PROTECTING AGAINST INTRUSION BETWEEN INTERNAL DEPARTMENTS</i> | 78 |
| <i>INTRODUCING FIREWALL ARCHITECTURE</i> | 79 |
| <i>UNDERSTANDING FIREWALLS</i> | 80 |
| <i>ISOLATING YOUR NETWORK</i> | 80 |
| <i>UNDERSTANDING REGIONS OF RISK</i> | 81 |
| <i>UNDERSTANDING THE FIREWALL'S LIMITATIONS</i> | 82 |
| <i>DESIGNING YOUR FIREWALL</i> | 84 |

| | |
|---|----|
| <i>UNDERSTANDING THE THREE TYPES OF FIREWALLS</i> | 84 |
| <i>NETWORK-LEVEL FIREWALL</i> | 85 |
| <i>APPLICATION-LEVEL FIREWALLS</i> | 86 |
| <i>CIRCUIT-LEVEL FIREWALLS</i> | 88 |
| <i>UNDERSTANDING FIREWALL ARCHITECTURES</i> | 89 |
| <i>UNDERSTANDING DUAL-HOMED HOST FIREWALLS</i> | 89 |
| <i>UNDERSTANDING SCREENED-HOST FIREWALLS</i> | 91 |
| <i>UNDERSTANDING SCREENED-SUBNET FIREWALLS</i> | 91 |
| <i>MINIMUM SECURITY RATINGS</i> | 92 |
| <i>DIVISION D SECURITY RATING</i> | 92 |
| <i>DIVISION C SECURITY RATING</i> | 92 |
| <i>CLASS C1 RATING</i> | 92 |
| <i>CLASS C2 RATING</i> | 93 |
| <i>DIVISION B SECURITY RATINGS</i> | 93 |
| <i>CLASS B1 RATING</i> | 94 |
| <i>CLASS B2 RATING</i> | 94 |
| <i>CLASS B3 RATING</i> | 95 |
| <i>DIVISION A SECURITY RATINGS</i> | 96 |
| <i>CLASS A1 SECURITY</i> | 96 |
| <i>FINDING OUT MORE ABOUT THE ORANGE BOOK RATINGS</i> | 97 |
| <i>PUTTING IT ALL TOGETHER</i> | 98 |
| <i>INTERNET RESOURCES RELATED TO FIREWALLS</i> | 99 |

4: PROTECTING YOUR TRANSMISSIONS WITH ENCRYPTION 101

| | |
|--|-----|
| <i>UNDERSTANDING WHY ENCRYPTION IS IMPORTANT</i> | 102 |
| <i>ENCRYPTION FUNDAMENTALS</i> | 102 |
| <i>THE LIMITATIONS OF CONVENTIONAL SINGLE-KEY CRYPTOSYSTEMS</i> | 103 |
| <i>USING PGP FOR WINDOWS TO ENCRYPT A DOCUMENT</i> | 104 |
| <i>PUBLIC-KEY CRYPTOSYSTEMS</i> | 108 |
| <i>REVISITING PRIVATE AND PUBLIC KEY LOCATIONS</i> | 108 |
| <i>UNDERSTANDING THE RIVEST, SHAMIR, AND ADLEMAN (RSA) ALGORITHM</i> | 109 |
| <i>THE RSA ALGORITHM ITSELF</i> | 110 |
| <i>THE RSA ALGORITHM'S MATH</i> | 111 |
| <i>DOWNLOAD RSA SOFTWARE AND PUBLICATIONS</i> | 112 |
| <i>INTRODUCING DIFFIE AND HELLMAN</i> | 113 |
| <i>UNDERSTANDING THE DIFFIE-HELLMAN ENCRYPTION ALGORITHM</i> | 113 |
| <i>RSA VERSUS DIFFIE-HELLMAN</i> | 114 |
| <i>MESSAGE AUTHENTICATION AS PART OF THE PUBLIC-KEY PROTOCOL</i> | 114 |
| <i>SECURE IS ONLY SO SECURE</i> | 115 |
| <i>HOW TO MANAGE PUBLIC-KEY ENCRYPTION EFFICIENTLY</i> | 116 |
| <i>KEY CERTIFICATES AND KEY RINGS</i> | 117 |
| <i>UNDERSTANDING MESSAGE DIGEST ALGORITHMS</i> | 118 |
| <i>DOWNLOAD UNIX CRYPTOGRAPHIC CHECKSUMS</i> | 119 |
| <i>UNDERSTANDING PRIVACY ENHANCED MAIL (PEM)</i> | 120 |
| <i>ORIGINATOR AUTHENTICATION WITH PEM</i> | 120 |
| <i>MESSAGE CONFIDENTIALITY IN PEM</i> | 120 |
| <i>DATA INTEGRITY IN PEM</i> | 120 |
| <i>DOWNLOAD SOME PEM-STANDARD COMPLIANT SOFTWARE</i> | 121 |
| <i>A BRIEF DISCUSSION OF THE MAJOR CRYPTOGRAPHY PROGRAMS</i> | 121 |
| <i>PRETTY GOOD PRIVACY (PGP)</i> | 121 |
| <i>PGP USES MULTIPLE CRYPTOGRAPHIC METHODS</i> | 122 |
| <i>REVISITING THE PUBLIC-KEY'S CONSTRUCTION</i> | 123 |
| <i>PGP IS IN WIDESPREAD USE</i> | 123 |

| | |
|---|------------|
| <i>LOOKING UP KEYS ON A PUBLIC-KEY RING</i> | 123 |
| <i>DOWNLOAD PGP FREWARE</i> | 124 |
| <i>CRYPT AND ENIGMA</i> | 124 |
| <i>UUENCODE AND SMTP</i> | 125 |
| <i>UNDERSTANDING MICROSOFT'S CRYPTOAPI</i> | 125 |
| <i>USING CRYPTOAPI</i> | 126 |
| <i>TIMING ATTACKS ON CRYPTOGRAPHIC SYSTEMS</i> | 129 |
| <i>THE NEW WAVE IN ENCRYPTION: ELLIPTIC-CURVE CRYPTOGRAPHY (ECC)</i> | 129 |
| <i>ELLIPTIC-CURVE SECURITY</i> | 130 |
| <i>ECC MATHEMATICS IN A NUTSHELL</i> | 131 |
| <i>DETERMINING WHETHER ECC IS BETTER THAN THE CURRENT-DAY SYSTEMS</i> | 131 |
| <i>PUTTING IT ALL TOGETHER</i> | 132 |
| <i>INTERNET RESOURCES FOR DOCUMENT ENCRYPTION AND TRANSMISSION</i> | 133 |
| 5: <i>VERIFYING INFORMATION SOURCES USING DIGITAL SIGNATURES</i> | 135 |
| <i>REVISITING THE DIGITAL SIGNATURE'S CONSTRUCTION</i> | 136 |
| <i>UNDERSTANDING DIGITAL SIGNATURES' IMPORTANCE</i> | 137 |
| <i>USING PGP FOR WINDOWS TO DIGITALLY SIGN A DOCUMENT</i> | 138 |
| <i>DIGITAL SIGNATURES VERSUS ELECTRONIC SIGNATURES</i> | 141 |
| <i>DIGITAL SIGNATURE USES</i> | 141 |
| <i>THE UNITED STATES DIGITAL-SIGNATURE STANDARD (DSS)</i> | 143 |
| <i>CONCERNS ABOUT THE DSS</i> | 143 |
| <i>UNDERSTANDING THE NSA'S ROLE</i> | 144 |
| <i>THE CLIPPER CHIP FIASCO</i> | 144 |
| <i>THE NSA INVOLVEMENT IN THE DEVELOPMENT OF SECURITY STANDARDS</i> | 145 |
| <i>DEVELOPMENTS IN THE DSS</i> | 146 |
| <i>DOWNLOAD A PERL INTERFACE TO THE SHA</i> | 147 |
| <i>DIGITAL SIGNATURES AND PRIVACY ENHANCED MAIL (PEM)</i> | 147 |
| <i>DSS/SHS VALIDATION LISTS FROM NIST</i> | 147 |
| <i>REVISITING THE DIFFIE-HELLMAN ALGORITHM</i> | 148 |
| <i>DOWNLOAD A DEMO VERSION OF HASHCIPHER FOR SHA</i> | 148 |
| <i>UNDERSTANDING THE FUTURE OF DIGITAL SIGNATURES</i> | 149 |
| <i>DIGITALLY SIGNING A FILE ON A UNIX SYSTEM USING PGP</i> | 150 |
| <i>UNDERSTANDING DIGITAL SIGNATURES AND FILE SIGNING</i> | 151 |
| <i>CERTIFICATE AUTHORITIES</i> | 153 |
| <i>SIGNING YOUR SOFTWARE</i> | 154 |
| <i>PUTTING IT ALL TOGETHER</i> | 155 |
| <i>INTERNET RESOURCES RELATED TO DIGITAL SIGNATURES</i> | 155 |
| 6: <i>INTRODUCING HYPERTEXT TRANSPORT PROTOCOL (HTTP)</i> | 157 |
| <i>HTTP IS THE WEB'S NATIVE PROTOCOL</i> | 158 |
| <i>UNDERSTANDING MIME</i> | 158 |
| <i>LOCATING WEB AND INTERNET STANDARDS</i> | 159 |
| <i>USING MIME ON THE WEB</i> | 159 |
| <i>LOOKING AT MIME TYPES AND SUBTYPES</i> | 160 |
| <i>EXAMINING MIME TYPES</i> | 162 |
| <i>LEARNING MORE ABOUT HTTP</i> | 163 |
| <i>HTTP IS STATELESS</i> | 163 |
| <i>BETTER UNDERSTANDING THE EFFICIENCY OF STATELESS COMMUNICATIONS</i> | 164 |
| <i>HTTP SUPPORTS DYNAMIC FORMATS</i> | 165 |
| <i>LOOKING AT HTTP HEADER INFORMATION</i> | 165 |
| <i>HTTP IS HUMAN-READABLE</i> | 165 |
| <i>HTTP IS A GENERIC PROTOCOL</i> | 166 |

| | |
|---|-----|
| <i>HOW HTTP SEEKS, RETRIEVES, AND ANNOTATES</i> | 167 |
| <i>SEEKING A RESOURCE</i> | 167 |
| <i>RETRIEVING A RESOURCE</i> | 167 |
| <i>ANNOTATING A RESOURCE</i> | 167 |
| <i>UNDERSTANDING THE FOUR-STEP HTTP TRANSACTION</i> | 168 |
| <i>STEP 1: ESTABLISH A CONNECTION</i> | 168 |
| <i>STEP 2: CLIENT ISSUES A REQUEST</i> | 169 |
| <i>STEP 3: SERVER ISSUES A RESPONSE</i> | 169 |
| <i>STEP 4: SERVER TERMINATES THE CONNECTION</i> | 170 |
| <i>UNDERSTANDING THE HTTP RESPONSE-CODE CLASSES</i> | 171 |
| <i>A CLOSER LOOK AT URIs</i> | 172 |
| <i>REVIEWING URLs</i> | 172 |
| <i>RELATING URLs, PROTOCOLS, AND FILE TYPES</i> | 173 |
| <i>UNDERSTANDING URL PIECES</i> | 174 |
| <i>LOOKING AT URLs AND HTML</i> | 174 |
| <i>INTRODUCING ABSOLUTE AND RELATIVE URLs</i> | 175 |
| <i>DEFINING ABSOLUTE URLs</i> | 175 |
| <i>DEFINING RELATIVE URLs</i> | 175 |
| <i>GOING FURTHER WITH RELATIVE URLs</i> | 176 |
| <i>DEFINING HTTP METHODS</i> | 177 |
| <i>UNDERSTANDING THE GET METHOD</i> | 178 |
| <i>UNDERSTANDING THE HEAD METHOD</i> | 178 |
| <i>UNDERSTANDING THE POST METHOD</i> | 178 |
| <i>INTRODUCING OTHER HTTP METHODS</i> | 179 |
| <i>UNDERSTANDING GENERAL-HEADER FIELDS</i> | 180 |
| <i>UNDERSTANDING THE HTTP DATE FIELD</i> | 180 |
| <i>UNDERSTANDING THE MIME-VERSION FIELD</i> | 181 |
| <i>UNDERSTANDING THE PRAGMA FIELD</i> | 181 |
| <i>UNDERSTANDING REQUEST-HEADER FIELDS</i> | 181 |
| <i>DEFINING THE ACCEPT FIELD</i> | 182 |
| <i>DEFINING THE AUTHORIZATION FIELD</i> | 182 |
| <i>DEFINING THE FROM FIELD</i> | 183 |
| <i>DEFINING THE IF-MODIFIED-SINCE FIELD</i> | 183 |
| <i>DEFINING THE REFERER FIELD</i> | 183 |
| <i>DEFINING THE USER-AGENT FIELD</i> | 183 |
| <i>DEFINING ENTITY-HEADER FIELDS</i> | 184 |
| <i>UNDERSTANDING THE ALLOW FIELD</i> | 184 |
| <i>UNDERSTANDING THE CONTENT-ENCODING FIELD</i> | 185 |
| <i>UNDERSTANDING THE CONTENT-LENGTH FIELD</i> | 185 |
| <i>UNDERSTANDING THE CONTENT-TYPE FIELD</i> | 185 |
| <i>UNDERSTANDING THE EXPIRES FIELD</i> | 185 |
| <i>UNDERSTANDING THE EXTENSION-HEADER FIELD</i> | 186 |
| <i>UNDERSTANDING THE LAST-MODIFIED FIELD</i> | 186 |
| <i>UNDERSTANDING RESPONSES</i> | 187 |
| <i>UNDERSTANDING HTTP RESPONSE-HEADER FIELDS</i> | 187 |
| <i>UNDERSTANDING THE LOCATION FIELD</i> | 187 |
| <i>HOW THE SERVER FIELD FUNCTIONS</i> | 187 |
| <i>UNDERSTANDING THE WWW-AUTHENTICATE FIELD</i> | 188 |
| <i>DEFINING ENTITY BODIES</i> | 188 |
| <i>UNDERSTANDING WEB DATA COMMUNICATION</i> | 189 |
| <i>LOOKING AT AN HTTP TRANSACTION EXAMPLE</i> | 190 |
| <i>PUTTING IT ALL TOGETHER</i> | 190 |
| <i>INTERNET RESOURCES RELATING TO PROGRAMMING IN HTTP</i> | 190 |

| | | |
|-----------|---|------------|
| 7: | UNDERSTANDING SECURE HYPERTEXT TRANSPORT PROTOCOL (S-HTTP)..... | 193 |
| | INTRODUCING S-HTTP..... | 193 |
| | UNDERSTANDING HOW S-HTTP CREATES MESSAGES..... | 194 |
| | UNDERSTANDING HOW S-HTTP RECOVERS MESSAGES..... | 196 |
| | S-HTTP'S ENCRYPTION METHOD..... | 197 |
| | SSL VERSUS S-HTTP..... | 200 |
| | S-HTTP DETAILS..... | 200 |
| | GETTING S-HTTP..... | 201 |
| | MAJOR ADDITIONS TO HTTP IN S-HTTP'S FEATURES..... | 202 |
| | CRYPTOGRAPHIC ALGORITHM AND DIGITAL SIGNATURE MODES FOR S-HTTP..... | 203 |
| | DIGITAL SIGNATURES AND S-HTTP..... | 203 |
| | KEY EXCHANGE AND ENCRYPTION..... | 203 |
| | MESSAGE INTEGRITY AND SENDER AUTHENTICATION..... | 204 |
| | FRESHNESS OF S-HTTP TRANSACTIONS..... | 205 |
| | HTTP ENCAPSULATION..... | 205 |
| | UNDERSTANDING THE S-HTTP REQUEST LINE..... | 205 |
| | UNDERSTANDING THE S-HTTP RESPONSE LINE..... | 206 |
| | S-HTTP HEADER LINES..... | 206 |
| | S-HTTP'S ACCEPTED CONTENT-TYPES..... | 206 |
| | BREAKING APART THE S-HTTP HEADER: PREARRANGED-KEY-INFO..... | 207 |
| | UNDERSTANDING THE MAC-INFO HEADER..... | 208 |
| | CONTENT OF S-HTTP MESSAGES..... | 208 |
| | S-HTTP AND CONTENT-PRIVACY-DOMAIN: PEM..... | 209 |
| | CORRESPONDENCE BETWEEN PEM AND S-HTTP MODES..... | 209 |
| | NEGOTIATION UNDER S-HTTP..... | 210 |
| | NEGOTIATION HEADER FORMAT..... | 210 |
| | UNDERSTANDING S-HTTP NEGOTIATION HEADERS..... | 211 |
| | KEY PATTERN PARAMETERS..... | 213 |
| | EXAMPLE HEADER BLOCK FOR A TYPICAL S-HTTP SERVER..... | 214 |
| | S-HTTP DEFAULTS..... | 214 |
| | S-HTTP HEADER LINES..... | 215 |
| | CERTIFICATE-INFO HEADER LINE..... | 215 |
| | KEY-ASSIGN HEADER..... | 216 |
| | USING INBAND KEY ASSIGNMENT..... | 216 |
| | USING KERBEROS KEY ASSIGNMENT..... | 217 |
| | USING S-HTTP NONCES..... | 217 |
| | DEALING WITH SERVER STATUS ERROR REPORTS UNDER S-HTTP..... | 217 |
| | SPECIFIC S-HTTP RETRY BEHAVIORS..... | 218 |
| | LIMITATIONS ON AUTOMATIC RETRIES UNDER S-HTTP..... | 218 |
| | AUTOMATIC ENCRYPTION RETRY..... | 218 |
| | THE S-HTTP HTML ELEMENTS..... | 219 |
| | S-HTTP HTML AND URL FORMAT EXTENSIONS..... | 219 |
| | UNDERSTANDING THE CERTS ELEMENT..... | 219 |
| | UNDERSTANDING THE CRYPTOPTS ELEMENT..... | 220 |
| | PUTTING IT ALL TOGETHER..... | 220 |
| | S-HTTP-RELATED INTERNET RESOURCES..... | 220 |
| 8: | USING THE SECURE SOCKET LAYER FOR SECURE INTERNET TRANSMISSIONS..... | 223 |
| | INTRODUCING SECURE SOCKET LAYER 3.0 (SSL)..... | 223 |
| | PRIVACY IN COMMUNICATIONS..... | 224 |
| | UNDERSTANDING HOW SSL PROVIDES TRANSMISSION PROTECTION..... | 225 |
| | SSL USES DIGITAL CERTIFICATES TO VERIFY SERVERS..... | 226 |
| | UNDERSTANDING HOW SSL SECURES TRANSACTIONS END-TO-END..... | 226 |

| | |
|---|------------|
| <i>SSL Uses RSA Encryption</i> | 228 |
| <i>SSL Creates Secure Connections</i> | 228 |
| <i>SSL Browser and Server Particulars</i> | 229 |
| <i>Determining When You Are Transmitting Across a Secure Connection</i> | 229 |
| <i>Verifying Secure Communications Within Navigator and Internet Explorer</i> | 229 |
| <i>Understanding SSL Servers</i> | 231 |
| <i>Download the SSLREF C-Source Code Library</i> | 231 |
| <i>SSLD—The SSL Daemon</i> | 232 |
| <i>The SSLD Configuration File</i> | 233 |
| <i>Closing Notes on SSLD Security</i> | 235 |
| <i>SSL and Firewall Tunnels</i> | 236 |
| <i>SSL Tunneling and the Connect Method</i> | 237 |
| <i>SSL Plus from Consensus Development</i> | 238 |
| <i>SSL Tunneling and Security Considerations</i> | 239 |
| <i>SSL Tunneling and Extensibility</i> | 239 |
| <i>SSLAVA from Phaos Technologies</i> | 240 |
| <i>Understanding S/MIME</i> | 241 |
| <i>Netscape Object Signing</i> | 242 |
| <i>Netscape Security API</i> | 243 |
| <i>Learning More About the SSL Protocol</i> | 244 |
| <i>Putting It All Together</i> | 244 |
| <i>Related Resources on the Internet</i> | 245 |
| 9: Identifying and Defending Against Some Common Hacker Attacks | 247 |
| <i>The Simplest Hacker Attack</i> | 248 |
| <i>Defending Against Sequence-Number Prediction Attacks</i> | 249 |
| <i>Transport Control Protocol (TCP) Hijacking Attack</i> | 250 |
| <i>Sniffer Attacks</i> | 251 |
| <i>The Active Desynchronization Attacks</i> | 252 |
| <i>The Post-Desynchronization Hijacking Attack</i> | 252 |
| <i>TCP ACK Storm</i> | 255 |
| <i>Early Desynchronization Attack</i> | 256 |
| <i>Null Data-Desynchronization Attack</i> | 258 |
| <i>Telnet Session Attack</i> | 258 |
| <i>More on ACK Storms</i> | 259 |
| <i>Detection and Side Effects</i> | 260 |
| <i>Preventing the Post-Desynchronization Hijacking Attack</i> | 261 |
| <i>Another Sniffing Scenario—The Masquerade Attack</i> | 261 |
| <i>All About Spoofing</i> | 262 |
| <i>Spoofing E-Mail</i> | 264 |
| <i>Spoofing E-Mail from Within Your Internet Mail Program</i> | 264 |
| <i>Detecting Spoofing</i> | 265 |
| <i>Using tcpdump and netlog to Defend Against Spoofing</i> | 265 |
| <i>Preventing Spoofing</i> | 266 |
| <i>All About Hijacked Session Attacks</i> | 266 |
| <i>Detecting Hijacked Sessions</i> | 267 |
| <i>Preventing Hijacked Sessions</i> | 267 |
| <i>Hyperlink Spoofing: An Attack on SSL Server Authentication</i> | 267 |
| <i>Hyperlink Spoofing's Background</i> | 268 |
| <i>The Hyperlink Spoofing Attack in Action</i> | 268 |
| <i>Possible Fixes to Prevent Hyperlink Spoofing</i> | 270 |
| <i>The Long Term Fix for Hyperlink Spoofing</i> | 273 |
| <i>Introducing Web-Spoofing</i> | 274 |

| | |
|---|------------|
| WEB-SPOOFING'S CONSEQUENCES | 275 |
| SPOOFING THE WHOLE WEB..... | 276 |
| EXPLAINING HOW THE ATTACK WORKS..... | 276 |
| REVISITING FORMS AND SECURE CONNECTIONS | 277 |
| STARTING THE WEB-SPOOFING ATTACK..... | 278 |
| COMPLETING THE ILLUSION—THE STATUS BAR | 278 |
| THE LOCATION LINE | 279 |
| VIEWING THE DOCUMENT SOURCE..... | 280 |
| VIEWING DOCUMENT INFORMATION..... | 280 |
| TRACING THE HACKER | 280 |
| REMEDIES TO THE WEB-SPOOFING ATTACK..... | 280 |
| LONG-TERM SOLUTIONS TO WEB-SPOOFING | 281 |
| PUTTING IT ALL TOGETHER..... | 281 |
| INTERNET RESOURCES RELATED TO COMMON HACKER ATTACKS | 282 |
| 10: USING KERBEROS KEY EXCHANGE ON DISTRIBUTED SYSTEMS..... | 285 |
| INTRODUCING KERBEROS | 285 |
| UNDERSTANDING DISTRIBUTED SYSTEMS | 286 |
| CONSIDERING KERBEROS FROM A DIFFERENT PERSPECTIVE..... | 289 |
| FREE DOWNLOAD OF KERBEROS, VERSION 5, PATCH LEVEL 1 | 289 |
| KERBEROS EXPORT RESTRICTIONS | 289 |
| REVISITING THE KERBEROS AUTHENTICATION PROCESS..... | 290 |
| THE KERBEROS PROTOCOL | 291 |
| UNDERSTANDING REPLAYS..... | 292 |
| KERBEROS CROSS-REALM OPERATION | 293 |
| UNDERSTANDING INTER-REALM KEYS | 293 |
| UNDERSTANDING AUTHENTICATION PATHS..... | 294 |
| KERBEROS WITH NO TEETH | 296 |
| TICKET FLAG USES AND REQUESTS | 296 |
| INITIAL TICKETS | 297 |
| PRE-AUTHENTICATED TICKETS..... | 297 |
| INVALID TICKETS | 297 |
| RENEWABLE TICKETS | 297 |
| POSTDATED TICKETS | 298 |
| PROXIABLE AND PROXY TICKETS..... | 299 |
| FORWARDABLE TICKETS..... | 300 |
| OTHER AUTHENTICATION SERVER OPTIONS..... | 301 |
| THE KERBEROS DATABASE | 301 |
| DATABASE CONTENTS | 301 |
| ADDITIONAL DATABASE FIELDS | 302 |
| FREQUENTLY CHANGING DATABASE FIELDS..... | 303 |
| REALM NAMES..... | 303 |
| PRINCIPAL NAMES | 304 |
| KERBEROS' KNOWN SUSCEPTIBILITIES | 305 |
| NECESSARY ASSUMPTIONS KERBEROS MAKES | 306 |
| KERBEROS VERSIONS 4 AND 5 COMPATIBILITY | 307 |
| KERBEROS MAILING LISTS..... | 307 |
| PUTTING IT ALL TOGETHER..... | 308 |
| WEB RESOURCES RELATED TO KERBEROS | 308 |
| 11: PROTECTING YOURSELF DURING THE COMMISSION OF INTERNET COMMERCE | 311 |
| REVISITING INTERNET COMMERCE'S BASIC ISSUES..... | 311 |
| INTRODUCING DIGITAL CASH | 313 |
| LEARNING MORE ABOUT CYBERCASH | 314 |

| | |
|---|------------|
| <i>UNDERSTANDING HOW DIGITAL CASH PROVIDES TRANSACTION PRIVACY</i> | 314 |
| <i>UNDERSTANDING DIGITAL CASH SECURITY</i> | 316 |
| <i>PROBLEMS WITH DIGITAL CASH</i> | 317 |
| <i>BETTER UNDERSTANDING THE LOGIC BEHIND "BLIND" SIGNATURES</i> | 318 |
| <i>THE MOST COMMON DIGITAL CASH—ECASH</i> | 320 |
| <i>UNDERSTANDING CREDIT CARD USAGE AND THE INTERNET</i> | 320 |
| <i>VERIFYING SECURE COMMUNICATIONS WITHIN NAVIGATOR AND INTERNET EXPLORER</i> | 321 |
| <i>VIEWING CERTIFICATES</i> | 323 |
| <i>FIRST VIRTUAL'S SOLUTION TO CREDIT CARD SECURITY</i> | 324 |
| <i>PUTTING IT ALL TOGETHER</i> | 324 |
| <i>INTERNET RESOURCES RELATED TO INTERNET COMMERCE</i> | 325 |
| 12: USING AUDIT TRAILS TO TRACK AND REPEL INTRUDERS | 327 |
| <i>SIMPLIFYING THE AUDIT TRAIL</i> | 328 |
| <i>ENABLING AUDIT TRAILS</i> | 329 |
| <i>PROBLEMS WITH AUDITING</i> | 329 |
| <i>AUDIT TRAIL TOOLS ONLINE</i> | 329 |
| <i>AUDIT TRAILS AND UNIX</i> | 330 |
| <i>CHECKING A USER'S LAST ACCESS WITH LASTLOG</i> | 330 |
| <i>STALKER AUDIT-TRAIL TOOL</i> | 331 |
| <i>TRACKING CURRENTLY LOGGED IN USERS WITH UTMP</i> | 331 |
| <i>MORE INTRUSION DETECTION SOFTWARE</i> | 332 |
| <i>TRACKING WHO LOGGED IN PREVIOUSLY WITH WTMP</i> | 332 |
| <i>USING THE SYSLOG LOG</i> | 333 |
| <i>DOWNLOAD WATCHDOG FOR SUNOS AUDIT TRAILS</i> | 335 |
| <i>TRACKING USER SWITCHES WITH SULOG</i> | 336 |
| <i>TRACKING DIAL-OUT ACCESS WITH ACULOG</i> | 336 |
| <i>RECORDING TIME-SPECIFIED TRANSACTIONS</i> | 337 |
| <i>USING SENDMAIL LOGS TO TRACK SMTP INTRUDERS</i> | 337 |
| <i>THE SHELL HISTORY LOG</i> | 338 |
| <i>WINDOWS NT AUDITING</i> | 338 |
| <i>ACTIVATING NT SECURITY LOGGING</i> | 339 |
| <i>AUDITING BASE OBJECTS WITH NT</i> | 341 |
| <i>BASE OBJECT AUDITING</i> | 341 |
| <i>PRIVILEGE AUDITING WITH NT</i> | 343 |
| <i>SHUTDOWN OPTION ON FULL AUDIT LOG WITH WINDOWS NT</i> | 345 |
| <i>NOVELL NETWARE AUDITING</i> | 346 |
| <i>HOW NETWARE DEFINES AUDITING SERVICES</i> | 346 |
| <i>TURN ON NETWARE AUDITING</i> | 347 |
| <i>VIEW AUDIT RECORDS</i> | 347 |
| <i>ENABLING AN AUDITOR WITHIN NOVELL NETWARE</i> | 348 |
| <i>ENABLING AUDITING FOR A VOLUME</i> | 349 |
| <i>ENABLING AUDITING FOR AN NDS CONTAINER</i> | 350 |
| <i>NON-ENGLISH LANGUAGE AUDIT-TRAIL TOOLS</i> | 351 |
| <i>PUTTING IT ALL TOGETHER</i> | 352 |
| <i>ADDITIONAL INTERNET RESOURCES RELATED TO AUDIT TRAILS</i> | 353 |
| 13: SECURITY ISSUES SURROUNDING THE JAVA PROGRAMMING LANGUAGE | 355 |
| <i>UNDERSTANDING JAVA</i> | 356 |
| <i>BETTER UNDERSTANDING BYTECODE</i> | 356 |
| <i>DOWNLOADING JAVA</i> | 359 |
| <i>UNDERSTANDING HOW JAVA EXECUTES FROM WITHIN THE BROWSER</i> | 359 |
| <i>JAVA COMPONENTS</i> | 360 |
| <i>THE APPLLET-CLASS LOADER</i> | 360 |

| | |
|--|------------|
| <i>MORE ON NAME-SPACES</i> | 361 |
| <i>THE APPLET VERIFIER</i> | 362 |
| <i>VERIFIER IMPLEMENTATION BUG</i> | 362 |
| <i>THE APPLET SECURITY MANAGER</i> | 363 |
| <i>BASIC JAVA APPLET SECURITY PROBLEMS</i> | 363 |
| <i>UNDERSTANDING JAVA SECURITY</i> | 364 |
| <i>UNDERSTANDING JAVA FUNDAMENTALS</i> | 365 |
| <i>LIMITATIONS ON JAVA APPLET FUNCTIONALITY</i> | 365 |
| <i>READING OR WRITING FILES WITH APPLETS</i> | 366 |
| <i>EDITING THE ACCESS-CONTROL LIST TO READ FILES</i> | 366 |
| <i>THE HOTJAVA BROWSER</i> | 367 |
| <i>EDITING THE ACCESS-CONTROL LIST TO WRITE FILES</i> | 368 |
| <i>READING SYSTEM PROPERTIES WITHIN AN APPLET</i> | 368 |
| <i>HIDING SYSTEM PROPERTIES</i> | 369 |
| <i>DISPLAYING PROTECTED SYSTEM PROPERTIES</i> | 370 |
| <i>OPENING A CONNECTION TO ANOTHER COMPUTER WITHIN AN APPLET</i> | 370 |
| <i>OPENING A NETWORK CONNECTION TO AN APPLET'S ORIGINATING HOST</i> | 371 |
| <i>MAINTAINING PERSISTENT APPLETS</i> | 372 |
| <i>SPAWNING PROGRAMS FROM THE APPLET</i> | 372 |
| <i>RUDIMENTARY PRECAUTIONS AGAINST JAVA-ATTACKS</i> | 373 |
| <i>BUILDING SECURE APPLETS WITH JAVA</i> | 374 |
| <i>UNDERSTANDING THE DIFFERENCE APPLET ORIGIN MAKES</i> | 376 |
| <i>CREATING A JAVA TRUSTED COMPUTING BASE</i> | 377 |
| <i>KIMERA JAVA SECURITY PROJECT</i> | 377 |
| <i>USING THE KIMERA DISASSEMBLER AND BYTECODE VERIFIER TO TEST CLASSES</i> | 378 |
| <i>REVIEWING SOME MALICIOUS APPLETS</i> | 379 |
| <i>THE JIGSAW SERVER</i> | 381 |
| <i>PUTTING IT ALL TOGETHER</i> | 381 |
| <i>ADDITIONAL INTERNET RESOURCES RELATED TO JAVA SECURITY</i> | 382 |
| 14: INOCULATING YOUR SYSTEM AGAINST VIRUSES | 385 |
| <i>UNDERSTANDING HOW A VIRUS WORKS</i> | 385 |
| <i>COMMON VIRUS SYMPTOMS</i> | 387 |
| <i>DETERMINING THE RISK AND NUMBER OF COMPUTER VIRUSES</i> | 388 |
| <i>MOST COMMON INFECTION RISKS</i> | 389 |
| <i>THE THREAT OF VIRUS TRANSMISSION VIA E-MAIL</i> | 390 |
| <i>CREATING A VIRUS FOR AN EXECUTABLE FILE</i> | 390 |
| <i>UNDERSTANDING THE DIFFERENT TYPES OF VIRUSES</i> | 391 |
| <i>TROJAN HORSES</i> | 391 |
| <i>POLYMORPHIC VIRUSES</i> | 392 |
| <i>STEALTH VIRUSES</i> | 393 |
| <i>SLOW VIRUSES</i> | 394 |
| <i>RETRO VIRUSES</i> | 395 |
| <i>MULTIPARTITE VIRUSES</i> | 396 |
| <i>ARMORED VIRUSES</i> | 396 |
| <i>COMPANION VIRUSES</i> | 396 |
| <i>PHAGE VIRUSES</i> | 396 |
| <i>REVISITING WORMS</i> | 397 |
| <i>VIRUS THREATS SPECIFIC TO NETWORKS AND THE INTERNET</i> | 397 |
| <i>ABOUT FILE VIRUSES</i> | 398 |
| <i>ABOUT MACRO VIRUSES</i> | 400 |
| <i>A SAMPLE MACRO VIRUS</i> | 401 |
| <i>SOME PREVALENT MACRO VIRUSES</i> | 402 |

| | |
|---|------------|
| <i>THE BEST SOLUTIONS FOR MACRO VIRUSES</i> | 406 |
| <i>VIRUS HOAXES ON THE INTERNET</i> | 407 |
| <i>THE IRINA VIRUS</i> | 407 |
| <i>THE GOOD TIMES VIRUS</i> | 407 |
| <i>AOL4FREE.COM: THE HOAX THAT IS NO LONGER A HOAX</i> | 408 |
| <i>HOW TO IDENTIFY A GENUINE VIRUS WARNING</i> | 408 |
| <i>PREVENTING VIRUSES FROM THE INTERNET FROM INFECTING YOUR NETWORK</i> | 409 |
| <i>HOW ANTI-VIRUS SOFTWARE DETECTS A VIRUS</i> | 409 |
| <i>PUBLISHERS OF ANTI-VIRUS SOFTWARE</i> | 409 |
| <i>PUTTING IT ALL TOGETHER</i> | 411 |
| <i>ADDITIONAL WEB RESOURCES RELATED TO VIRUSES</i> | 411 |
| 15: SECURING WINDOWS NT NETWORKS AGAINST ATTACKS | 413 |
| <i>INTRODUCING WINDOWS NT</i> | 413 |
| <i>UNDERSTANDING SHARES</i> | 415 |
| <i>UNDERSTANDING NTFS VULNERABILITIES</i> | 415 |
| <i>UNDERSTANDING THE BASIC WINDOWS NT SECURITY MODEL</i> | 415 |
| <i>REVISITING SECURITY RATINGS</i> | 419 |
| <i>UNDERSTANDING HOW SAM AUTHENTICATES USERS</i> | 420 |
| <i>UNDERSTANDING DOMAINS, AND WORKGROUPS</i> | 421 |
| <i>UNDERSTANDING SERVICE PACKS</i> | 422 |
| <i>UNDERSTANDING MORE ABOUT GROUPS AND PERMISSIONS</i> | 423 |
| <i>UNDERSTANDING NT'S DEFAULT DOMAIN GROUPS</i> | 423 |
| <i>UNDERSTANDING NT'S DEFAULT LOCAL GROUPS</i> | 424 |
| <i>UNDERSTANDING WINDOWS NT'S DEFAULT DIRECTORY PERMISSIONS?</i> | 425 |
| <i>UNDERSTANDING ADMINISTRATORS AND EQUIVALENTS</i> | 425 |
| <i>USING SECURITY ADMINISTRATION IDs</i> | 426 |
| <i>UNDERSTANDING THE ADMINISTRATIVE TOOLS GROUP</i> | 426 |
| <i>SECURE THE ADMINISTRATORS GROUP</i> | 427 |
| <i>UNDERSTANDING HOW NT STORES PASSWORDS</i> | 428 |
| <i>SECURING THE NT SERVER</i> | 429 |
| <i>UNDERSTANDING HOW HACKERS "BREAK" PASSWORDS</i> | 430 |
| <i>USING BRUTE-FORCE ATTACKS WITH WINDOWS NT</i> | 430 |
| <i>DEFENDING WINDOWS NT AGAINST DICTIONARY ATTACKS</i> | 431 |
| <i>ENFORCING BETTER PASSWORDS</i> | 431 |
| <i>WINDOWS NT WITH NO LOCKOUT ENABLED</i> | 431 |
| <i>WINDOWS NT ADMINISTRATOR WITHOUT A PASSWORD</i> | 431 |
| <i>WINDOWS NT ADMINISTRATOR ACCOUNT</i> | 432 |
| <i>WINDOWS NT GUEST ACCOUNT WITHOUT A PASSWORD</i> | 432 |
| <i>PHYSICALLY SECURING THE SERVER</i> | 432 |
| <i>NT AS IT RELATES TO TCP/IP AND HTTP</i> | 433 |
| <i>IIS 4.0 BETA AVAILABLE FOR DOWNLOAD</i> | 434 |
| <i>WINDOWS NT SUPPORTS MULTIPLE SECURITY PROTOCOLS</i> | 434 |
| <i>INTRODUCING SECURE MESSAGE BLOCK SERVICES</i> | 435 |
| <i>UNDERSTANDING SAMBA'S IMPORTANCE</i> | 436 |
| <i>MICROSOFT-KNOWN SAMBA BUG</i> | 436 |
| <i>RECOGNIZING SOME WINDOWS NT VULNERABILITIES</i> | 436 |
| <i>NT ALERTER AND MESSENGER SERVICES</i> | 437 |
| <i>DEFENDING YOUR NETWORK FROM THE ALL ACCESS NETBIOS SHARE</i> | 437 |
| <i>UNDERSTANDING LAN MANAGER SECURITY</i> | 437 |
| <i>WINDOWS NT NETWORK MONITOR</i> | 438 |
| <i>WINDOWS NT RSH SERVICE</i> | 438 |
| <i>WINDOWS NT SCHEDULE SERVICE</i> | 438 |

| | |
|--|------------|
| <i>WINDOWS NT REGISTRY</i> | 439 |
| <i>NT SYSTEMS AND COMPUTER VIRUSES</i> | 439 |
| <i>NT AND THE PING OF DEATH ATTACK</i> | 440 |
| <i>FTP SERVER SECURITY AND NT</i> | 440 |
| <i>ROLLBACK.EXE UTILITY</i> | 441 |
| <i>DOWNLOAD THE NETBIOS AUDITING TOOL</i> | 441 |
| <i>WINDOWS NT REMOTE ACCESS SERVICES (RAS) SECURITY</i> | 441 |
| <i>NT LOGGING AND AUDITING</i> | 444 |
| <i>DOWNLOAD A FREE WORKAROUND FOR WINDOWS NT "ANONYMOUS" VULNERABILITY</i> | 445 |
| <i>SPECIFIC ATTACKS AGAINST A WINDOWS NT SERVER</i> | 445 |
| <i>NETWORK SNIFFING ATTACK</i> | 445 |
| <i>DENIAL OF SERVICE ATTACKS</i> | 446 |
| <i>WINDOWS NT VULNERABILITY TO TCP ATTACKS</i> | 446 |
| <i>SPECIAL NOTE ON AN IMPORTANT BUG FIX FOR NT ADMINISTRATORS AND USERS</i> | 447 |
| <i>PUTTING IT ALL TOGETHER</i> | 447 |
| <i>WEB RESOURCES RELATED TO WINDOWS NT</i> | 447 |
| 16: ADDRESSING NOVELL NETWARE-SPECIFIC SECURITY ISSUES | 449 |
| <i>INTRODUCING NOVELL NETWARE</i> | 450 |
| <i>INTRODUCING NETWARE SECURITY FUNDAMENTALS</i> | 450 |
| <i>ATTACHING USERS AND COMPUTERS TO NETWARE</i> | 451 |
| <i>UNDERSTANDING NETWARE USERS, GROUPS, AND SERVERS</i> | 451 |
| <i>UNDERSTANDING TRUSTEE ASSIGNMENTS</i> | 452 |
| <i>UNDERSTANDING ADMINISTRATORS, SUPERVISORS, AND SUPERVISOR-EQUIVALENTS</i> | 453 |
| <i>UNDERSTANDING THE INHERITED RIGHTS MASK</i> | 453 |
| <i>GRANTING RIGHTS TO APPLICATIONS</i> | 454 |
| <i>UNDERSTANDING TRUSTEE ASSIGNMENT OVERRIDES</i> | 454 |
| <i>PASSWORD CONTROL</i> | 455 |
| <i>UNDERSTANDING HOW NETWARE ENCRYPTS THE PASSWORD</i> | 455 |
| <i>USING THE SYSCON UTILITY</i> | 456 |
| <i>MANAGING PASSWORDS WITH SYSCON</i> | 456 |
| <i>CONTROLLING FILE SERVER ACCESS</i> | 456 |
| <i>HOME DIRECTORY ACCESS</i> | 457 |
| <i>UNDERSTANDING SUPERVISOR IDs AND EQUIVALENTS</i> | 457 |
| <i>USING SECURITY ADMINISTRATION IDs</i> | 458 |
| <i>UNDERSTANDING INTRUDER DETECTION</i> | 458 |
| <i>LOCKING OUT USERS</i> | 459 |
| <i>NETWARE 4.0 STORES PASSWORDS TO A TEMPORARY FILE</i> | 459 |
| <i>UNDERSTANDING LOG-IN SCRIPTS</i> | 460 |
| <i>NETWARE PROVIDES NO AUDIT TRAIL</i> | 460 |
| <i>UNDERSTANDING SECURITY ADMINISTRATION RESPONSIBILITIES</i> | 461 |
| <i>STARTING TO CHECK YOUR INSTALLATION'S SECURITY</i> | 461 |
| <i>THE NETWARE SECURITY PROGRAM</i> | 461 |
| <i>FREWARE FOR AUDITING NETWARE VERSION 4</i> | 462 |
| <i>UNDERSTANDING THE NETWARE FILER PROGRAM</i> | 462 |
| <i>NETWARE SECURITY WEAKNESSES</i> | 463 |
| <i>BASIC DEFENSES: SECURING THE SERVER</i> | 463 |
| <i>PHYSICALLY SECURE THE SERVER</i> | 463 |
| <i>SECURE IMPORTANT FILES OFF-LINE</i> | 464 |
| <i>PROTECTING LOG-IN SCRIPTS</i> | 464 |
| <i>MAKE A LIST OF USERS AND THEIR ACCESSES</i> | 464 |
| <i>MONITOR THE CONSOLE</i> | 465 |

| | |
|---|-----|
| <i>TURN ON ACCOUNTING</i> | 465 |
| <i>DO NOT USE THE SUPERVISOR ACCOUNT</i> | 466 |
| <i>USE PACKET SIGNATURES</i> | 466 |
| <i>UNDERSTANDING PACKET SIGNATURES</i> | 466 |
| <i>UNDERSTANDING HOW HACKERS BYPASS PACKET SIGNATURES</i> | 467 |
| <i>USE RCONSOLE SPARINGLY</i> | 468 |
| <i>CHECK THE NAME AND LOCATION OF RCONSOLE</i> | 468 |
| <i>MOVE ALL NETWARE CONFIGURATION FILES TO A MORE SECURE LOCATION</i> | 468 |
| <i>UPGRADE TO NETWARE 4.X</i> | 469 |
| <i>REMOVE [PUBLIC] FROM [ROOT] IN 4.1's NDS</i> | 469 |
| <i>ACCESSING NETWARE ACCOUNTS</i> | 469 |
| <i>NETWARE DEFAULT AND SYSTEM ACCOUNTS</i> | 469 |
| <i>DEFENDING ACCOUNT NAMES</i> | 470 |
| <i>LOW-LEVEL SYSTEM RESET TECHNIQUE</i> | 470 |
| <i>HACKING AND DEFENDING PASSWORDS</i> | 471 |
| <i>HOW HACKERS CRACK NOVELL PASSWORDS</i> | 472 |
| <i>USING BRUTE FORCE ATTACKS WITH NETWARE</i> | 473 |
| <i>DEFENDING NETWARE AGAINST DICTIONARY ATTACKS</i> | 473 |
| <i>ANOTHER REASON TO PHYSICALLY SECURE THE CONSOLE</i> | 473 |
| <i>ACCOUNTING AND ACCOUNT SECURITY</i> | 474 |
| <i>DEFEATING ACCOUNTING</i> | 474 |
| <i>GETTING ACCOUNTING REPORTS</i> | 474 |
| <i>LIMITING HACKERS WITH STATION AND TIME RESTRICTIONS</i> | 474 |
| <i>DEFENDING THE CONSOLE</i> | 475 |
| <i>HOW THE HACKER DEFEATS CONSOLE LOGGING</i> | 475 |
| <i>HOW HACKERS GET AROUND A LOCKED MONITOR</i> | 475 |
| <i>DEFENDING FILES AND DIRECTORIES</i> | 476 |
| <i>HOW HACKERS HIDE THEIR PRESENCE AFTER ALTERING FILES</i> | 476 |
| <i>UNDERSTANDING NETWARE-AWARE TROJANS</i> | 476 |
| <i>UNDERSTANDING NETWARE'S NFS AND ITS SECURITY</i> | 477 |
| <i>USING THE COMMAND-LINE TO DETERMINE YOUR RIGHTS</i> | 478 |
| <i>PROTECTING DISK SPACE REQUIREMENTS</i> | 479 |
| <i>UNDERSTANDING SOME SECURITY CONSIDERATIONS ACROSS LARGER INSTALLATIONS</i> | 479 |
| <i>WHY NETWARE UTILITIES DO NOT HAVE HOLES AS DO UNIX UTILITIES</i> | 480 |
| <i>NETWARE AND WINDOWS 95</i> | 481 |
| <i>BASIC PROBLEMS WITH RUNNING WINDOWS 95 OVER NETWARE</i> | 481 |
| <i>ONGOING WINDOWS 95 AND NETWARE PROBLEMS</i> | 482 |
| <i>INTERACTION BETWEEN WINDOWS 95 AND NETWARE PASSWORDS</i> | 482 |
| <i>WINDOWS 95 LOG-IN BYPASSES NETWARE SECURITY</i> | 482 |
| <i>NOVELL INTRANETWARE FOR NETWARE</i> | 483 |
| <i>USING INTRANETWARE TO CONTROL ACCESS BY TIME OF DAY</i> | 483 |
| <i>USING INTRANETWARE TO CONTROL ACCESS BY APPLICATION</i> | 484 |
| <i>CONTROLLING ACCESS BY SOURCE AND DESTINATION IP ADDRESSES</i> | 484 |
| <i>INTRANETWARE TOOLS FOR ACCESS REPORTING AND AUDIT TRAILS</i> | 484 |
| <i>INTRANETWARE SECURITY</i> | 485 |
| <i>HOW HACKERS CAN COMPROMISE INTRANETWARE</i> | 485 |
| <i>BUGS IN INTRANETWARE FTP NLM</i> | 485 |
| <i>DEFENDING INTRANETWARE SERVERS FROM INTERNET COMPROMISE</i> | 486 |
| <i>DEFENDING THE PASSWORD FILE</i> | 487 |
| <i>PUTTING IT ALL TOGETHER</i> | 487 |
| <i>ADDITIONAL INTERNET RESOURCES RELATED TO NOVELL NETWARE</i> | 488 |

| | |
|---|------------|
| 17: UNIX AND X-WINDOWS SECURITY | 491 |
| INTRODUCING UNIX | 491 |
| UNDERSTANDING UNIX ACCOUNTS | 492 |
| UNDERSTANDING THE USERNAME'S FORMAT | 493 |
| UNDERSTANDING UNIX PASSWORDS | 493 |
| UNDERSTANDING UNIX SPECIAL CHARACTERS | 494 |
| UNDERSTANDING THE UNIX SHELL | 495 |
| UNDERSTANDING THE UNIX FILE AND DIRECTORY STRUCTURE | 496 |
| INTRODUCING THE BASIC UNIX COMMAND SET | 497 |
| UNDERSTANDING WILDCARDS | 498 |
| UNDERSTANDING THE REDIRECTION CHARACTERS | 498 |
| UNDERSTANDING COMMAND-LINE OPTIONS | 499 |
| INTRODUCING THE PIPE CHARACTER | 499 |
| UNDERSTANDING BACKGROUND PROCESSING | 500 |
| UNDERSTANDING THE PING COMMAND | 500 |
| INTRODUCING THE FINGER COMMAND | 501 |
| BERKELEY -r (REMOTE) COMMANDS | 502 |
| INTRODUCING THE RLOGIN COMMAND | 503 |
| INTRODUCING THE RCP COMMAND | 503 |
| INTRODUCING THE RSH COMMAND | 504 |
| DISABLING -r COMMANDS | 504 |
| UNDERSTANDING THE SWITCH USER (su) COMMAND | 505 |
| DETERMINING WHETHER TO USE THE su COMMAND | 505 |
| UNDERSTANDING DAEMONS | 505 |
| UNDERSTANDING THE INIT DAEMON | 506 |
| UNDERSTANDING THE LPD DAEMON | 506 |
| UNDERSTANDING THE SENDMAIL DAEMON | 506 |
| REVIEWING UNIX THUS FAR | 507 |
| UNDERSTANDING HOW UNIX STORES PASSWORDS | 507 |
| UNDERSTANDING HOW HACKERS "BREAK" PASSWORDS | 508 |
| SHADOW YOUR PASSWORD FILE FOR GREATER PROTECTION | 508 |
| USING BRUTE FORCE ATTACKS WITH UNIX | 509 |
| DEFENDING UNIX AGAINST DICTIONARY ATTACKS | 509 |
| ENFORCING BETTER PASSWORDS | 510 |
| UNDERSTANDING UNIX FILE AND DIRECTORY PROTECTIONS | 510 |
| UNDERSTANDING THE CHMOD COMMAND | 512 |
| UNDERSTANDING THE SPECIAL UNIX FILES | 513 |
| UNDERSTANDING UNIX KNOWN VULNERABILITIES | 514 |
| THE UNIX TOP SEVEN HACKER TARGETS | 515 |
| CONSIDER REMOVING /etc/hosts.equiv | 515 |
| PROTECT AGAINST MULTIPLE COPIES OF \$HOME/.rhosts | 516 |
| UNDERSTANDING THE SENDMAIL DEBUG HOLE | 516 |
| UNDERSTANDING THE SENDMAIL BOUNCE TO PROGRAM HOLE | 517 |
| UNDERSTANDING THE FINGERD BUFFER PROBLEM | 517 |
| UNIX FILE ENCRYPTION | 517 |
| SECURE PROGRAMMING METHODS FOR UNIX | 517 |
| UNIX FILTERING | 518 |
| UNDERSTANDING X-WINDOWS | 519 |
| UNDERSTANDING HOW X-WINDOWS WORKS | 519 |
| HOW HACKERS FIND OPEN X DISPLAYS | 520 |
| THE X-WINDOWS LOCALHOST PROBLEM | 521 |
| X-WINDOWS SNOOPING TECHNIQUES - DUMPING WINDOWS | 521 |
| X-WINDOWS SNOOPING TECHNIQUES | 521 |
| UNDERSTANDING THE XTERM SECURE KEYBOARD OPTION | 521 |

| | |
|--|------------|
| <i>PUTTING IT ALL TOGETHER</i> | 522 |
| <i>ADDITIONAL INTERNET RESOURCES RELATED TO UNIX SECURITY</i> | 522 |
| 18: TESTING YOUR SYSTEM'S VULNERABILITIES | 525 |
| <i>INTRODUCING SATAN</i> | 526 |
| <i>INSTALLING SATAN</i> | 527 |
| <i>USING SATAN WITH LINUX SYSTEMS</i> | 527 |
| <i>SATAN ARCHITECTURE OVERVIEW</i> | 528 |
| <i>UNDERSTANDING THE MAGIC COOKIE GENERATOR</i> | 529 |
| <i>UNDERSTANDING THE POLICY ENGINE</i> | 530 |
| <i>BETTER UNDERSTANDING PROXIMITY LEVELS</i> | 530 |
| <i>UNDERSTANDING WHY YOU MUST KEEP SATAN AWAY FROM OTHER NETWORKS</i> | 531 |
| <i>UNDERSTANDING TARGET ACQUISITION</i> | 531 |
| <i>UNDERSTANDING SUBNET SCANS</i> | 531 |
| <i>UNDERSTANDING THE DATA ACQUISITION ENGINE</i> | 531 |
| <i>UNDERSTANDING SCANNING LEVELS</i> | 532 |
| <i>UNDERSTANDING THE INFERENCE ENGINE</i> | 533 |
| <i>REPORT AND ANALYSIS</i> | 534 |
| <i>MULTIPLE SATAN PROCESSES</i> | 534 |
| <i>SCANNING FOR THE FIRST TIME WITH SATAN</i> | 535 |
| <i>ANALYZING SATAN OUTPUT</i> | 535 |
| <i>MORE ON LOOKING AT AND UNDERSTANDING RESULTS</i> | 536 |
| <i>MORE ON VULNERABILITIES</i> | 537 |
| <i>PRINTING REPORTS</i> | 537 |
| <i>MORE ON HOST INFORMATION</i> | 538 |
| <i>RECOGNIZING THE LIMITATIONS OF SATAN'S VULNERABILITY ANALYSIS</i> | 539 |
| <i>ANALYZING NETWARE AND WINDOWS NT NETWORKS</i> | 539 |
| <i>KSA EVALUATION COPY</i> | 540 |
| <i>KSA FOR WINDOWS NT</i> | 541 |
| <i>STARTING THE KSA</i> | 541 |
| <i>SETTING THE SECURITY STANDARD</i> | 542 |
| <i>SETTING THE ACCOUNT RESTRICTIONS</i> | 543 |
| <i>SETTING THE PASSWORD STRENGTH OPTIONS</i> | 543 |
| <i>SETTING THE ACCESS CONTROL OPTIONS</i> | 543 |
| <i>SETTING THE SYSTEM MONITORING OPTIONS</i> | 544 |
| <i>SETTING THE DATA INTEGRITY OPTIONS</i> | 544 |
| <i>SETTING THE DATA CONFIDENTIALITY OPTIONS</i> | 544 |
| <i>STARTING THE ANALYSIS</i> | 545 |
| <i>ANALYZING THE REPORT CARD</i> | 546 |
| <i>VIEWING THE RISK LIST</i> | 546 |
| <i>MISCELLANEOUS OPTIONS</i> | 547 |
| <i>KSA REPORTING</i> | 547 |
| <i>PUTTING IT ALL TOGETHER</i> | 548 |
| <i>INTERNET RESOURCES RELATED TO NETWORK SECURITY ADMINISTRATION</i> | 549 |
| 19: EXPOSING YOURSELF TO THE WORLD: WEB BROWSER SECURITY ISSUES | 551 |
| <i>THE BROWSER: TWO-WAY WINDOW TO THE WEB</i> | 552 |
| <i>TWO PRIMARY BROWSERS</i> | 552 |
| <i>THE PURPOSE OF BUG IDENTIFICATION</i> | 553 |
| <i>THE IMPORTANCE OF VERSION NUMBERS</i> | 553 |
| <i>OBTAINING THE LATEST PATCHES</i> | 553 |
| <i>MICROSOFT INTERNET EXPLORER SECURITY HOLES</i> | 554 |
| <i>INTERNET EXPLORER 3.02</i> | 554 |

| | |
|---|------------|
| <i>UNDERSTANDING LNK FILES</i> | 554 |
| <i>INTERNET EXPLORER 3.01-WPI BUG</i> | 555 |
| <i>MIT BUG</i> | 557 |
| <i>MICROSOFT BUG FIXES</i> | 558 |
| <i>INTERNET EXPLORER'S JAVA REDIRECT SECURITY ISSUE</i> | 559 |
| <i>THE UNDERLYING PROBLEM</i> | 560 |
| <i>UNDERSTANDING ACTIVE X SECURITY ISSUES</i> | 560 |
| <i>WHY ACTIVE X CONTROLS SAVE TO YOUR HARD DRIVE</i> | 561 |
| <i>SPECIFICS OF ACTIVE X SECURITY</i> | 562 |
| <i>ACTIVE X CONTROLS WITHIN NAVIGATOR</i> | 564 |
| <i>THE CHAOS COMPUTER CONTROL</i> | 565 |
| <i>THE EXPLODER CONTROL</i> | 565 |
| <i>INTERNET EXPLORER 4.0 SECURITY HOLES</i> | 566 |
| <i>NETSCAPE NAVIGATOR SECURITY HOLES</i> | 566 |
| <i>BERKELEY BUG</i> | 566 |
| <i>MICROSOFT AND NETSCAPE CONFIRM FLAW IN SECURE TRANSACTIONS</i> | 567 |
| <i>UNDERSTANDING THE COOKIE</i> | 567 |
| <i>USES FOR THE COOKIES.TXT FILE'S CONTENTS</i> | 568 |
| <i>THE ANONYMIZER</i> | 569 |
| <i>LEARNING ABOUT THE COOKIES.TXT FILE'S CONTENTS</i> | 569 |
| <i>EDITING THE COOKIE</i> | 570 |
| <i>PROTECTING AGAINST INDIVIDUAL COOKIES</i> | 570 |
| <i>CUTTING COOKIES</i> | 571 |
| <i>PROTECTING YOUR E-MAIL ADDRESS</i> | 571 |
| <i>TRICKING THE INVASIVE SERVER</i> | 575 |
| <i>PUTTING IT ALL TOGETHER</i> | 575 |
| <i>INTERNET SITES RELATED TO BROWSER SECURITY</i> | 575 |
| 20: DEFENDING YOURSELF FROM HOSTILE SCRIPTS | 577 |
| <i>UNDERSTANDING CGI</i> | 578 |
| <i>CGI SCRIPTS—THE BIG PICTURE</i> | 579 |
| <i>UNDERSTANDING WHY WEB SITES USE CGI</i> | 579 |
| <i>UNDERSTANDING WHERE CGI FITS IN</i> | 581 |
| <i>A SERVER PROGRAM MUST INVOKE A CGI SCRIPT</i> | 582 |
| <i>LOOKING AT THE BIG PICTURE WITH CGI</i> | 582 |
| <i>UNDERSTANDING THE SERVER—CGI SCRIPT RELATIONSHIP</i> | 583 |
| <i>SETTING UP YOUR COMPUTER AS A WEB SERVER</i> | 583 |
| <i>UNDERSTANDING HOW YOU FIND YOUR OWN IP ADDRESS</i> | 584 |
| <i>UNDERSTANDING HOW TO CONTACT YOUR SERVER</i> | 584 |
| <i>UNDERSTANDING A FIXED IP ADDRESS</i> | 586 |
| <i>UNDERSTANDING THE BASIC WEB SERVER—CGI SCRIPT INTERFACE</i> | 586 |
| <i>UNDERSTANDING CGI ENVIRONMENT VARIABLES</i> | 587 |
| <i>UNDERSTANDING THE AUTH_TYPE VARIABLE</i> | 587 |
| <i>UNDERSTANDING THE CONTENT_LENGTH VARIABLE</i> | 587 |
| <i>UNDERSTANDING THE CONTENT_TYPE VARIABLE</i> | 587 |
| <i>UNDERSTANDING THE GATEWAY_INTERFACE VARIABLE</i> | 587 |
| <i>UNDERSTANDING THE PATH_INFO VARIABLE</i> | 588 |
| <i>UNDERSTANDING THE PATH_TRANSLATED VARIABLE</i> | 588 |
| <i>UNDERSTANDING THE QUERY_STRING VARIABLE</i> | 588 |
| <i>UNDERSTANDING THE REMOTE_ADDR VARIABLE</i> | 589 |
| <i>UNDERSTANDING THE REMOTE_HOST VARIABLE</i> | 589 |
| <i>UNDERSTANDING REMOTE_IDENT VARIABLE</i> | 589 |
| <i>UNDERSTANDING THE REMOTE_USER VARIABLE</i> | 589 |

| | |
|---|-----|
| <i>UNDERSTANDING THE REQUEST_METHOD VARIABLE</i> | 589 |
| <i>UNDERSTANDING THE SCRIPT_NAME VARIABLE</i> | 590 |
| <i>UNDERSTANDING THE SERVER_NAME VARIABLE</i> | 590 |
| <i>UNDERSTANDING THE SERVER_SOFTWARE VARIABLE</i> | 590 |
| <i>UNDERSTANDING THE HTTP_ACCEPT VARIABLE</i> | 590 |
| <i>UNDERSTANDING CGI COMMAND-LINE OPTIONS</i> | 590 |
| <i>UNDERSTANDING DIRECT CGI OUTPUT TO A BROWSER</i> | 591 |
| <i>UNDERSTANDING CGI HEADERS</i> | 591 |
| <i>VIEWING YOUR FIRST CGI SCRIPT USING C++</i> | 592 |
| <i>UNDERSTANDING USEFUL LANGUAGES FOR SCRIPT PROGRAMMING</i> | 594 |
| <i>SCRIPTS ARE NOT YOUR ONLY SOLUTION</i> | 594 |
| <i>PERL IS A PROGRAMMING LANGUAGE</i> | 595 |
| <i>UNDERSTANDING THE HISTORY OF PERL</i> | 595 |
| <i>PERL IS AN INTERPRETED PROGRAMMING LANGUAGE</i> | 596 |
| <i>COMPARING PERL TO THE C/C++ PROGRAMMING LANGUAGE</i> | 596 |
| <i>PERL PROVIDES MANY FEATURES</i> | 596 |
| <i>USING PERL AS A DATA FILTER</i> | 597 |
| <i>USING PERL AS A SECURE GATEWAY</i> | 597 |
| <i>USING PERL AS A DATABASE FRONTEND</i> | 598 |
| <i>USING PERL AS A CGI SCRIPTING LANGUAGE</i> | 598 |
| <i>GETTING STARTED WITH PERL</i> | 598 |
| <i>HELLO WORLD IN PERL</i> | 599 |
| <i>INVOKING PERL</i> | 599 |
| <i>UNDERSTANDING PERL STATEMENTS</i> | 600 |
| <i>LOOKING AT SIMPLE AND COMPOUND STATEMENTS</i> | 600 |
| <i>MAKING SCRIPTS EASIER TO READ AND UNDERSTAND</i> | 601 |
| <i>INVOKING EXTERNAL PROGRAMS FROM A PERL SCRIPT</i> | 601 |
| <i>CGI SCRIPT SECURITY ISSUES</i> | 601 |
| <i>RECENTLY-EXPOSED SECURITY HOLES</i> | 602 |
| <i>UNDERSTANDING HOW A BROKEN CGI SCRIPT IMPACTS SECURITY</i> | 602 |
| <i>WEB-SERVER ACCESS LEVELS</i> | 603 |
| <i>EXAMPLES OF CGI SCRIPT SECURITY HOLES</i> | 603 |
| <i>FORKING THE SHELL</i> | 604 |
| <i>BEST SOLUTIONS TO SECURING CGI SCRIPTS</i> | 604 |
| <i>CERT CGI-VULNERABILITY WARNING</i> | 606 |
| <i>CGI SCRIPT VULNERABILITY IMPACT</i> | 606 |
| <i>CGI SCRIPT VULNERABILITY SOLUTION</i> | 606 |
| <i>OVERALL RULES ABOUT PERL SCRIPTS</i> | 607 |
| <i>INTRODUCING JAVASCRIPT SECURITY ISSUES</i> | 608 |
| <i>WHERE JAVASCRIPT FITS IN</i> | 609 |
| <i>USING HTML COMMENTS TO TURN OFF JAVASCRIPT COMMAND DISPLAY</i> | 610 |
| <i>UNDERSTANDING JAVASCRIPT COMMENTS</i> | 611 |
| <i>UNDERSTANDING THE <SCRIPT> ELEMENT</i> | 611 |
| <i>UNDERSTANDING JAVASCRIPT STRINGS</i> | 611 |
| <i>PERFORMING SIMPLE OUTPUT USING JAVASCRIPT</i> | 612 |
| <i>CREATING SIMPLE MESSAGE BOXES</i> | 612 |
| <i>UNDERSTANDING JAVASCRIPT VARIABLES</i> | 613 |
| <i>GETTING USER TEXT INPUT</i> | 614 |
| <i>UNDERSTANDING JAVASCRIPT FUNCTIONS</i> | 615 |
| <i>UNDERSTANDING JAVASCRIPT OBJECTS</i> | 615 |
| <i>CREATING YOUR OWN JAVASCRIPT OBJECTS</i> | 615 |
| <i>UNDERSTANDING JAVASCRIPT EVENTS</i> | 616 |
| <i>USING JAVASCRIPT TO INTERACT WITH FORMS</i> | 617 |

| | |
|--|------------|
| <i>UNDERSTANDING LIVE WIRE</i> | 618 |
| <i>SECURITY RISKS INHERENT IN JAVASCRIPT</i> | 618 |
| <i>MORE SECURITY ISSUES IN RECENT VERSIONS OF NAVIGATOR</i> | 618 |
| <i>BELL LABS' FIX FOR JAVASCRIPT PRIVACY PROBLEM NOW AVAILABLE</i> | 619 |
| <i>EXPLAINING THE PROBLEM BELL LABS DISCOVERED</i> | 619 |
| <i>PUTTING IT ALL TOGETHER</i> | 619 |
| <i>INTERNET RESOURCES RELATING TO SCRIPTS</i> | 620 |
| 21: PUTTING IT ALL TOGETHER: CREATING A NETWORK-SECURITY POLICY | 623 |
| <i>UNDERSTANDING SECURITY POLICIES</i> | 623 |
| <i>DETERMINE WHY YOU NEED A SECURITY POLICY</i> | 625 |
| <i>THE BASIC APPROACH TO DEVELOPING A SECURITY POLICY</i> | 625 |
| <i>ESTABLISHING AN OFFICIAL POLICY ON COMPUTER SECURITY</i> | 626 |
| <i>DETERMINE RESPONSIBILITY FOR THE POLICY'S CREATION</i> | 627 |
| <i>IMPLEMENTATION RESPONSIBILITIES</i> | 627 |
| <i>RISK ASSESSMENT</i> | 628 |
| <i>IDENTIFYING YOUR SYSTEM'S ASSETS</i> | 628 |
| <i>IDENTIFYING THE THREATS</i> | 630 |
| <i>SPECIFICS ABOUT THE POLICY</i> | 630 |
| <i>DETERMINE WHO CAN USE EACH RESOURCE</i> | 631 |
| <i>DETERMINE THE PROPER USE OF EACH RESOURCE</i> | 631 |
| <i>DETERMINE WHO IS AUTHORIZED TO GRANT ACCESS AND APPROVE USE</i> | 633 |
| <i>DETERMINE WHO SHOULD AND WILL HAVE SYSTEM ADMINISTRATION PRIVILEGES</i> | 634 |
| <i>DETERMINE THE USER'S RIGHTS AND RESPONSIBILITIES</i> | 634 |
| <i>DETERMINE SYSTEM ADMINISTRATOR AND USER RIGHTS AND RESPONSIBILITIES</i> | 635 |
| <i>SECURING AND PROTECTING SENSITIVE AND NORMAL INFORMATION</i> | 635 |
| <i>RESPONDING WHEN SOMEONE VIOLATES THE POLICY</i> | 636 |
| <i>DETERMINE THE RESPONSE TO POLICY VIOLATIONS</i> | 636 |
| <i>YOUR RESPONSE WHEN LOCAL USERS VIOLATE THE POLICY OF A REMOTE SITE</i> | 636 |
| <i>DEFINING CONTACTS AND RESPONSIBILITIES TO OUTSIDE ORGANIZATIONS</i> | 637 |
| <i>ISSUES FOR INCIDENT HANDLING PROCEDURES</i> | 637 |
| <i>LOCKING IN OR OUT</i> | 637 |
| <i>INTERPRETING THE POLICY</i> | 639 |
| <i>PUBLICIZING THE POLICY</i> | 639 |
| <i>ESTABLISHING PROCEDURES TO PREVENT SECURITY PROBLEMS</i> | 640 |
| <i>IDENTIFYING POSSIBLE PROBLEMS</i> | 640 |
| <i>CHOOSE CONTROLS TO PROTECT ASSETS IN A COST-EFFECTIVE WAY</i> | 641 |
| <i>THE SITE SECURITY HANDBOOK</i> | 642 |
| <i>PUTTING IT ALL TOGETHER</i> | 643 |
| <i>INTERNET RESOURCES RELATED TO SECURITY POLICIES</i> | 643 |
| INDEX | 645 |

