

# Contents

|                                                  |           |
|--------------------------------------------------|-----------|
| Preface .....                                    | 33        |
| <b>1 Introduction</b> .....                      | <b>39</b> |
| <b>1.1 Hacking</b> .....                         | <b>39</b> |
| 1.1.1 Hacking Contests, Capture the Flag .....   | 40        |
| 1.1.2 Penetration Test versus Hacking .....      | 41        |
| 1.1.3 Hacking Procedure .....                    | 41        |
| 1.1.4 Hacking Targets .....                      | 44        |
| 1.1.5 Hacking Tools .....                        | 46        |
| <b>1.2 Security</b> .....                        | <b>47</b> |
| 1.2.1 Why Are IT Systems So Insecure? .....      | 48        |
| 1.2.2 Attack Vectors .....                       | 49        |
| 1.2.3 Who Is Your Enemy? .....                   | 53        |
| 1.2.4 Intrusion Detection .....                  | 55        |
| 1.2.5 Forensics .....                            | 55        |
| 1.2.6 Ten Steps to Greater Safety .....          | 56        |
| 1.2.7 Security Is Not Visible .....              | 57        |
| 1.2.8 Security Is Inconvenient .....             | 57        |
| 1.2.9 The Limits of This Book .....              | 58        |
| <b>1.3 Exploits</b> .....                        | <b>58</b> |
| 1.3.1 Zero-Day Exploits .....                    | 60        |
| 1.3.2 The Value of Exploits .....                | 61        |
| 1.3.3 Exploit Types .....                        | 61        |
| 1.3.4 Finding Vulnerabilities and Exploits ..... | 62        |
| 1.3.5 Common Vulnerabilities and Exposures ..... | 62        |
| 1.3.6 Common Vulnerability Scoring System .....  | 62        |
| 1.3.7 Vulnerability and Exploit Databases .....  | 63        |
| 1.3.8 Vulnerability Scanner .....                | 64        |
| 1.3.9 Exploit Collections .....                  | 65        |
| <b>1.4 Authentication and Passwords</b> .....    | <b>65</b> |
| 1.4.1 Password Rules .....                       | 66        |
| 1.4.2 Phishing .....                             | 66        |
| 1.4.3 Storage of Passwords (Hash Codes) .....    | 67        |
| 1.4.4 Alternatives to Passwords .....            | 68        |
| 1.4.5 Fast Identity Online .....                 | 69        |

|            |                                                                    |           |
|------------|--------------------------------------------------------------------|-----------|
| <b>1.5</b> | <b>Security Risk IPv6 .....</b>                                    | <b>70</b> |
| 1.5.1      | Security Complications .....                                       | 71        |
| <b>1.6</b> | <b>Legal Framework .....</b>                                       | <b>72</b> |
| 1.6.1      | Unauthorized Hacking Is Punishable by Law .....                    | 72        |
| 1.6.2      | Negligent Handling of IT Security Is Also a Criminal Offense ..... | 73        |
| 1.6.3      | European General Data Protection Regulation .....                  | 74        |
| 1.6.4      | Critical Infrastructure, Banks .....                               | 74        |
| 1.6.5      | Security Guidelines and Standards .....                            | 75        |
| <b>1.7</b> | <b>Security Organizations and Government Institutions .....</b>    | <b>75</b> |
| <br>       |                                                                    |           |
| <b>2</b>   | <b>Kali Linux .....</b>                                            | <b>77</b> |
| <hr/>      |                                                                    |           |
| <b>2.1</b> | <b>Kali Alternatives .....</b>                                     | <b>77</b> |
| <b>2.2</b> | <b>Trying Out Kali Linux without Installation .....</b>            | <b>78</b> |
| 2.2.1      | Verifying the Download .....                                       | 78        |
| 2.2.2      | Verifying the Signature of the Checksum File .....                 | 79        |
| 2.2.3      | Trying Kali Linux in VirtualBox .....                              | 80        |
| 2.2.4      | Saving Data Permanently .....                                      | 83        |
| 2.2.5      | Forensic Mode .....                                                | 83        |
| <b>2.3</b> | <b>Installing Kali Linux in VirtualBox .....</b>                   | <b>84</b> |
| 2.3.1      | Option 1: Using a Prebuilt VirtualBox Image .....                  | 85        |
| 2.3.2      | Option 2: Installing Kali Linux Yourself .....                     | 85        |
| 2.3.3      | Installation .....                                                 | 85        |
| 2.3.4      | Login and sudo .....                                               | 88        |
| 2.3.5      | Time Zone and Time Display .....                                   | 88        |
| 2.3.6      | Network Connection .....                                           | 88        |
| 2.3.7      | Using Kali Linux via SSH .....                                     | 89        |
| 2.3.8      | Clipboard for Kali Linux and the Host Computer .....               | 91        |
| <b>2.4</b> | <b>Kali Linux and Hyper-V .....</b>                                | <b>91</b> |
| <b>2.5</b> | <b>Kali Linux in the Windows Subsystem for Linux .....</b>         | <b>93</b> |
| 2.5.1      | Kali Linux in Graphic Mode .....                                   | 94        |
| 2.5.2      | WSL1 versus WSL2 .....                                             | 95        |
| 2.5.3      | Practical Experience .....                                         | 96        |
| <b>2.6</b> | <b>Kali Linux on Raspberry Pi .....</b>                            | <b>96</b> |
| <b>2.7</b> | <b>Running Kali Linux on Apple PCs with ARM CPUs .....</b>         | <b>97</b> |
| <b>2.8</b> | <b>Simple Application Examples .....</b>                           | <b>99</b> |
| 2.8.1      | Address Scan on the Local Network .....                            | 100       |

|            |                                                                                  |            |
|------------|----------------------------------------------------------------------------------|------------|
| 2.8.2      | Port Scan of a Server .....                                                      | 101        |
| 2.8.3      | Hacking Metasploitable .....                                                     | 103        |
| <b>2.9</b> | <b>Internal Details of Kali .....</b>                                            | <b>103</b> |
| 2.9.1      | Basic Coverage .....                                                             | 103        |
| 2.9.2      | Package Sources .....                                                            | 104        |
| 2.9.3      | Rolling Release .....                                                            | 104        |
| 2.9.4      | Performing Updates .....                                                         | 104        |
| 2.9.5      | Installing Software .....                                                        | 105        |
| 2.9.6      | Python 2 .....                                                                   | 105        |
| 2.9.7      | Network Services and Firewall .....                                              | 106        |
| 2.9.8      | kali-tweaks .....                                                                | 106        |
| 2.9.9      | Undercover Mode .....                                                            | 107        |
| 2.9.10     | PowerShell .....                                                                 | 107        |
| <b>3</b>   | <b>Setting Up the Learning Environment:<br/>Metasploitable, Juice Shop .....</b> | <b>109</b> |
| <b>3.1</b> | <b>Honeypots .....</b>                                                           | <b>110</b> |
| <b>3.2</b> | <b>Metasploitable 2 .....</b>                                                    | <b>110</b> |
| 3.2.1      | Installation in VirtualBox .....                                                 | 111        |
| 3.2.2      | Network Settings .....                                                           | 111        |
| 3.2.3      | Host-Only Network .....                                                          | 112        |
| 3.2.4      | Using Metasploitable 2 .....                                                     | 113        |
| 3.2.5      | Hacking Metasploitable 2 .....                                                   | 114        |
| 3.2.6      | rlogin Exploit .....                                                             | 115        |
| <b>3.3</b> | <b>Metasploitable 3 (Ubuntu Variant) .....</b>                                   | <b>116</b> |
| 3.3.1      | Why No Ready-Made Images? .....                                                  | 117        |
| 3.3.2      | Requirements .....                                                               | 117        |
| 3.3.3      | Installation .....                                                               | 118        |
| 3.3.4      | Starting and Stopping Metasploitable 3 .....                                     | 120        |
| 3.3.5      | Administrating Metasploitable 3 .....                                            | 120        |
| 3.3.6      | Network Configuration .....                                                      | 121        |
| 3.3.7      | Hacking Metasploitable 3 .....                                                   | 122        |
| <b>3.4</b> | <b>Metasploitable 3 (Windows Variant) .....</b>                                  | <b>123</b> |
| 3.4.1      | Administrating Metasploitable 3 .....                                            | 124        |
| 3.4.2      | SSH login .....                                                                  | 126        |
| 3.4.3      | Internal Details and Installation Variants .....                                 | 126        |
| 3.4.4      | Overview of Services in Metasploitable 3 (Windows Variant) .....                 | 127        |
| 3.4.5      | Hacking Metasploitable 3 .....                                                   | 129        |

|            |                                            |            |
|------------|--------------------------------------------|------------|
| <b>3.5</b> | <b>Juice Shop .....</b>                    | <b>133</b> |
| 3.5.1      | Installation with Vagrant .....            | 133        |
| 3.5.2      | Installation with Docker .....             | 134        |
| 3.5.3      | Docker in Kali Linux .....                 | 135        |
| 3.5.4      | Hacking Juice Shop .....                   | 135        |
| <br>       |                                            |            |
| <b>4</b>   | <b>Hacking Tools .....</b>                 | <b>137</b> |
| <br>       |                                            |            |
| <b>4.1</b> | <b>nmap .....</b>                          | <b>138</b> |
| 4.1.1      | Syntax .....                               | 138        |
| 4.1.2      | Examples .....                             | 140        |
| 4.1.3      | Variants and Alternatives .....            | 141        |
| <b>4.2</b> | <b>hydra .....</b>                         | <b>142</b> |
| 4.2.1      | Syntax .....                               | 142        |
| 4.2.2      | Password Lists .....                       | 144        |
| 4.2.3      | Examples .....                             | 144        |
| 4.2.4      | Attacks on Web Forms and Login Pages ..... | 145        |
| 4.2.5      | Alternatives .....                         | 146        |
| <b>4.3</b> | <b>sslyze, sslscan, and testssl .....</b>  | <b>148</b> |
| 4.3.1      | sslscan and sslyze .....                   | 148        |
| 4.3.2      | testssl .....                              | 149        |
| 4.3.3      | Online Tests .....                         | 150        |
| <b>4.4</b> | <b>whois, host, and dig .....</b>          | <b>151</b> |
| 4.4.1      | whois .....                                | 152        |
| 4.4.2      | host .....                                 | 152        |
| 4.4.3      | dig .....                                  | 153        |
| 4.4.4      | dnsrecon .....                             | 154        |
| <b>4.5</b> | <b>Wireshark .....</b>                     | <b>154</b> |
| 4.5.1      | Installation .....                         | 155        |
| 4.5.2      | Basic Functions .....                      | 156        |
| 4.5.3      | Working Techniques .....                   | 158        |
| 4.5.4      | Alternatives .....                         | 159        |
| <b>4.6</b> | <b>tcpdump .....</b>                       | <b>159</b> |
| 4.6.1      | Syntax .....                               | 160        |
| 4.6.2      | Examples .....                             | 161        |
| 4.6.3      | ngrep .....                                | 162        |
| <b>4.7</b> | <b>Netcat (nc) .....</b>                   | <b>163</b> |
| 4.7.1      | Syntax .....                               | 163        |

---

|             |                                                                     |            |
|-------------|---------------------------------------------------------------------|------------|
| 4.7.2       | Examples .....                                                      | 163        |
| 4.7.3       | socat .....                                                         | 166        |
| <b>4.8</b>  | <b>OpenVAS .....</b>                                                | <b>166</b> |
| 4.8.1       | Installation .....                                                  | 167        |
| 4.8.2       | Starting and Updating OpenVAS .....                                 | 169        |
| 4.8.3       | Operation .....                                                     | 169        |
| 4.8.4       | Alive Test .....                                                    | 172        |
| 4.8.5       | Setting Up Tasks Yourself .....                                     | 173        |
| 4.8.6       | High Resource Requirements .....                                    | 175        |
| 4.8.7       | Alternatives .....                                                  | 175        |
| <b>4.9</b>  | <b>Metasploit Framework .....</b>                                   | <b>176</b> |
| 4.9.1       | Operation in Kali Linux .....                                       | 177        |
| 4.9.2       | Installation on Linux .....                                         | 177        |
| 4.9.3       | Installation on macOS .....                                         | 178        |
| 4.9.4       | Installation on Windows .....                                       | 179        |
| 4.9.5       | Updates .....                                                       | 180        |
| 4.9.6       | The Metasploit Console (“msfconsole”) .....                         | 180        |
| 4.9.7       | A Typical “msfconsole” Session .....                                | 181        |
| 4.9.8       | Searching Modules .....                                             | 182        |
| 4.9.9       | Applying Modules .....                                              | 183        |
| 4.9.10      | Meterpreter .....                                                   | 185        |
| <b>4.10</b> | <b>Empire Framework .....</b>                                       | <b>187</b> |
| 4.10.1      | Installation .....                                                  | 188        |
| 4.10.2      | Getting to Know and Setting Up Listeners .....                      | 189        |
| 4.10.3      | Selecting and Creating Stagers .....                                | 190        |
| 4.10.4      | Creating and Managing Agents .....                                  | 192        |
| 4.10.5      | Finding the Right Module .....                                      | 193        |
| 4.10.6      | Obtaining Local Administrator Rights with the Empire Framework .... | 195        |
| 4.10.7      | The Empire Framework as a Multiuser System .....                    | 197        |
| 4.10.8      | Alternatives .....                                                  | 197        |
| <b>4.11</b> | <b>The Koadic Postexploitation Framework .....</b>                  | <b>197</b> |
| 4.11.1      | Installing the Server .....                                         | 198        |
| 4.11.2      | Using Helper Tools in the Program .....                             | 199        |
| 4.11.3      | Creating Connections from a Client to the Server .....              | 199        |
| 4.11.4      | Creating a First Connection: Zombie 0 .....                         | 201        |
| 4.11.5      | The Modules of Koadic .....                                         | 202        |
| 4.11.6      | Extending Rights and Reading Password Hashes .....                  | 203        |
| 4.11.7      | Conclusion and Countermeasures .....                                | 205        |
| <b>4.12</b> | <b>Social Engineer Toolkit .....</b>                                | <b>205</b> |
| 4.12.1      | Syntax .....                                                        | 206        |
| 4.12.2      | Example .....                                                       | 206        |

- 4.12.3 The dnstwist Command ..... 210
  - 4.12.4 Other SET Modules ..... 211
  - 4.12.5 Alternatives ..... 212
- 4.13 Burp Suite ..... 212**
  - 4.13.1 Installation and Setup ..... 213
  - 4.13.2 Modules ..... 213
  - 4.13.3 Burp Proxy ..... 214
  - 4.13.4 Burp Scanner ..... 216
  - 4.13.5 Burp Intruder ..... 217
  - 4.13.6 Burp Repeater ..... 218
  - 4.13.7 Burp Extensions ..... 218
  - 4.13.8 Alternatives ..... 219
- 4.14 Sliver ..... 219**
  - 4.14.1 Installation ..... 220
  - 4.14.2 Implants and Listeners ..... 220
  - 4.14.3 Other C2 Frameworks ..... 224

**5**

**Offline Hacking**

227

---

- 5.1 BIOS/EFI: Basic Principles ..... 228**
  - 5.1.1 The Boot Process ..... 228
  - 5.1.2 EFI Settings and Password Protection ..... 229
  - 5.1.3 UEFI Secure Boot ..... 229
  - 5.1.4 When the EFI Is Insurmountable: Remove the Hard Drive ..... 230
- 5.2 Accessing External Systems ..... 230**
  - 5.2.1 Booting the Notebook with Kali Linux ..... 230
  - 5.2.2 Reading the Windows File System ..... 231
  - 5.2.3 Vault Files ..... 233
  - 5.2.4 Write Access to the Windows File System ..... 235
  - 5.2.5 Linux ..... 235
  - 5.2.6 macOS ..... 236
  - 5.2.7 Does That Mean That Login Passwords Are Useless? ..... 236
- 5.3 Accessing External Hard Drives or SSDs ..... 236**
  - 5.3.1 Hard Drives and SSDs Removed from Notebooks ..... 237
- 5.4 Resetting the Windows Password ..... 237**
  - 5.4.1 Tools ..... 238
  - 5.4.2 Undesirable Side Effects ..... 239
  - 5.4.3 Resetting the Local Windows Password Using chntpw ..... 240
  - 5.4.4 Activating a Windows Administrator User via chntpw ..... 242

|            |                                                       |     |
|------------|-------------------------------------------------------|-----|
| <b>5.5</b> | <b>Resetting Linux and macOS Passwords</b>            | 244 |
| 5.5.1      | Resetting a Linux Password                            | 244 |
| 5.5.2      | Resetting a macOS Password                            | 245 |
| <b>5.6</b> | <b>Encrypting Hard Drives</b>                         | 246 |
| 5.6.1      | BitLocker                                             | 246 |
| 5.6.2      | Access to BitLocker File Systems on Linux (dislocker) | 249 |
| 5.6.3      | BitLocker Security                                    | 250 |
| 5.6.4      | BitLocker Alternatives                                | 251 |
| 5.6.5      | macOS: FileVault                                      | 252 |
| 5.6.6      | Linux: Linux Unified Key Setup                        | 253 |
| 5.6.7      | Security Concerns Regarding LUKS                      | 253 |
| 5.6.8      | File System Encryption on the Server                  | 254 |

---

## 6 Passwords 255

---

|            |                                                    |     |
|------------|----------------------------------------------------|-----|
| <b>6.1</b> | <b>Hash Procedures</b>                             | 256 |
| 6.1.1      | Hash Collisions                                    | 257 |
| 6.1.2      | SHA-2 and SHA-3 Hash Codes                         | 258 |
| 6.1.3      | Checksums or Hash Codes for Downloads              | 258 |
| <b>6.2</b> | <b>Brute-Force Password Cracking</b>               | 259 |
| 6.2.1      | Estimating the Time Required for Password Cracking | 259 |
| <b>6.3</b> | <b>Rainbow Tables</b>                              | 260 |
| 6.3.1      | Password Salting                                   | 261 |
| <b>6.4</b> | <b>Dictionary Attacks</b>                          | 262 |
| <b>6.5</b> | <b>Password Tools</b>                              | 263 |
| 6.5.1      | John the Ripper: Offline CPU Cracker               | 264 |
| 6.5.2      | hashcat: Offline GPU Cracker                       | 265 |
| 6.5.3      | Crunch: Password List Generator                    | 268 |
| 6.5.4      | hydra: Online Cracker                              | 269 |
| 6.5.5      | makepasswd: Password Generator                     | 270 |
| 6.5.6      | One-Time Secret: Send Passwords by Email           | 270 |
| <b>6.6</b> | <b>Default Passwords</b>                           | 271 |
| <b>6.7</b> | <b>Data Breaches</b>                               | 272 |
| <b>6.8</b> | <b>Multifactor Authentication</b>                  | 275 |
| <b>6.9</b> | <b>Implementing Secure Password Handling</b>       | 276 |
| 6.9.1      | Implementation Tips                                | 277 |

7

IT Forensics

279

---

|       |                                                |     |
|-------|------------------------------------------------|-----|
| 7.1   | Methodical Analysis of Incidents .....         | 281 |
| 7.1.1 | Digital Traces .....                           | 281 |
| 7.1.2 | Forensic Investigation .....                   | 281 |
| 7.1.3 | Areas of IT Forensics .....                    | 282 |
| 7.1.4 | Analysis of Security Incidents .....           | 284 |
| 7.2   | Postmortem Investigation .....                 | 284 |
| 7.2.1 | Forensic Backup of Memory .....                | 284 |
| 7.2.2 | Recovering Deleted Files by File Carving ..... | 286 |
| 7.2.3 | Metadata and File Analysis .....               | 288 |
| 7.2.4 | System Analyses with Autopsy .....             | 290 |
| 7.2.5 | Basic System Information .....                 | 292 |
| 7.2.6 | Reading the Last Activities .....              | 295 |
| 7.2.7 | Analyzing Web Activities .....                 | 296 |
| 7.2.8 | Tracing Data Exchanges .....                   | 298 |
| 7.3   | Live Analysis .....                            | 300 |
| 7.3.1 | Finding User Data .....                        | 301 |
| 7.3.2 | Called Domains and URLs .....                  | 301 |
| 7.3.3 | Active Network Connections .....               | 302 |
| 7.3.4 | Extracting the TrueCrypt Password .....        | 302 |
| 7.4   | Forensic Readiness .....                       | 303 |
| 7.4.1 | Strategic Preparations .....                   | 303 |
| 7.4.2 | Operational Preparations .....                 | 304 |
| 7.4.3 | Effective Logging .....                        | 304 |
| 7.4.4 | Protection against Tampering .....             | 305 |
| 7.4.5 | Integrity Verification .....                   | 305 |
| 7.4.6 | Digital Signatures .....                       | 305 |
| 7.5   | Summary .....                                  | 305 |

8

Wi-Fi, Bluetooth, and SDR

307

---

|       |                                            |     |
|-------|--------------------------------------------|-----|
| 8.1   | 802.11x Systems: Wi-Fi .....               | 307 |
| 8.1.1 | Preparation and Infrastructure .....       | 308 |
| 8.1.2 | Wireless Equivalent Privacy .....          | 310 |
| 8.1.3 | WPA/WPA-2: Wireless Protected Access ..... | 315 |
| 8.1.4 | Wireless Protected Setup .....             | 317 |
| 8.1.5 | Wi-Fi Default Passwords .....              | 320 |
| 8.1.6 | WPA-2-KRACK Attack .....                   | 321 |

|            |                                                          |            |
|------------|----------------------------------------------------------|------------|
| 8.1.7      | WPA-2 Enterprise .....                                   | 322        |
| 8.1.8      | Wi-Fi Client: Man-in-the-Middle .....                    | 323        |
| 8.1.9      | WPA-3 .....                                              | 325        |
| <b>8.2</b> | <b>Collecting WPA-2 Handshakes with Pwnagotchi .....</b> | <b>325</b> |
| <b>8.3</b> | <b>Bluetooth .....</b>                                   | <b>332</b> |
| 8.3.1      | Bluetooth Technology .....                               | 332        |
| 8.3.2      | Identifying Bluetooth Classic Devices .....              | 334        |
| 8.3.3      | Hiding (and Still Finding) Bluetooth Devices .....       | 339        |
| 8.3.4      | Bluetooth Low Energy (BTLE) .....                        | 343        |
| 8.3.5      | Listening In on Bluetooth Low Energy Communication ..... | 344        |
| 8.3.6      | Identifying Apple Devices via Bluetooth .....            | 346        |
| 8.3.7      | Bluetooth Attacks .....                                  | 347        |
| 8.3.8      | Modern Bluetooth Attacks .....                           | 349        |
| <b>8.4</b> | <b>Software-Defined Radios .....</b>                     | <b>349</b> |
| 8.4.1      | SDR Devices .....                                        | 351        |
| 8.4.2      | Decoding a Wireless Remote Control .....                 | 353        |

## **9 Attack Vector USB Interface** 359

---

|            |                                                                      |            |
|------------|----------------------------------------------------------------------|------------|
| <b>9.1</b> | <b>USB Rubber Ducky .....</b>                                        | <b>360</b> |
| 9.1.1      | Structure and Functionality .....                                    | 360        |
| 9.1.2      | DuckyScript .....                                                    | 360        |
| 9.1.3      | Installing a Backdoor on Windows 11 .....                            | 363        |
| 9.1.4      | Use With Duck Encoder to Create the Finished Payload .....           | 366        |
| <b>9.2</b> | <b>Digispark: A Wolf in Sheep's Clothing .....</b>                   | <b>367</b> |
| 9.2.1      | Downloading and Setting Up the Arduino Development Environment ..... | 368        |
| 9.2.2      | The Script Language of the Digispark .....                           | 370        |
| 9.2.3      | Setting Up a Linux Backdoor with Digispark .....                     | 371        |
| <b>9.3</b> | <b>Bash Bunny .....</b>                                              | <b>375</b> |
| 9.3.1      | Structure and Functionality .....                                    | 375        |
| 9.3.2      | Configuring the Bash Bunny .....                                     | 377        |
| 9.3.3      | Status LED .....                                                     | 378        |
| 9.3.4      | Software Installation .....                                          | 379        |
| 9.3.5      | Connecting to the Bash Bunny .....                                   | 379        |
| 9.3.6      | Connecting the Bash Bunny to the Internet: Linux Host .....          | 381        |
| 9.3.7      | Connecting the Bash Bunny to the Internet: Windows Host .....        | 382        |
| 9.3.8      | Bunny Script: The Scripting Language of the Bash Bunny .....         | 384        |
| 9.3.9      | Using Custom Extensions and Functions .....                          | 386        |

|            |                                                     |            |
|------------|-----------------------------------------------------|------------|
| 9.3.10     | Setting Up a macOS Backdoor with Bash Bunny .....   | 387        |
| 9.3.11     | The payload.txt Files for Switch1 and Switch2 ..... | 390        |
| 9.3.12     | Updating the Bash Bunny .....                       | 394        |
| 9.3.13     | Key Takeaways .....                                 | 395        |
| <b>9.4</b> | <b>P4wnP1: The Universal Talent .....</b>           | <b>396</b> |
| 9.4.1      | Structure and Functionality .....                   | 396        |
| 9.4.2      | Installation and Connectivity .....                 | 397        |
| 9.4.3      | HID Scripts .....                                   | 398        |
| 9.4.4      | CLI Client .....                                    | 399        |
| 9.4.5      | An Attack Scenario with the P4wnP1 .....            | 399        |
| 9.4.6      | Creating a Dictionary .....                         | 400        |
| 9.4.7      | Launching a Brute-Force Attack .....                | 401        |
| 9.4.8      | Setting Up a Trigger Action .....                   | 404        |
| 9.4.9      | Deploying the P4wnP1 on the Target System .....     | 405        |
| 9.4.10     | Key Takeaways .....                                 | 405        |
| <b>9.5</b> | <b>MalDuino W .....</b>                             | <b>406</b> |
| 9.5.1      | The Web Interface of the MalDuino W .....           | 407        |
| 9.5.2      | The Scripting Language and the CLI .....            | 408        |
| 9.5.3      | An Attack Scenario with the MalDuino W .....        | 408        |
| 9.5.4      | How Does the Attack Work? .....                     | 409        |
| 9.5.5      | Key Takeaways .....                                 | 412        |
| <b>9.6</b> | <b>Countermeasures .....</b>                        | <b>412</b> |
| 9.6.1      | Hardware Measures .....                             | 413        |
| 9.6.2      | Software Measures .....                             | 413        |

## **10 External Security Checks** 419

---

|             |                                              |            |
|-------------|----------------------------------------------|------------|
| <b>10.1</b> | <b>Reasons for Professional Checks .....</b> | <b>419</b> |
| <b>10.2</b> | <b>Types of Security Checks .....</b>        | <b>420</b> |
| 10.2.1      | Open-Source Intelligence .....               | 420        |
| 10.2.2      | Vulnerability Scan .....                     | 422        |
| 10.2.3      | Vulnerability Assessment .....               | 424        |
| 10.2.4      | Penetration Test .....                       | 425        |
| 10.2.5      | Red Teaming .....                            | 425        |
| 10.2.6      | Purple Teaming .....                         | 427        |
| 10.2.7      | Bug Bounty Programs .....                    | 428        |
| 10.2.8      | Type of Performance .....                    | 428        |
| 10.2.9      | Depth of Inspection: Attacker Type .....     | 429        |
| 10.2.10     | Prior to the Order .....                     | 430        |

|             |                                           |            |
|-------------|-------------------------------------------|------------|
| <b>10.3</b> | <b>Legal Protection .....</b>             | <b>430</b> |
| <b>10.4</b> | <b>Objectives and Scope .....</b>         | <b>432</b> |
| 10.4.1      | Sample Objective .....                    | 432        |
| 10.4.2      | Sample Worst-Case Scenarios .....         | 433        |
| 10.4.3      | Sample Scope .....                        | 433        |
| <b>10.5</b> | <b>Implementation Methods .....</b>       | <b>433</b> |
| <b>10.6</b> | <b>Reporting .....</b>                    | <b>434</b> |
| <b>10.7</b> | <b>Selecting the Right Provider .....</b> | <b>437</b> |

## **11 Penetration Testing .....** **441**

---

|             |                                                                |            |
|-------------|----------------------------------------------------------------|------------|
| <b>11.1</b> | <b>Gathering Information .....</b>                             | <b>442</b> |
| 11.1.1      | Searching for Information about a Company .....                | 442        |
| 11.1.2      | Using Metadata of Published Files .....                        | 445        |
| 11.1.3      | Identifying the Structure of Email Addresses .....             | 447        |
| 11.1.4      | Database and Password Leaks .....                              | 449        |
| 11.1.5      | Partial Automation with Maltego .....                          | 450        |
| 11.1.6      | Automating Maltego Transforms .....                            | 456        |
| 11.1.7      | Defense .....                                                  | 458        |
| <b>11.2</b> | <b>Initial Access with Code Execution .....</b>                | <b>459</b> |
| 11.2.1      | Checking External IP Addresses of the PTA .....                | 459        |
| <b>11.3</b> | <b>Scanning Targets of Interest .....</b>                      | <b>463</b> |
| 11.3.1      | Gathering Information via DNS .....                            | 463        |
| 11.3.2      | Detecting Active Hosts .....                                   | 465        |
| 11.3.3      | Detecting Active Services with nmap .....                      | 467        |
| 11.3.4      | Using nmap in Combination with Metasploit .....                | 469        |
| <b>11.4</b> | <b>Searching for Known Vulnerabilities Using nmap .....</b>    | <b>470</b> |
| <b>11.5</b> | <b>Exploiting Known Vulnerabilities Using Metasploit .....</b> | <b>472</b> |
| 11.5.1      | Example: GetSimple CMS .....                                   | 474        |
| <b>11.6</b> | <b>Attacking Using Known or Weak Passwords .....</b>           | <b>478</b> |
| <b>11.7</b> | <b>Email Phishing Campaigns for Companies .....</b>            | <b>481</b> |
| 11.7.1      | Organizational Preparatory Measures .....                      | 481        |
| 11.7.2      | Preparing a Phishing Campaign with Gophish .....               | 483        |
| <b>11.8</b> | <b>Phishing Attacks with Office Macros .....</b>               | <b>490</b> |
| <b>11.9</b> | <b>Phishing Attacks with ISO and ZIP Files .....</b>           | <b>494</b> |
| 11.9.1      | Creating an Executable File with Metasploit .....              | 495        |
| 11.9.2      | Creating a File with ScareCrow to Bypass Virus Scanners .....  | 499        |

|              |                                                                           |            |
|--------------|---------------------------------------------------------------------------|------------|
| 11.9.3       | Disguising and Deceiving: From EXE to PDF File .....                      | 502        |
| 11.9.4       | Defense .....                                                             | 503        |
| <b>11.10</b> | <b>Attack Vector USB Phishing .....</b>                                   | <b>504</b> |
| <b>11.11</b> | <b>Network Access Control and 802.1X in Local Networks .....</b>          | <b>506</b> |
| 11.11.1      | Getting to Know the Network by Listening .....                            | 506        |
| 11.11.2      | Network Access Control and 802.1X .....                                   | 507        |
| <b>11.12</b> | <b>Extending Rights on the System .....</b>                               | <b>509</b> |
| 11.12.1      | Local Privilege Escalation .....                                          | 510        |
| 11.12.2      | Bypassing Windows User Account Control Using the<br>Default Setting ..... | 512        |
| 11.12.3      | Bypassing UAC Using the Highest Setting .....                             | 515        |
| <b>11.13</b> | <b>Collecting Credentials and Tokens .....</b>                            | <b>517</b> |
| 11.13.1      | Reading Passwords from Local and Domain Accounts .....                    | 518        |
| 11.13.2      | Bypassing Windows 10 Protection against mimikatz .....                    | 519        |
| 11.13.3      | Stealing Windows Tokens to Impersonate a User .....                       | 520        |
| 11.13.4      | Matching Users with DCSync .....                                          | 521        |
| 11.13.5      | Golden Ticket .....                                                       | 522        |
| 11.13.6      | Reading Local Password Hashes .....                                       | 523        |
| 11.13.7      | Broadcasting within the Network by Means of Pass-the-Hash .....           | 524        |
| 11.13.8      | Man-in-the-Middle Attacks in Local Area Networks .....                    | 527        |
| 11.13.9      | Basic Principles .....                                                    | 527        |
| 11.13.10     | LLMNR/NBT-NS and SMB Relaying .....                                       | 534        |
| <b>11.14</b> | <b>SMB Relaying Attack on Ordinary Domain Users .....</b>                 | <b>540</b> |
| 11.14.1      | Command-and-Control .....                                                 | 542        |

---

## **12 Securing Windows Servers** 543

---

|             |                                              |            |
|-------------|----------------------------------------------|------------|
| <b>12.1</b> | <b>Local Users, Groups, and Rights .....</b> | <b>544</b> |
| 12.1.1      | User and Password Properties .....           | 545        |
| 12.1.2      | Local Admin Password Solution .....          | 548        |
| <b>12.2</b> | <b>Manipulating the File System .....</b>    | <b>553</b> |
| 12.2.1      | Attacks on Virtualized Machines .....        | 556        |
| 12.2.2      | Protection .....                             | 557        |
| 12.2.3      | Attacking through the Registry .....         | 557        |
| <b>12.3</b> | <b>Server Hardening .....</b>                | <b>558</b> |
| 12.3.1      | Ensure a Secure Foundation .....             | 559        |
| 12.3.2      | Harden New Installations .....               | 559        |
| 12.3.3      | Protect Privileged Users .....               | 559        |

|             |                                              |     |
|-------------|----------------------------------------------|-----|
| 12.3.4      | Threat Detection .....                       | 560 |
| 12.3.5      | Secure Virtual Machines as Well .....        | 560 |
| 12.3.6      | Security Compliance Toolkit .....            | 560 |
| <b>12.4</b> | <b>Microsoft Defender</b> .....              | 561 |
| 12.4.1      | Defender Configuration .....                 | 562 |
| 12.4.2      | Defender Administration via PowerShell ..... | 563 |
| <b>12.5</b> | <b>Windows Firewall</b> .....                | 564 |
| 12.5.1      | Basic Configuration .....                    | 565 |
| 12.5.2      | Advanced Configuration .....                 | 565 |
| 12.5.3      | IP Security .....                            | 567 |
| <b>12.6</b> | <b>Windows Event Viewer</b> .....            | 568 |
| 12.6.1      | Classification of Events .....               | 569 |
| 12.6.2      | Log Types .....                              | 570 |
| 12.6.3      | Linking Actions to Event Logs .....          | 572 |
| 12.6.4      | Windows Event Forwarding .....               | 573 |
| 12.6.5      | Event Viewer Tools .....                     | 575 |

## **13 Active Directory** 579

---

|             |                                                                     |     |
|-------------|---------------------------------------------------------------------|-----|
| <b>13.1</b> | <b>What Is Active Directory?</b> .....                              | 579 |
| 13.1.1      | Domains .....                                                       | 580 |
| 13.1.2      | Partitions .....                                                    | 580 |
| 13.1.3      | Access Control Lists .....                                          | 583 |
| 13.1.4      | Security Descriptor Propagator .....                                | 585 |
| 13.1.5      | Standard Permissions .....                                          | 588 |
| 13.1.6      | The Confidentiality Attribute .....                                 | 592 |
| <b>13.2</b> | <b>Manipulating the Active Directory Database or its Data</b> ..... | 592 |
| 13.2.1      | ntdsutil Command .....                                              | 593 |
| 13.2.2      | dsamain Command .....                                               | 594 |
| 13.2.3      | Accessing the AD Database via Backups .....                         | 595 |
| <b>13.3</b> | <b>Manipulating Group Policies</b> .....                            | 596 |
| 13.3.1      | Configuration Files for Group Policies .....                        | 598 |
| 13.3.2      | Example: Changing a Password .....                                  | 600 |
| <b>13.4</b> | <b>Domain Authentication: Kerberos</b> .....                        | 603 |
| 13.4.1      | Kerberos: Basic Principles .....                                    | 603 |
| 13.4.2      | Kerberos in a Theme Park .....                                      | 604 |
| 13.4.3      | Kerberos on Windows .....                                           | 604 |
| 13.4.4      | Kerberos Tickets .....                                              | 605 |
| 13.4.5      | krbtgt Account .....                                                | 606 |

|              |                                                                                    |            |
|--------------|------------------------------------------------------------------------------------|------------|
| 13.4.6       | TGS Request and Reply .....                                                        | 608        |
| 13.4.7       | Older Authentication Protocols .....                                               | 610        |
| <b>13.5</b>  | <b>Attacks against Authentication Protocols and LDAP .....</b>                     | <b>611</b> |
| <b>13.6</b>  | <b>Pass-the-Hash Attacks: mimikatz .....</b>                                       | <b>612</b> |
| 13.6.1       | Setting up a Defender Exception .....                                              | 613        |
| 13.6.2       | Windows Credentials Editor .....                                                   | 614        |
| 13.6.3       | mimikatz .....                                                                     | 617        |
| 13.6.4       | The mimikatz “sekurlsa” Module .....                                               | 618        |
| 13.6.5       | mimikatz and Kerberos .....                                                        | 621        |
| 13.6.6       | PowerSploit .....                                                                  | 623        |
| <b>13.7</b>  | <b>Golden Ticket and Silver Ticket .....</b>                                       | <b>624</b> |
| 13.7.1       | Creating a Golden Ticket Using mimikatz .....                                      | 625        |
| 13.7.2       | Silver Ticket and Trust Ticket .....                                               | 627        |
| 13.7.3       | BloodHound .....                                                                   | 628        |
| 13.7.4       | Deathstar .....                                                                    | 628        |
| <b>13.8</b>  | <b>Reading Sensitive Data from the Active Directory Database .....</b>             | <b>628</b> |
| <b>13.9</b>  | <b>Basic Coverage .....</b>                                                        | <b>631</b> |
| 13.9.1       | Core Server .....                                                                  | 631        |
| 13.9.2       | Roles in the Core Server .....                                                     | 632        |
| 13.9.3       | Nano Server .....                                                                  | 633        |
| 13.9.4       | Updates .....                                                                      | 633        |
| 13.9.5       | Hardening the Domain Controller .....                                              | 634        |
| <b>13.10</b> | <b>More Security through Tiers .....</b>                                           | <b>635</b> |
| 13.10.1      | Group Policies for the Tier Model .....                                            | 636        |
| 13.10.2      | Authentication Policies and Silos .....                                            | 636        |
| <b>13.11</b> | <b>Protective Measures against Pass-the-Hash and Pass-the-Ticket Attacks... ..</b> | <b>639</b> |
| 13.11.1      | Kerberos Reset .....                                                               | 639        |
| 13.11.2      | Kerberos Policies .....                                                            | 641        |
| 13.11.3      | Kerberos Claims and Armoring .....                                                 | 642        |
| 13.11.4      | Monitoring and Detection .....                                                     | 643        |
| 13.11.5      | Microsoft Advanced Threat Analytics: Legacy .....                                  | 644        |
| 13.11.6      | Other Areas of Improvement in Active Directory .....                               | 647        |

---

## **14 Securing Linux** 649

---

|             |                                   |            |
|-------------|-----------------------------------|------------|
| <b>14.1</b> | <b>Other Linux Chapters .....</b> | <b>649</b> |
| <b>14.2</b> | <b>Installation .....</b>         | <b>650</b> |
| 14.2.1      | Server Distributions .....        | 650        |

---

|             |                                                               |            |
|-------------|---------------------------------------------------------------|------------|
| 14.2.2      | Partitioning the Data Medium .....                            | 652        |
| 14.2.3      | IPv6 .....                                                    | 653        |
| <b>14.3</b> | <b>Software Updates .....</b>                                 | <b>654</b> |
| 14.3.1      | Is a Restart Necessary? .....                                 | 655        |
| 14.3.2      | Automating Updates .....                                      | 655        |
| 14.3.3      | Configuring Automatic Updates on RHEL .....                   | 656        |
| 14.3.4      | Configuring Automatic Updates on Ubuntu .....                 | 656        |
| 14.3.5      | The Limits of Linux Update Systems .....                      | 657        |
| <b>14.4</b> | <b>Kernel Updates: Live Patches .....</b>                     | <b>658</b> |
| 14.4.1      | Kernel Live Patches .....                                     | 659        |
| 14.4.2      | Kernel Live Patches for RHEL .....                            | 660        |
| 14.4.3      | Kernel Live Patches on Ubuntu .....                           | 660        |
| <b>14.5</b> | <b>Securing SSH .....</b>                                     | <b>661</b> |
| 14.5.1      | sshd_config .....                                             | 661        |
| 14.5.2      | Blocking the Root Login .....                                 | 662        |
| 14.5.3      | Authentication with Keys .....                                | 663        |
| 14.5.4      | Authenticating with Keys in the Cloud .....                   | 664        |
| 14.5.5      | Blocking IPv6 .....                                           | 665        |
| <b>14.6</b> | <b>2FA with Google Authenticator .....</b>                    | <b>665</b> |
| 14.6.1      | Setting Up Google Authenticator .....                         | 666        |
| 14.6.2      | 2FA with Password and One-Time Code .....                     | 668        |
| 14.6.3      | What Happens if the Smartphone Is Lost? .....                 | 669        |
| 14.6.4      | Authy as an Alternative to the Google Authenticator App ..... | 670        |
| <b>14.7</b> | <b>2FA with YubiKey .....</b>                                 | <b>670</b> |
| 14.7.1      | PAM Configuration .....                                       | 671        |
| 14.7.2      | Mapping File .....                                            | 671        |
| 14.7.3      | SSH Configuration .....                                       | 672        |
| <b>14.8</b> | <b>Fail2ban .....</b>                                         | <b>673</b> |
| 14.8.1      | Installation .....                                            | 673        |
| 14.8.2      | Configuration .....                                           | 674        |
| 14.8.3      | Basic Parameters .....                                        | 676        |
| 14.8.4      | Securing SSH .....                                            | 676        |
| 14.8.5      | Securing Other Services .....                                 | 677        |
| 14.8.6      | Securing Custom Web Applications .....                        | 678        |
| 14.8.7      | Fail2ban Client .....                                         | 678        |
| <b>14.9</b> | <b>Firewall .....</b>                                         | <b>679</b> |
| 14.9.1      | From Netfilter to nftables .....                              | 680        |
| 14.9.2      | Basic Principles .....                                        | 680        |
| 14.9.3      | Determining the Firewall Status .....                         | 682        |
| 14.9.4      | Defining Rules .....                                          | 683        |

|              |                                                                               |     |
|--------------|-------------------------------------------------------------------------------|-----|
| 14.9.5       | Syntax for Firewall Rules .....                                               | 685 |
| 14.9.6       | Example: Simple Protection of a Web Server .....                              | 687 |
| 14.9.7       | Firewalld: RHEL .....                                                         | 688 |
| 14.9.8       | firewall-cmd Command .....                                                    | 689 |
| 14.9.9       | ufw: Ubuntu .....                                                             | 691 |
| 14.9.10      | Firewall Protection in the Cloud .....                                        | 693 |
| <b>14.10</b> | <b>SELinux</b> .....                                                          | 693 |
| 14.10.1      | Concept .....                                                                 | 693 |
| 14.10.2      | The Right Security Context .....                                              | 694 |
| 14.10.3      | Process Context: Domain .....                                                 | 695 |
| 14.10.4      | Policies .....                                                                | 696 |
| 14.10.5      | SELinux Parameters: Booleans .....                                            | 696 |
| 14.10.6      | Status .....                                                                  | 697 |
| 14.10.7      | Fixing SELinux Issues .....                                                   | 698 |
| <b>14.11</b> | <b>AppArmor</b> .....                                                         | 699 |
| 14.11.1      | AppArmor on Ubuntu .....                                                      | 700 |
| 14.11.2      | Rules: Profiles .....                                                         | 701 |
| 14.11.3      | Structure of Rule Files .....                                                 | 701 |
| 14.11.4      | Rule Parameters: Tunables .....                                               | 703 |
| 14.11.5      | Logging and Maintenance .....                                                 | 703 |
| <b>14.12</b> | <b>Kernel Hardening</b> .....                                                 | 704 |
| 14.12.1      | Changing Kernel Options Using sysctl .....                                    | 704 |
| 14.12.2      | Setting Kernel Boot Options in the GRUB Configuration .....                   | 706 |
| <b>14.13</b> | <b>Apache</b> .....                                                           | 706 |
| 14.13.1      | Certificates .....                                                            | 707 |
| 14.13.2      | Certificate Files .....                                                       | 708 |
| 14.13.3      | Apache Configuration .....                                                    | 709 |
| 14.13.4      | HTTPS Is Not HTTP .....                                                       | 710 |
| <b>14.14</b> | <b>MySQL and MariaDB</b> .....                                                | 712 |
| 14.14.1      | MySQL versus MariaDB .....                                                    | 712 |
| 14.14.2      | Login System .....                                                            | 713 |
| 14.14.3      | MySQL and MariaDB on Debian/Ubuntu .....                                      | 714 |
| 14.14.4      | Securing MySQL on RHEL .....                                                  | 715 |
| 14.14.5      | Securing MariaDB on RHEL .....                                                | 715 |
| 14.14.6      | Hash Codes in the “mysql.user” Table: Old MySQL and<br>MariaDB Versions ..... | 716 |
| 14.14.7      | Privileges .....                                                              | 717 |
| 14.14.8      | Server Configuration .....                                                    | 718 |
| <b>14.15</b> | <b>Postfix</b> .....                                                          | 719 |
| 14.15.1      | Postfix: Basic Settings .....                                                 | 719 |

|              |                                                        |            |
|--------------|--------------------------------------------------------|------------|
| 14.15.2      | Sending and Receiving Emails in Encrypted Form .....   | 720        |
| 14.15.3      | Spam and Virus Defense .....                           | 722        |
| <b>14.16</b> | <b>Dovecot .....</b>                                   | <b>724</b> |
| 14.16.1      | Using Custom Certificates for IMAP and POP .....       | 724        |
| 14.16.2      | SMTP Authentication for Postfix .....                  | 725        |
| <b>14.17</b> | <b>Rootkit Detection and Intrusion Detection .....</b> | <b>726</b> |
| 14.17.1      | chkrootkit .....                                       | 727        |
| 14.17.2      | rkhunter .....                                         | 728        |
| 14.17.3      | Lynis .....                                            | 729        |
| 14.17.4      | ISPProtect .....                                       | 730        |
| 14.17.5      | Snort .....                                            | 731        |
| 14.17.6      | Verifying Files from Packages .....                    | 731        |
| 14.17.7      | Scanning for Suspicious Ports and Processes .....      | 732        |

## **15 Security of Samba File Servers** 735

---

|             |                                               |            |
|-------------|-----------------------------------------------|------------|
| <b>15.1</b> | <b>Preliminary Considerations .....</b>       | <b>735</b> |
| 15.1.1      | Compiling Samba, SerNet Packages .....        | 736        |
| <b>15.2</b> | <b>Basic CentOS Installation .....</b>        | <b>737</b> |
| 15.2.1      | Partitions .....                              | 737        |
| 15.2.2      | Disabling IPv6 .....                          | 738        |
| 15.2.3      | Installing Samba Packages on CentOS .....     | 741        |
| <b>15.3</b> | <b>Basic Debian Installation .....</b>        | <b>741</b> |
| 15.3.1      | The Partitions .....                          | 741        |
| 15.3.2      | Disabling IPv6 .....                          | 742        |
| 15.3.3      | Installing Samba Packages on Debian .....     | 743        |
| <b>15.4</b> | <b>Configuring the Samba Server .....</b>     | <b>743</b> |
| 15.4.1      | Configuring the Kerberos Client .....         | 745        |
| <b>15.5</b> | <b>Samba Server in Active Directory .....</b> | <b>746</b> |
| 15.5.1      | Joining the Samba Server .....                | 746        |
| 15.5.2      | Testing the Server .....                      | 748        |
| <b>15.6</b> | <b>Shares on the Samba Server .....</b>       | <b>750</b> |
| 15.6.1      | File System Rights on Linux .....             | 750        |
| 15.6.2      | File System Rights on Windows .....           | 750        |
| 15.6.3      | Special Shares on a Windows Server .....      | 751        |
| 15.6.4      | The Admin Share on Samba .....                | 751        |
| 15.6.5      | Creating the Admin Share .....                | 751        |
| 15.6.6      | Creating the User Shares .....                | 752        |

- 15.7 Changes to the Registry** ..... 755
  - 15.7.1 Accessing the Registry from Windows ..... 757
- 15.8 Samba Audit Functions** ..... 758
- 15.9 Firewall** ..... 760
  - 15.9.1 Testing the Firewall Script ..... 763
  - 15.9.2 Starting Firewall Script Automatically ..... 764
- 15.10 Attack Scenarios on Samba File Servers** ..... 765
  - 15.10.1 Known Vulnerabilities in Recent Years ..... 766
- 15.11 Checking Samba File Servers** ..... 768
  - 15.11.1 Tests with nmap ..... 768
  - 15.11.2 Testing the Samba Protocols ..... 769
  - 15.11.3 Testing the Open Ports ..... 769
  - 15.11.4 smb-os-discovery ..... 771
  - 15.11.5 smb2-capabilities ..... 771
  - 15.11.6 ssh-brute ..... 772

**16 Intrusion Detection Systems** ..... 775

---

- 16.1 Intrusion Detection Methods** ..... 775
  - 16.1.1 Pattern Recognition: Static ..... 775
  - 16.1.2 Anomaly Detection (Dynamic) ..... 777
- 16.2 Host-Based versus Network-Based Intrusion Detection** ..... 778
  - 16.2.1 Host-Based IDS ..... 778
  - 16.2.2 Network-Based IDS ..... 779
  - 16.2.3 NIDS Metadata ..... 780
  - 16.2.4 NIDS Connection Contents ..... 782
- 16.3 Responses** ..... 783
  - 16.3.1 Automatic Intrusion Prevention ..... 783
  - 16.3.2 Walled Garden ..... 784
  - 16.3.3 Swapping Computers ..... 784
- 16.4 Bypassing and Manipulating Intrusion Detection** ..... 785
  - 16.4.1 Insertions ..... 785
  - 16.4.2 Evasions ..... 786
  - 16.4.3 Resource Consumption ..... 786
- 16.5 Snort** ..... 787
  - 16.5.1 Installation and Launch ..... 787
  - 16.5.2 Getting Started ..... 789
  - 16.5.3 IDS or IPS ..... 790

|             |                                                             |            |
|-------------|-------------------------------------------------------------|------------|
| 16.5.4      | Configuration .....                                         | 791        |
| 16.5.5      | Modules .....                                               | 791        |
| 16.5.6      | Snort Event Logging .....                                   | 792        |
| <b>16.6</b> | <b>Snort Rules .....</b>                                    | <b>793</b> |
| 16.6.1      | Syntax of Snort Rules .....                                 | 793        |
| 16.6.2      | Service Rules .....                                         | 794        |
| 16.6.3      | General Rule Options .....                                  | 795        |
| 16.6.4      | Matching Options .....                                      | 797        |
| 16.6.5      | Hyperscan .....                                             | 798        |
| 16.6.6      | Inspector-Specific Options .....                            | 799        |
| 16.6.7      | Managing Rule Sets with PulledPork .....                    | 800        |
| <b>17</b>   | <b>Security of Web Applications .....</b>                   | <b>803</b> |
| <b>17.1</b> | <b>Architecture of Web Applications .....</b>               | <b>803</b> |
| 17.1.1      | Components of Web Applications .....                        | 804        |
| 17.1.2      | Authentication and Authorization .....                      | 805        |
| 17.1.3      | Session Management .....                                    | 806        |
| <b>17.2</b> | <b>Attacks against Web Applications .....</b>               | <b>806</b> |
| 17.2.1      | Attacks against Authentication .....                        | 806        |
| 17.2.2      | Session Hijacking .....                                     | 807        |
| 17.2.3      | HTML Injection .....                                        | 808        |
| 17.2.4      | Cross-Site Scripting .....                                  | 811        |
| 17.2.5      | Session Fixation .....                                      | 815        |
| 17.2.6      | Cross-Site Request Forgery .....                            | 815        |
| 17.2.7      | Directory Traversal .....                                   | 816        |
| 17.2.8      | Local File Inclusion .....                                  | 817        |
| 17.2.9      | Remote File Inclusion .....                                 | 819        |
| 17.2.10     | File Upload .....                                           | 820        |
| 17.2.11     | SQL Injection .....                                         | 821        |
| 17.2.12     | sqlmap .....                                                | 823        |
| 17.2.13     | Advanced SQL Injection: Blind SQL Injection (Boolean) ..... | 824        |
| 17.2.14     | Advanced SQL Injection: Blind SQL Injection (Time) .....    | 825        |
| 17.2.15     | Advanced SQL Injection: Out-of-Band Data Exfiltration ..... | 827        |
| 17.2.16     | Advanced SQL Injection: Error-Based SQL Injection .....     | 827        |
| 17.2.17     | Command Injection .....                                     | 828        |
| 17.2.18     | Clickjacking .....                                          | 830        |
| 17.2.19     | XML Attacks .....                                           | 832        |
| 17.2.20     | Server Side Request Forgery .....                           | 834        |
| 17.2.21     | Angular Template Injection .....                            | 835        |

|             |                                                                    |            |
|-------------|--------------------------------------------------------------------|------------|
| 17.2.22     | Attacks on Object Serialization .....                              | 835        |
| 17.2.23     | Vulnerabilities in Content Management Systems .....                | 836        |
| <b>17.3</b> | <b>Practical Analysis of a Web Application .....</b>               | <b>837</b> |
| 17.3.1      | Information Gathering .....                                        | 838        |
| 17.3.2      | Testing SQL Injection .....                                        | 840        |
| 17.3.3      | Directory Traversal .....                                          | 845        |
| 17.3.4      | Port Knocking .....                                                | 847        |
| 17.3.5      | SSH Login .....                                                    | 849        |
| 17.3.6      | Privilege Escalation .....                                         | 850        |
| 17.3.7      | Automatic Analysis via Burp .....                                  | 855        |
| <b>17.4</b> | <b>Protection Mechanisms and Defense against Web Attacks .....</b> | <b>859</b> |
| 17.4.1      | Minimizing the Server Signature .....                              | 860        |
| 17.4.2      | Turning Off the Directory Listing .....                            | 860        |
| 17.4.3      | Restricted Operating System Account for the Web Server .....       | 861        |
| 17.4.4      | Running the Web Server in a “chroot” Environment .....             | 861        |
| 17.4.5      | Disabling Unneeded Modules .....                                   | 861        |
| 17.4.6      | Restricting HTTP Methods .....                                     | 862        |
| 17.4.7      | Restricting the Inclusion of External Content .....                | 862        |
| 17.4.8      | Protecting Cookies from Access .....                               | 863        |
| 17.4.9      | Server Timeout .....                                               | 863        |
| 17.4.10     | Secure Socket Layer .....                                          | 863        |
| 17.4.11     | HTTP Strict Transport Security .....                               | 864        |
| 17.4.12     | Input and Output Validation .....                                  | 865        |
| 17.4.13     | Web Application Firewall .....                                     | 866        |
| <b>17.5</b> | <b>Security Analysis of Web Applications .....</b>                 | <b>867</b> |
| 17.5.1      | Code Analysis .....                                                | 868        |
| 17.5.2      | Analysis of Binary Files .....                                     | 869        |
| 17.5.3      | Fuzzing .....                                                      | 869        |

## **18 Software Exploitation** 871

---

|             |                                       |            |
|-------------|---------------------------------------|------------|
| <b>18.1</b> | <b>Software Vulnerabilities .....</b> | <b>871</b> |
| 18.1.1      | Race Conditions .....                 | 871        |
| 18.1.2      | Logic Error .....                     | 872        |
| 18.1.3      | Format String Attacks .....           | 873        |
| 18.1.4      | Buffer Overflows .....                | 873        |
| 18.1.5      | Memory Leaks .....                    | 873        |

---

|              |                                                                      |            |
|--------------|----------------------------------------------------------------------|------------|
| <b>18.2</b>  | <b>Detecting Security Gaps .....</b>                                 | <b>874</b> |
| <b>18.3</b>  | <b>Executing Programs on x86 Systems .....</b>                       | <b>874</b> |
| 18.3.1       | Memory Areas .....                                                   | 874        |
| 18.3.2       | Stack Operations .....                                               | 876        |
| 18.3.3       | Calling Functions .....                                              | 879        |
| <b>18.4</b>  | <b>Exploiting Buffer Overflows .....</b>                             | <b>884</b> |
| 18.4.1       | Analysis of the Program Functionality .....                          | 884        |
| 18.4.2       | Creating a Program Crash .....                                       | 886        |
| 18.4.3       | Reproducing the Program Crash .....                                  | 888        |
| 18.4.4       | Analysis of the Crash .....                                          | 889        |
| 18.4.5       | Offset Calculation .....                                             | 891        |
| 18.4.6       | Creating the Exploit Structure .....                                 | 893        |
| 18.4.7       | Generating Code .....                                                | 895        |
| 18.4.8       | Dealing with Prohibited Characters .....                             | 896        |
| <b>18.5</b>  | <b>Structured Exception Handling .....</b>                           | <b>899</b> |
| <b>18.6</b>  | <b>Heap Spraying .....</b>                                           | <b>901</b> |
| <b>18.7</b>  | <b>Protective Mechanisms against Buffer Overflows .....</b>          | <b>903</b> |
| 18.7.1       | Address Space Layout Randomization .....                             | 903        |
| 18.7.2       | Stack Canaries or Stack Cookies .....                                | 904        |
| 18.7.3       | Data Execution Prevention .....                                      | 905        |
| 18.7.4       | SafeSEH and Structured Exception Handling Overwrite Protection ..... | 906        |
| 18.7.5       | Protection Mechanisms against Heap Spraying .....                    | 907        |
| <b>18.8</b>  | <b>Bypassing Protective Measures against Buffer Overflows .....</b>  | <b>907</b> |
| 18.8.1       | Bypassing Address Space Layout Randomization .....                   | 907        |
| 18.8.2       | Bypassing Stack Cookies .....                                        | 908        |
| 18.8.3       | Bypassing SafeSEH and SEHOP .....                                    | 908        |
| 18.8.4       | Return-Oriented Programming .....                                    | 908        |
| 18.8.5       | DEP Bypass .....                                                     | 911        |
| <b>18.9</b>  | <b>Preventing Buffer Overflows as a Developer .....</b>              | <b>914</b> |
| <b>18.10</b> | <b>Spectre and Meltdown .....</b>                                    | <b>915</b> |
| 18.10.1      | Meltdown .....                                                       | 915        |
| 18.10.2      | Defense Measures .....                                               | 916        |
| 18.10.3      | Proof of Concept (Meltdown) .....                                    | 917        |
| 18.10.4      | Spectre .....                                                        | 918        |
| 18.10.5      | Proof of Concept (Spectre) .....                                     | 919        |
| 18.10.6      | The Successors to Spectre and Meltdown .....                         | 921        |

**19 Bug Bounty Programs** 923

---

|                                                             |     |
|-------------------------------------------------------------|-----|
| <b>19.1 The Idea Behind Bug Bounties</b>                    | 923 |
| 19.1.1 Providers                                            | 923 |
| 19.1.2 Variants                                             | 924 |
| 19.1.3 Earning Opportunities                                | 925 |
| <b>19.2 Reporting Vulnerabilities</b>                       | 926 |
| 19.2.1 Testing Activities                                   | 926 |
| <b>19.3 Tips and Tricks for Analysts</b>                    | 927 |
| 19.3.1 Scope                                                | 927 |
| 19.3.2 Exploring the Response Quality of the Target Company | 927 |
| 19.3.3 Take Your Time                                       | 927 |
| 19.3.4 Finding Errors in Systems or Systems with Errors     | 928 |
| 19.3.5 Spend Money                                          | 928 |
| 19.3.6 Get Tips, Learn from the Pros                        | 928 |
| 19.3.7 Companies Buy Companies                              | 928 |
| 19.3.8 Creating a Test Plan                                 | 929 |
| 19.3.9 Automating Standard Processes                        | 929 |
| <b>19.4 Tips for Companies</b>                              | 930 |

**20 Security in the Cloud** 931

---

|                                             |     |
|---------------------------------------------|-----|
| <b>20.1 Overview</b>                        | 931 |
| 20.1.1 Arguments for the Cloud              | 932 |
| 20.1.2 Cloud Risks and Attack Vectors       | 933 |
| 20.1.3 Recommendations                      | 934 |
| <b>20.2 Amazon Simple Storage Service</b>   | 935 |
| 20.2.1 Basic Security and User Management   | 937 |
| 20.2.2 The aws Command                      | 938 |
| 20.2.3 Encrypting Files                     | 939 |
| 20.2.4 Public Access to Amazon S3 Files     | 941 |
| 20.2.5 Amazon S3 Hacking Tools              | 942 |
| <b>20.3 Nextcloud and ownCloud</b>          | 943 |
| 20.3.1 Installing Nextcloud                 | 944 |
| 20.3.2 Blocking Access to the “data Folder” | 946 |
| 20.3.3 Performing Updates                   | 947 |

|        |                                                                 |     |
|--------|-----------------------------------------------------------------|-----|
| 20.3.4 | File Encryption .....                                           | 948 |
| 20.3.5 | Security Testing for ownCloud and Nextcloud Installations ..... | 949 |
| 20.3.6 | Brute-Force Attacks and Protection .....                        | 950 |

## **21 Securing Microsoft 365** 953

---

|             |                                                                              |            |
|-------------|------------------------------------------------------------------------------|------------|
| <b>21.1</b> | <b>Identities and Access Management .....</b>                                | <b>954</b> |
| 21.1.1      | Azure Active Directory and Microsoft 365 .....                               | 954        |
| 21.1.2      | User Management in AAD .....                                                 | 957        |
| 21.1.3      | Application Integration .....                                                | 958        |
| <b>21.2</b> | <b>Security Assessment .....</b>                                             | <b>960</b> |
| <b>21.3</b> | <b>Multifactor Authentication .....</b>                                      | <b>961</b> |
| 21.3.1      | Preliminary Considerations .....                                             | 962        |
| 21.3.2      | Enabling Multifactor Authentication for a User Account .....                 | 962        |
| 21.3.3      | User Configuration of Multifactor Authentication .....                       | 963        |
| 21.3.4      | App Passwords for Incompatible Applications and Apps .....                   | 965        |
| <b>21.4</b> | <b>Conditional Access .....</b>                                              | <b>969</b> |
| 21.4.1      | Creating Policies .....                                                      | 970        |
| 21.4.2      | Conditions for Policies .....                                                | 972        |
| 21.4.3      | Access Controls .....                                                        | 973        |
| <b>21.5</b> | <b>Identity Protection .....</b>                                             | <b>975</b> |
| 21.5.1      | Responding to Vulnerabilities .....                                          | 975        |
| <b>21.6</b> | <b>Privileged Identities .....</b>                                           | <b>976</b> |
| 21.6.1      | Enabling Privileged Identities .....                                         | 977        |
| 21.6.2      | Configuring a User as a Privileged Identity .....                            | 979        |
| 21.6.3      | Requesting Administrator Permissions .....                                   | 980        |
| <b>21.7</b> | <b>Detecting Malicious Code .....</b>                                        | <b>982</b> |
| 21.7.1      | Protection for File Attachments .....                                        | 986        |
| 21.7.2      | Protection for Files in SharePoint Online and OneDrive for<br>Business ..... | 988        |
| 21.7.3      | Protection for Links .....                                                   | 989        |
| 21.7.4      | Protection for Links in Office Applications .....                            | 991        |
| <b>21.8</b> | <b>Security in Data Centers .....</b>                                        | <b>992</b> |
| 21.8.1      | Encryption of Your Data .....                                                | 992        |
| 21.8.2      | Access Governance .....                                                      | 994        |
| 21.8.3      | Audits and Privacy .....                                                     | 995        |

|             |                                                                  |      |
|-------------|------------------------------------------------------------------|------|
| <b>22</b>   | <b>Mobile Security</b>                                           | 997  |
| <b>22.1</b> | <b>Android and iOS Security: Basic Principles</b>                | 997  |
| 22.1.1      | Sandboxing                                                       | 998  |
| 22.1.2      | Authorization Concept                                            | 998  |
| 22.1.3      | Protection against Brute-Force Attacks when the Screen Is Locked | 999  |
| 22.1.4      | Device Encryption                                                | 1000 |
| 22.1.5      | Patch Days                                                       | 1001 |
| <b>22.2</b> | <b>Threats to Mobile Devices</b>                                 | 1003 |
| 22.2.1      | Theft or Loss of a Mobile Device                                 | 1003 |
| 22.2.2      | Unsecured and Open Networks                                      | 1004 |
| 22.2.3      | Insecure App Behavior at Runtime                                 | 1004 |
| 22.2.4      | Abuse of Authorizations                                          | 1006 |
| 22.2.5      | Insecure Network Communication                                   | 1007 |
| 22.2.6      | Attacks on Data Backups                                          | 1009 |
| 22.2.7      | Third-Party Stores                                               | 1013 |
| <b>22.3</b> | <b>Malware and Exploits</b>                                      | 1014 |
| 22.3.1      | Stagefright (Android)                                            | 1019 |
| 22.3.2      | Pegasus (iOS)                                                    | 1023 |
| 22.3.3      | Spy Apps                                                         | 1024 |
| <b>22.4</b> | <b>Technical Analysis of Apps</b>                                | 1025 |
| 22.4.1      | Reverse Engineering of Apps                                      | 1025 |
| 22.4.2      | Automated Vulnerability Analysis of Mobile Applications          | 1031 |
| <b>22.5</b> | <b>Protective Measures for Android and iOS</b>                   | 1036 |
| 22.5.1      | Avoid Rooting or Jailbreaking                                    | 1036 |
| 22.5.2      | Update Operating Systems and Apps                                | 1037 |
| 22.5.3      | Device Encryption                                                | 1038 |
| 22.5.4      | Antitheft Protection and Activation Lock                         | 1038 |
| 22.5.5      | Lock Screen                                                      | 1039 |
| 22.5.6      | Antivirus Apps                                                   | 1041 |
| 22.5.7      | Two-Factor Authentication                                        | 1042 |
| 22.5.8      | Critical Review of Permissions                                   | 1044 |
| 22.5.9      | Installing Apps from Alternative App Stores                      | 1045 |
| 22.5.10     | Using VPN Connections                                            | 1046 |
| 22.5.11     | Related Topic: WebAuthn and FIDO2                                | 1046 |
| 22.5.12     | Using Android and iOS in the Enterprise                          | 1048 |
| <b>22.6</b> | <b>Apple Supervised Mode and Apple Configurator</b>              | 1048 |
| 22.6.1      | Conclusion                                                       | 1055 |
| <b>22.7</b> | <b>Enterprise Mobility Management</b>                            | 1055 |
| 22.7.1      | Role and Authorization Management                                | 1057 |

|        |                                                                      |      |
|--------|----------------------------------------------------------------------|------|
| 22.7.2 | Device Management .....                                              | 1058 |
| 22.7.3 | App Management .....                                                 | 1059 |
| 22.7.4 | System Settings .....                                                | 1061 |
| 22.7.5 | Container Solutions Based on the Example of Android Enterprise ..... | 1062 |
| 22.7.6 | Tracking Managed Devices .....                                       | 1062 |
| 22.7.7 | Reporting .....                                                      | 1063 |
| 22.7.8 | Conclusion .....                                                     | 1064 |

## **23 Internet of Things Security** 1065

---

|             |                                                                |             |
|-------------|----------------------------------------------------------------|-------------|
| <b>23.1</b> | <b>What Is the Internet of Things? .....</b>                   | <b>1065</b> |
| <b>23.2</b> | <b>Finding IoT Vulnerabilities .....</b>                       | <b>1067</b> |
| 23.2.1      | Shodan Search Engine for Publicly Accessible IoT Devices ..... | 1067        |
| 23.2.2      | Using Shodan .....                                             | 1068        |
| 23.2.3      | For Professionals: Filtering Using Search Commands .....       | 1069        |
| 23.2.4      | Printer Exploitation Toolkit .....                             | 1071        |
| 23.2.5      | RouterSploit .....                                             | 1073        |
| 23.2.6      | AutoSploit .....                                               | 1077        |
| 23.2.7      | Consumer Devices as a Gateway .....                            | 1081        |
| 23.2.8      | Attacks from the Inside via a Port Scanner .....               | 1081        |
| 23.2.9      | Sample Port Scan of an Entertainment Device .....              | 1082        |
| 23.2.10     | Local Network versus Internet .....                            | 1083        |
| 23.2.11     | Incident Scenarios with Cheap IoT Devices .....                | 1083        |
| 23.2.12     | Danger from Network Operator Interfaces .....                  | 1084        |
| <b>23.3</b> | <b>Securing IoT Devices in Networks .....</b>                  | <b>1085</b> |
| <b>23.4</b> | <b>IoT Protocols and Services .....</b>                        | <b>1086</b> |
| 23.4.1      | MQ Telemetry Transport .....                                   | 1087        |
| 23.4.2      | Installing an MQTT Broker .....                                | 1089        |
| 23.4.3      | MQTT Example .....                                             | 1091        |
| 23.4.4      | \$SYS Topic Tree .....                                         | 1092        |
| 23.4.5      | Securing the Mosquitto MQTT Broker .....                       | 1094        |
| <b>23.5</b> | <b>Wireless IoT Technologies .....</b>                         | <b>1097</b> |
| 23.5.1      | 6LoWPAN .....                                                  | 1098        |
| 23.5.2      | Zigbee .....                                                   | 1098        |
| 23.5.3      | LoRaWAN .....                                                  | 1099        |
| 23.5.4      | NFC and RFID .....                                             | 1100        |
| 23.5.5      | NFC Hacking .....                                              | 1101        |
| <b>23.6</b> | <b>IoT from the Developer's Perspective .....</b>              | <b>1102</b> |
| 23.6.1      | Servers for IoT Operation .....                                | 1103        |

|                   |                                                                             |             |
|-------------------|-----------------------------------------------------------------------------|-------------|
| 23.6.2            | Embedded Linux, Android, or Windows IoT Devices .....                       | 1104        |
| 23.6.3            | Embedded Devices and Controllers without Classic Operating<br>Systems ..... | 1105        |
| <b>23.7</b>       | <b>Programming Languages for Embedded Controllers .....</b>                 | <b>1107</b> |
| 23.7.1            | C .....                                                                     | 1107        |
| 23.7.2            | C++ .....                                                                   | 1108        |
| 23.7.3            | Lua .....                                                                   | 1108        |
| <b>23.8</b>       | <b>Rules for Secure IoT Programming .....</b>                               | <b>1109</b> |
| 23.8.1            | Processes as Simple as Possible .....                                       | 1110        |
| 23.8.2            | Short, Testable Functions .....                                             | 1111        |
| 23.8.3            | Transfer Values Must Be Checked in Their Entirety .....                     | 1112        |
| 23.8.4            | Returning Error Codes .....                                                 | 1113        |
| 23.8.5            | Fixed Boundaries in Loops .....                                             | 1115        |
| 23.8.6            | No Dynamic Memory Allocation (or as Little as Possible) .....               | 1115        |
| 23.8.7            | Make Dimensioning Buffers or Arrays Sufficiently Large .....                | 1116        |
| 23.8.8            | Always Pass Buffer and Array Sizes .....                                    | 1116        |
| 23.8.9            | Use Caution with Function Pointers .....                                    | 1117        |
| 23.8.10           | Enabling Compiler Warnings .....                                            | 1118        |
| 23.8.11           | String Copy for Few Resources .....                                         | 1118        |
| 23.8.12           | Using Libraries .....                                                       | 1119        |
| The Authors ..... |                                                                             | 1121        |
| Index .....       |                                                                             | 1123        |