Table of Contents

Introduction 1

Part I - Securing Local Networks 3

1 Dealing with Local Network Security in the Real World 15

1.1 Introduction 15

1.2 Security Challenges 18

1.2.1 Hijacking and Espionage of Computer Networks 18

1.2.2 Monster DDOS Attacks 19

1.2.3 IT Consumerization and the Loss of Visibility 20

1.2.4 Issue of Password Fault 20

1.3 References 21

2 Networking Basics in Detail 24
2.1 Basics of Networking 24
2.2 Network Nodes 25
2.2.1 Switches 25
2.2.2 Network Interfaces 28
2.2.3 Repeaters and Hubs 28
2.2.4 Bridges 30
2.2.5 Routers 32
2.2.6 Modems 33
2.2.7 Firewalls 34
2.2.8 Access Points 34
2.3 Campus Area Networks or Corporate Area Networks (CANs) 35
2.4 Metropolitan Area Network(MAN) 37
2.5 Wireless Local Area Network (WLANs) 40
2.6 Storage Area Network (SANs) 40
2.7 The OSI Model in Detail 42
2.7.1 Hardware Layers 43
2.7.2 Software Layers 49
2.8 Data Transmission Packets 51
2.8.1 Ethernet Packet Format and Routing 52
2.8.2 Addressing of Devices 53
2.9 Packet Switched Network 55
2.10 Network Topologies 58
2.10.1 Bus Topology 60
2.10.2 Ring Topology 62
2.10.3 Star Topology 65
2.10.4 Mesh Topology 67
2.10.5 Logical Topology 70
2.11 References 72
3 Detailed Overview of Network Protocols 76
3.1 Introduction 76
3.2 Fundamentals of Network Protocols 77
3.2.1 Internet Protocols (IP) 77
3.2.2 Wireless Network Protocols 78
3.2.3 Network Routing Protocols 79
3.3 How to implement Network Protocols? 80

3.4 MAC Addresses 81
3.4.1 The Open System Interconnection Model 81
3.4.2 Address Details 83
3.4.3 Usage in Hosts 85
3.5 TCP/IP 86
3.5.1 Network Access Layer 87
3.5.2 Internet Layer 87
3.5.3 Transport Layer 88
3.5.4 Application Layer 88
3.6 Detailed Overview of Ethernet 89
3.6.1 Ethernet 89
3.6.2 Fast Ethernet 89
3.6.3 Gigabit Ethernet 90
3.6.4 10 Gigabit Ethernet 91
3.6.5 Asynchronous Transfer Mode (ATM) 91
3.6.6 Power over Ethernet (PoE) 92
3.6.7 Token Ring 92
3.7 Network Control Strategies 93
3.7.1 About Network Infrastructure Devices 93
3.7.2 Threats to Network Infrastructure Devices 94
3.7.3 How to Improve Security in Network Infrastructure Devices 94
3.7.4 Separate and Segment Networks along with the Functions 95
3.7.5 Separating the Sensitive Information Physically 95
3.7.6 Separating Sensitive Information Virtually 95
3.7.7 Restrict Lateral Communications which are not Necessary 96
3.7.8 Harden Network Devices 96
3.7.9 Provide Secured Access to Infrastructure Devices 97
3.7.10 Perform Out-of-Band Management 98
3.7.11 Validate Authenticity of both Software and Hardware 99
3.8 References 100

4 Detailed Overview of Network Servers 103

4.1 Introduction 103
4.2 Basics of Network Server 104
4.3 Key Components of a Server 105

4.3.1 Processor 105
4.3.2 RAM 105
4.3.3 Power Supply 106
4.3.4 Hard Disk 106
4.4 Server Security 107
4.4.1 SSH Keys 107
4.4.2 Brief About Firewalls 108
4.4.3 Private Networking and VPNs 109
4.4.4 Using PKI (Public Key Infrastructure) as well as SSL/TLS Encryption 109
4.4.5 Service Auditing 110
4.4.6 File Auditing and IDS 110
4.4.7 Isolated Execution Environments 110
4.5 Network Administrator 111
4.6 User Accounts 111
4.7 Network Authentication Options 112
4.7.1 Biometrics 112
4.7.2 Token Authentication 112
4.7.3 Transaction Authentication 113
4.7.4 Multi-factor Authentication 113
4.7.5 Out of band Authentication 114
4.8 Establishing Resource Controls 114
4.9 Vulnerability Scanning 115
4.9.1 Authenticated Scans 115
4.9.2 Unauthenticated Scans 116
4.10 References 116
5 Detailed Overview of Network Connectivity Devices 120
5.1 Overview 120
5.1.1 The Network Interface Card (NIC) 122
5.1.2 Hub 122
5.1.3 Switch 123
5.1.4 Bridge 124
5.1.5 Gateways 124
5.1.6 Router 125
5.1.7 Other Devices 126
5.2 Network Switches 129

5.2.1 Classification 130
5.2.2 Configuration of Switches 130
5.2.3 Roles and Functions 131
5.3 Routers 132
5.3.1 Types of Message Deliver 133
5.3.2 Routing Concepts 134
5.3.3 Adaptive and Non-adaptive Routing 135
5.3.4 Routing Protocols 136
5.4 Gateway 141
5.4.1 Types of Gateways 141
5.5 Network Bridges 143
5.5.1 Types of Bridging 143
5.6 Wireless Network Connectivity 146
5.6.1 Types of Wireless Networks 146
5.7 Vulnerabilities of Network Connectivity Device 153
5.7.1 Vulnerability 153
5.7.2 Vulnerability Assessment 154
5.7.3 Penetration Testing 154
5.8 Network Connectivity Device Attacks 156
5.8.1 Attack on Switches 156
5.8.2 Attacks on Routers 161
5.8.3 Attacks on Wireless Network 163
5.9 Network Connectivity Defense 165
5.10 Network Hardening 169
5.10.1 Resetting Default Account Settings 169
5.10.2 Password Phrasing 169
5.10.3 Shut Unnecessary Ports 170
5.10.4 Remove Rogue Connections 170
5.10.5 Debloating 170
5.10.6 Implementing Security Patches 170
5.10.7 Installing an IDS 170
5.10.8 Setting Up Intrusion Prevention System 171
5.10.9 Backup and Restoration of Data 171
5.10.10 Disabling Cookies 171
5.10.11 Using Virtual Machines 171
5.10.12 Using Anti-malware 172
5.10.13 Installing Firewalls 172
5.11 References 172

6 Network Transmission Media Security 177

6.1 Overview 177
6.2 Essentials of Network Transmission Media 178
6.3 Types of Transmission Media 179
6.4 Media Selection 180
6.4.1 Copper Media 181
6.4.2 Wireless Media 181
6.5 Guided Media or Bound or Wired Transmission Media 182
6.5.1 Twisted Pair Cable 183
6.5.2 Coaxial Cable 185
6.5.3 Optical Fiber Cable 186
6.6 Unguided Media or Unbound or Wireless Transmission Media 188
6.6.1 Radio Waves 189
6.6.2 Microwaves 189
6.6.3 Infrared 190
6.7 Bandwidth 191
6.8 Light Waves 192
6.9 Wireless Communication Technologies 193
6.9.1 Radio Frequency Transmission 193
6.9.2 Infrared Transmission 193
6.9.3 Microwave Transmission 193
6.9.4 Light Wave Transmission 194
6.10 Wireless Signals 195
6.10.1 What are Wireless Signals? 196
6.10.2 Types of Wireless Signals 196
6.11 Transmission Media Vulnerabilities 200
6.11.1 Vulnerabilities (Computing) 200
6.11.2 Causes of Vulnerabilities and Prevention 200
6.12 Security for Various Types of Transmission Media 201
6.12.1 Securing Wireless Network 202
6.12.2 Working of a Wireless Network 202
6.12.3 Types of Attacks Generally Wireless Network Posses 203
6.12.4 Ways to Improve Wireless Security 203
6.13 Technology as a Saving Mode 204
6.14 References 205

Part II - Securing The Perimeter 209

7 Real World Perimeter Security Threats and How to Deal With Them 214

7.1 What is Perimeter Security? 214
7.2 Perimeter Security Fundamentals 215
7.3 The Perimeter 215
7.4 Security Challenges 216
7.5 Security Scenario 1 216
7.6 Security Scenario 2 217
7.7 References 219

8 Understanding the Environment 222

8.1 Essentials of Internet Security 222
8.2 Understanding the Environment 223
8.3 Basic Internet Concepts 223
8.4 How do Hackers Hack your Passwords? 225
8.4.1 How to Enhance your Safety by an Excellent Passcode 226
8.4.2 Understanding Identity Theft 226
8.4.3 What do Identity thieves do? 227
8.4.4 How to Prevent It? 227
8.5 Internet Services 228
8.5.1 Types of Internet Services 228
8.6 Standards & RFCs 230
8.6.1 Standardization Process 230
8.6.2 Proposed Standard 231
8.7 References 232

9 How to Hide the Private Network? 234

9.1 Introduction 234
9.2 History of Private Networks 235
9.2.1 Enterprise Private Network (EPN) 235
9.2.2 Virtual Private Network (VPN) 236
9.3 Evolution of IP Address that Private Networks Use 238
9.3.1 IPv4 238
9.3.2 IPv6 239
9.4 Network Address Translation (NAT) 240

9.4.1 IP Masquerading 240
9.4.2 Advantages of NAT 240
9.4.3 Disadvantages of NAT 240
9.4.4 Types of NAT 241
9.4.5 Network Address Translation in IPv6 243
9.4.6 Problems and Limitations 243
9.5 Port Address Translation (PAT) 243
9.5.1 Difference between NAT and PAT 244
9.6 Port Forwarding or Mapping 245
9.6.1 Applications of Port Forwarding or Mapping 245
9.6.2 Types of Port Forwarding or Mapping 246
9.7 Network Segmentation 249
9.7.1 Improving Security 249
9.7.2 Importance of Network Segmentation 250
9.7.3 Demerits of Network Segmentation 250
9.8 Software Defined Networking (SDN) 251
9.8.1 SDN Control Plane 253
9.8.2 Applications of SDN 254
9.8.3 Disadvantage of SDN 255
9.9 References 255

10 Everything You Should Know About Securing the Perimeter 259

10.1 Understanding the Perimeter 259
10.1.1 Physical Defense at the Perimeter 260
10.1.2 Perimeter Security for Data Centres 261
10.2 Detailed Overview of Firewalls 262
10.2.1 History of Firewalls 262
10.2.2 Categories of Firewall 263
10.2.3 Limitations of Firewalls 264
10.2.4 Firewall Software & Tools 264
10.2.5 Steps of Installing Firewalls 266
10.3 Firewall Considerations 268
10.4 Extranets 270
10.4.1 How does it Work? 271
10.4.2 Difference Between Extranet and Intranet 271
10.4.3 Advantages of Extranet 272
10.4.4 Disadvantages of Extranet 273

10.4.5 History of Extranet 273
10.4.6 How to Use it? 274
10.5 Network Appliances 274
10.5.1 Advantages of Network Appliances 275
10.5.2 Components of Network Perimeter 275
10.6 Network Perimeter Requirements 277
10.6.1 Network Perimeter Guidelines 277
10.7 Proxy Server 278
10.7.1 Uses of Proxy Servers 279
10.7.2 Benefits of Proxy Server 279
10.7.3 How does it Work? 280
10.7.4 Types of Proxy Servers 280
10.7.5 Proxy Hacking 283
10.7.6 Proxy Server Security 284
10.8 Demilitarized Zones (DMZs) 284
10.8.1 Purpose of DMZ 285
10.8.2 Importance of DMZ 285
10.8.3 Services Provided By DMZ 286
10.8.4 Demilitarized Zone Designs 286
10.8.5 DMZ Placement and Function 287
10.8.6 Benefits of Demilitarized Zone 287
10.8.7 Weakness of DMZ 288
10.9 Single Firewall DMZ 288
10.10 Dual Firewall DMZ 291
10.11 Honeypots 293
10.11.1 Mechanism of Honeypots 294
10.11.2 Benefits and Drawbacks of Honeypots 294
10.11.3 Types of Honeypots 295
10.12 References 296

11 How to Protect Moving Data on Internet? 299

11.1 Secure the Moving Data 299
11.2 Confine Cloud Sharing or Elective Exchange Techniques 300
11.3 Distinguish Basic Resources and Vulnerabilities 300
11.3.1 Execute Security Structure for Information 301
11.3.2 Data in Transit and Data in Motion 301
11.4 Authentication 302

11.5 Cryptography 303
11.6 Digital Certificates 304
11.6.1 Who can Issue a Computerized Declaration? 307
11.6.2 Contrast between Computerized Endorsement and Advanced Mark 307
11.7 Hash Tables 307
11.7.1 Basics of Hash Table 307
11.7.2 Hash Work 309
11.8 Cookies 309
11.8.1 What do Web Cookies Do? 309
11.8.2 Data Obtained by Cookies 310
11.9 Captcha 311
11.9.1 Know the Importance of Captcha 311
11.9.2 Instructions to Create CAPTCHA 311
11.9.3 Why CAPTCHA is Important? 312
11.10 Virtual Private Networks (VPN) 312
11.10.1 Remote Access VPN 312
11.10.2 Site-to-site VPN 313
11.10.3 Portable VPN 313
11.10.4 Equipment VPN 313
11.10.5 VPN Apparatus 314
11.10.6 How can it Help? 314
11.11 References 314
12 Utilities and Tools for Securing the Perimeter 317
12.1 Introduction 317
12.2 Using Basic Tools 318
12.3 Ifconfig/Ipconfig 319
12.3.1 Ifconfig 319
12.3.2 Ipconfig 321
12.4 Whois 324
12.5 Nslookup 325
12.6 PING 327
12.7 Traceroute 330
12.8 Telnet 332
12.9 Secure Shell 333
12.10 Monitoring Tools and Software 335
12.10.1 How is Network Threat Visibility Important? 335

12.10.2 Network Security Monitoring Tools into Action 336
12.10.3 New Technologies in the Market 337
12.10.4 The Best Network Security Monitoring Tools Available 337
12.11 Introducing Nagios 338
12.11.1 Nagios Core and Nagios XI 338
12.11.2 Working of Nagios 339
12.11.3 Features 340
12.12 Solarwinds 340
12.12.1 What are the Problems that Solarwinds Help to Resolve? 343
12.12.2 How Templates Help to Simplify Monitoring? 343
12.12.3 Solarwinds Monitoring on Orion Platform 344
12.12.4 Solar Winds Licensing 344
12.13 Wireshark 344
12.13.1 Purpose 345
12.13.2 Features 345
12.13.3 Do not get Confused Wireshark with 347
12.14 SNORT 347
12.14.1 Uses of Snort 347
12.14.2 Third Party Tools interfacing with Snort 348
12.14.3 Business Benefits of Snort 348
12.15 NMap 349
12.16 Nikto 350
12.16.1 How does the Scan on Nikto Work? 351
12.17 OpenVAS 351
12.18 Mestaspolit 353
12.18.1 Metasploit Framework Edition 354
12.18.2 Metasploit Community Edition 354
12.18.3 Metasploit Express 354
12.18.4 Metasploit Pro 354
12.18.5 Armitage 355
12.18.6 Cobalt Strike 355
12.19 The Browser Exploitation Framework (BeEF) 355
12.19.1 User Interface 356
12.19.2 A Communication Server 356
12.20 Other Products 357
12.20.1 Cacti 357

12.20.2 Zabbix 357
12.20.3 Ntop 357
12.20.4 Icinga 358
12.20.5 Spiceworks 358
12.20.6 Observium 359
12.21 References 359

13 Identify Vulnerabilities and How to Defend them 364
13.1 Introduction 364
13.2 Malware Attacks 365
13.2.1 Proactive Solutions 365
13.2.2 How Proactive Malware Defense should be? 366
13.3 Botnets, Malware, & Known vs Unknown Vulnerabilities 367
13.4 Zero-day Vulnerability 368
13.4.1 Example of a Zero-day Attack 370
13.4.2 Few Facts about Zero-day Vulnerabilities 371
13.5 Software Exploit 371
13.5.1 Where do Exploits come from? 372
13.5.2 How do you Recognize Exploits? 372
13.5.3 How do you Fix Exploits? 373
13.5.4 How to Prevent Hackers from using Exploits? 373
13.5.5 Easily Protect yourself from Exploits 373
13.6 SQL Injection 373
13.6.1 How and Why is an SQL Injection Attack Performed 374
13.6.2 How to Prevent an SQL Injection? 375
13.7 Java Vulnerabilities 375
13.7.1 Java-specific Vulnerabilities 376
13.7.2 Top Java Vulnerabilities 376
13.8 Social Engineering Exploits 378
13.8.1 A breif about Social Engineering 378
13.8.2 Lifecycle of Social Engineering Attack 379
13.8.3 Social Engineering Prevention 382
13.9 Phishing Attacks 382
13.9.1 Phishing Attack Examples 383
13.9.2 Phishing Techniques 383
13.9.3 Phishing Protection 384
13.10 Network Threats 385
13.11 Broadcast Storm 386

13.11.1 What does Broadcast Storm mean? 386
13.12 Dictionary Attacks 388
13.12.1 Two Counter-measures against Dictionary Attacks 388
13.13 Freak Exploits 389
13.14 Logjam Exploits 389
13.15 Spams 391
13.16 Session Hijacking Attack 392
13.16.1 Examples 393
13.17 Tarpitting 394
13.17.1 The Tarpit Idea 394
13.17.2 SMTP Tarpit 395
13.18 Denial of Service 396
13.19 Transport Layer Security Vulnerability 397
13.19.1 POODLE 398
13.19.2 Prevention 399
13.20 References 399
Appendix A: Figures 407
Appendix B: Tables & Graphs 415
Tables 415
Graphs 416
Appendix C: Glossary 417
Index 432