

# Inhaltsverzeichnis

|          |                                   |          |
|----------|-----------------------------------|----------|
| <b>1</b> | <b>Installation .....</b>         | <b>1</b> |
| 1.1      | Das richtige Betriebssystem ..... | 1        |
| 1.2      | Die richtige Python-Version ..... | 2        |
| 1.3      | Entwicklungsumgebung .....        | 2        |
| 1.4      | Python-Module .....               | 3        |
| 1.5      | Pip.....                          | 3        |
| 1.6      | Virtualenv .....                  | 4        |
| <br>     |                                   |          |
| <b>2</b> | <b>Netzwerk 4 Newbies .....</b>   | <b>5</b> |
| 2.1      | Komponenten .....                 | 5        |
| 2.2      | Topologien .....                  | 6        |
| 2.3      | ISO/OSI Schichtenmodell .....     | 8        |
| 2.4      | Ethernet .....                    | 9        |
| 2.5      | VLAN.....                         | 10       |
| 2.6      | ARP .....                         | 10       |
| 2.7      | IP .....                          | 11       |
| 2.8      | ICMP.....                         | 13       |
| 2.9      | TCP .....                         | 15       |
| 2.10     | UDP .....                         | 17       |
| 2.11     | Ein Fallbeispiel .....            | 18       |
| 2.12     | Architektur.....                  | 19       |
| 2.13     | Gateway .....                     | 19       |
| 2.14     | Router .....                      | 19       |
| 2.15     | Bridge .....                      | 20       |
| 2.16     | Proxies .....                     | 20       |
| 2.17     | Virtual Private Networks .....    | 21       |
| 2.18     | Firewalls .....                   | 21       |
| 2.19     | Man-in-the-middle-Attacken .....  | 22       |

|          |                                       |    |
|----------|---------------------------------------|----|
| <b>3</b> | <b>Python Basics</b>                  | 25 |
| 3.1      | Aller Anfang ist einfach              | 25 |
| 3.2      | Die Python Philosophie                | 26 |
| 3.3      | Datentypen                            | 27 |
| 3.4      | Datenstrukturen                       | 28 |
| 3.5      | Funktionen                            | 29 |
| 3.6      | Kontrollstrukturen                    | 31 |
| 3.7      | Module                                | 33 |
| 3.8      | Exceptions                            | 34 |
| 3.9      | Reguläre Ausdrücke                    | 34 |
| 3.10     | Sockets                               | 36 |
| <b>4</b> | <b>Layer-2-Angriffe</b>               | 39 |
| 4.1      | Benötigte Module                      | 39 |
| 4.2      | ARP-Cache-Poisoning                   | 40 |
| 4.3      | ARP-Watcher                           | 43 |
| 4.4      | MAC-Flooder                           | 45 |
| 4.5      | VLAN-Hopping                          | 46 |
| 4.6      | Selber Switch spielen                 | 47 |
| 4.7      | ARP-Spoofing über VLAN-Hopping        | 47 |
| 4.8      | DTP-Abusing                           | 48 |
| 4.9      | Tools                                 | 49 |
| 4.9.1    | NetCommander                          | 49 |
| 4.9.2    | Hacker's Hideaway ARP Attack Tool     | 49 |
| 4.9.3    | Loki                                  | 49 |
| <b>5</b> | <b>TCP / IP Tricks</b>                | 51 |
| 5.1      | Benötigte Module                      | 51 |
| 5.2      | Ein einfacher Sniffer                 | 51 |
| 5.3      | PCAP-Dump-Dateien schreiben und lesen | 53 |
| 5.4      | Password-Sniffer                      | 56 |
| 5.5      | Sniffer Detection                     | 58 |
| 5.6      | IP-Spoofing                           | 59 |
| 5.7      | SYN-Flooder                           | 60 |
| 5.8      | Port-Scanning                         | 61 |
| 5.9      | Portscan-Detection                    | 64 |
| 5.10     | ICMP-Redirection                      | 65 |
| 5.11     | RST-Daemon                            | 67 |
| 5.12     | Automatic-Hijack-Daemon               | 69 |
| 5.13     | Tools                                 | 73 |
| 5.13.1   | Scapy                                 | 73 |

|          |                         |     |
|----------|-------------------------|-----|
| <b>6</b> | <b>WHOIS DNS?</b>       | 77  |
| 6.1      | Protokollübersicht      | 77  |
| 6.2      | Benötigte Module        | 78  |
| 6.3      | Fragen über Fragen      | 78  |
| 6.4      | WHOIS                   | 79  |
| 6.5      | DNS Dictionary Mapper   | 81  |
| 6.6      | Reverse DNS Scanner     | 82  |
| 6.7      | DNS-Spoofing            | 85  |
| 6.8      | Tools                   | 87  |
| 6.8.1    | Chaosmap                | 87  |
| <b>7</b> | <b>HTTP Hacks</b>       | 89  |
| 7.1      | Protokollübersicht      | 89  |
| 7.2      | Webservices             | 93  |
| 7.3      | Benötigte Module        | 93  |
| 7.4      | HTTP Header Dumper      | 94  |
| 7.5      | Referer Spoofing        | 94  |
| 7.6      | Manipulieren von Keksen | 95  |
| 7.7      | HTTP-Auth Sniffing      | 96  |
| 7.8      | Webserver Scanning      | 97  |
| 7.9      | SQL-Injection           | 100 |
| 7.10     | Command-Injection       | 106 |
| 7.11     | Cross-Site-Scripting    | 108 |
| 7.12     | HTTPS                   | 109 |
| 7.13     | SSL/TLS sniffing        | 112 |
| 7.14     | Drive-by-Download       | 114 |
| 7.15     | Proxy Scanner           | 115 |
| 7.16     | Proxy Port Scanner      | 118 |
| 7.17     | Tools                   | 120 |
| 7.17.1   | SSL Strip               | 120 |
| 7.17.2   | Cookie Monster          | 120 |
| 7.17.3   | Sqlmap                  | 120 |
| 7.17.4   | W3AF                    | 121 |
| <b>8</b> | <b>Wifi fun</b>         | 123 |
| 8.1      | Protokollübersicht      | 123 |
| 8.2      | Benötigte Module        | 127 |
| 8.3      | WLAN-Scanner            | 127 |
| 8.4      | WLAN-Sniffer            | 128 |
| 8.5      | Probe-Request-Sniffer   | 129 |
| 8.6      | Hidden SSID             | 130 |
| 8.7      | MAC-Address-Filter      | 131 |

|           |                                             |            |
|-----------|---------------------------------------------|------------|
| 8.8       | WEP .....                                   | 132        |
| 8.9       | WPA .....                                   | 133        |
| 8.10      | WPA2 .....                                  | 136        |
| 8.11      | WLAN-Packet-Injection .....                 | 137        |
| 8.12      | WLAN Client spielen .....                   | 138        |
| 8.13      | Deauth .....                                | 139        |
| 8.14      | PMKID .....                                 | 141        |
| 8.15      | WPS .....                                   | 141        |
| 8.16      | WLAN Man-in-the-middle .....                | 142        |
| 8.17      | Wireless Intrusion Detection .....          | 147        |
| 8.18      | Tools .....                                 | 149        |
| 8.18.1    | KRACK attack .....                          | 149        |
| 8.18.2    | KrØØk attack .....                          | 150        |
| 8.18.3    | WiFuzz .....                                | 150        |
| 8.18.4    | Pyrit .....                                 | 150        |
| 8.18.5    | Wifiphisher .....                           | 150        |
| <b>9</b>  | <b>Bluetooth auf den Zahn geföhlt .....</b> | <b>151</b> |
| 9.1       | Protokollübersicht .....                    | 152        |
| 9.2       | BLE – Bluetooth Low Energy .....            | 154        |
| 9.3       | Benötigte Module .....                      | 155        |
| 9.4       | Bluetooth-Scanner .....                     | 155        |
| 9.5       | BLE-Scanner .....                           | 156        |
| 9.6       | GAP .....                                   | 157        |
| 9.7       | GATT .....                                  | 158        |
| 9.8       | SDP-Browser .....                           | 160        |
| 9.9       | RFCOMM-Channel-Scanner .....                | 162        |
| 9.10      | OBEX .....                                  | 164        |
| 9.11      | BIAS .....                                  | 165        |
| 9.12      | KNOB Attack .....                           | 166        |
| 9.13      | BlueBorne .....                             | 167        |
| 9.14      | Blue Snarf Exploit .....                    | 168        |
| 9.15      | Blue Bug Exploit .....                      | 170        |
| 9.16      | Bluetooth-Spoofing .....                    | 171        |
| 9.17      | Sniffing .....                              | 172        |
| 9.18      | Tools .....                                 | 174        |
| 9.18.1    | BlueMaho .....                              | 174        |
| 9.18.2    | BtleJack .....                              | 175        |
| <b>10</b> | <b>Grabbelkisten-Kung-Fu .....</b>          | <b>177</b> |
| 10.1      | Benötigte Module .....                      | 177        |
| 10.2      | Fälschen eines E-Mail-Absenders .....       | 177        |

---

|                                             |                           |            |
|---------------------------------------------|---------------------------|------------|
| 10.3                                        | DHCP Hijack .....         | 179        |
| 10.4                                        | IP Bruteforcer .....      | 182        |
| 10.5                                        | Google-Hacks-Scanner..... | 183        |
| 10.6                                        | SMB-Share-Scanner .....   | 184        |
| 10.7                                        | Login Watcher .....       | 186        |
| <b>Anhang A: Scapy-Referenz .....</b>       |                           | <b>191</b> |
| <b>Anhang B: Weiterführende Links .....</b> |                           | <b>217</b> |
| <b>Stichwortverzeichnis .....</b>           |                           | <b>219</b> |