

Inhaltsverzeichnis

1	Installation	1
1.1	Das richtige Betriebssystem	1
1.2	Die richtige Python-Version	2
1.3	Entwicklungsumgebung	2
1.4	Python-Module	3
2	Netzwerk 4 Newbies	5
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	13
2.10	UDP	17
2.11	Ein Fallbeispiel	17
2.12	Architektur	18
2.13	Gateway	19
2.14	Router	19
2.15	Bridge	20
2.16	Proxies	20
2.17	Virtual Private Networks	20
2.18	Firewalls	21
2.19	Man-in-the-middle-Attacken	22
3	Python Basics	23
3.1	Aller Anfang ist einfach	23
3.2	Die Python Philosophie	24
3.3	Datentypen	25

- 3.4 Datenstrukturen 26
 - 3.5 Funktionen 27
 - 3.6 Kontrollstrukturen 28
 - 3.7 Module 30
 - 3.8 Exceptions 31
 - 3.9 Reguläre Ausdrücke 32
 - 3.10 Sockets 33
- 4 **Layer-2-Angriffe** 35
 - 4.1 Benötigte Module 35
 - 4.2 ARP-Cache-Poisoning 36
 - 4.3 ARP-Watcher 39
 - 4.4 MAC-Flooder 41
 - 4.5 VLAN-Hopping 42
 - 4.6 Selber Switch spielen 42
 - 4.7 ARP-Spoofing über VLAN-Hopping 43
 - 4.8 DTP-Abusing 43
 - 4.9 Tools 44
 - 4.9.1 NetCommander 44
 - 4.9.2 Hacker’s Hideaway ARP Attack Tool 45
 - 4.9.3 Loki 45
- 5 **TCP/IP Tricks** 47
 - 5.1 Benötigte Module 47
 - 5.2 Ein einfacher Sniffer 47
 - 5.3 PCAP-Dump-Dateien schreiben und lesen 49
 - 5.4 Password-Sniffer 51
 - 5.5 Sniffer Detection 53
 - 5.6 IP-Spoofing 54
 - 5.7 SYN-Flooder 55
 - 5.8 Port-Scanning 56
 - 5.9 Portscan-Detection 59
 - 5.10 ICMP-Redirection 60
 - 5.11 RST-Daemon 62
 - 5.12 Automatic-Hijack-Daemon 64
 - 5.13 Tools 67
 - 5.13.1 Scapy 67
- 6 **WHOIS DNS?** 71
 - 6.1 Protokollübersicht 71
 - 6.2 Benötigte Module 72
 - 6.3 Fragen über Fragen 72
 - 6.4 WHOIS 73
 - 6.5 DNS Dictionary Mapper 74
 - 6.6 Reverse DNS Scanner 75

- 6.7 DNS-Spoofing 78
 - 6.8 Tools 81
 - 6.8.1 Chaosmap 81
- 7 HTTP Hacks 83
 - 7.1 Protokollübersicht 83
 - 7.2 Webservices 86
 - 7.3 Benötigte Module 87
 - 7.4 HTTP Header Dumper 87
 - 7.5 Referer Spoofing 88
 - 7.6 Manipulieren von Keksen 88
 - 7.7 HTTP-Auth Sniffing 90
 - 7.8 Webserver Scanning 90
 - 7.9 SQL-Injection 93
 - 7.10 Command-Injection 99
 - 7.11 Cross-Site-Scripting 100
 - 7.12 SSL-Sniffing 101
 - 7.13 Proxy Scanner 105
 - 7.14 Proxy Port Scanner 107
 - 7.15 Tools 109
 - 7.15.1 SSL Strip 109
 - 7.15.2 Cookie Monster 109
 - 7.15.3 Sqlmap 109
 - 7.15.4 W3AF 109
- 8 Wifi fun 111
 - 8.1 Protokollübersicht 111
 - 8.2 Benötigte Module 114
 - 8.3 WLAN-Scanner 114
 - 8.4 WLAN-Sniffer 116
 - 8.5 Probe-Request-Sniffer 117
 - 8.6 Hidden SSID 118
 - 8.7 MAC-Address-Filter 118
 - 8.8 WEP 119
 - 8.9 WPA 120
 - 8.10 WPA2 123
 - 8.11 WLAN-Packet-Injection 123
 - 8.12 WLAN Client spielen 124
 - 8.13 Deauth 126
 - 8.14 WLAN Man-in-the-middle 127
 - 8.15 Wireless Intrusion Detection 131
 - 8.16 Tools 133
 - 8.16.1 WiFuzz 133
 - 8.16.2 Pyrit 133
 - 8.16.3 AirXploit 133

9	Bluetooth auf den Zahn gefühlt	135
9.1	Protokollübersicht	135
9.2	Benötigte Module	137
9.3	Bluetooth-Scanner	137
9.4	SDP-Browser	138
9.5	RFCOMM-Channel-Scanner	139
9.6	OBEX	140
9.7	Blue Snarf Exploit	141
9.8	Blue Bug Exploit	142
9.9	Bluetooth-Spoofing	143
9.10	Sniffing	144
9.11	Tools	146
9.11.1	BlueMaho	146
10	Grabbelkisten-Kung-Fu	147
10.1	Benötigte Module	147
10.2	Fälschen eines E-Mail-Absenders	147
10.3	DHCP Hijack	148
10.4	IP Bruteforcer	151
10.5	Google-Hacks-Scanner	152
10.6	SMB-Share-Scanner	154
10.7	Login Watcher	155
A	Scapy-Referenz	159
A.1	Protokolle	159
A.2	Funktionen	167
B	Weiterführende Links	169
	Sachverzeichnis	171