

Contents

- 1 Installation 1**
 - 1.1 The Right Operating System..... 1
 - 1.2 The Right Python Version 1
 - 1.3 Development Environment 2
 - 1.4 Python Modules 3
- 2 Network 4 Newbies 5**
 - 2.1 Components 5
 - 2.2 Topologies 5
 - 2.3 ISO/OSI Layer Model..... 7
 - 2.4 Ethernet 8
 - 2.5 VLAN..... 9
 - 2.6 ARP 10
 - 2.7 IP 10
 - 2.8 ICMP..... 12
 - 2.9 TCP 12
 - 2.10 UDP 16
 - 2.11 An Example Network 16
 - 2.12 Architecture..... 17
 - 2.13 Gateway..... 18
 - 2.14 Router 18
 - 2.15 Bridge 19
 - 2.16 Proxies 19
 - 2.17 Virtual Private Networks 19
 - 2.18 Firewalls 20
 - 2.19 Man-in-the-Middle-Attacks..... 21
- 3 Python Basics 23**
 - 3.1 Every Start Is Simple..... 23
 - 3.2 The Python Philosophy 24
 - 3.3 Data Types 25
 - 3.4 Data Structures 26

3.5	Functions	27
3.6	Control Structures	28
3.7	Modules	30
3.8	Exceptions	31
3.9	Regular Expressions	31
3.10	Sockets	33
4	Layer 2 Attacks	35
4.1	Required Modules	35
4.2	ARP-Cache-Poisoning	35
4.3	ARP-Watcher	39
4.4	MAC-Flooder	41
4.5	VLAN Hopping	42
4.6	Let's Play Switch	42
4.7	ARP Spoofing Over VLAN Hopping	43
4.8	DTP Abusing	44
4.9	Tools	45
4.9.1	NetCommander	45
4.9.2	Hacker's Hideaway ARP Attack Tool	45
4.9.3	Loki	45
5	TCP/IP Tricks	47
5.1	Required Modules	47
5.2	A Simple Sniffer	47
5.3	Reading and Writing PCAP Dump Files	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	Port-Scan Detection	59
5.10	ICMP-Redirection	61
5.11	RST Daemon	63
5.12	Automatic Hijack Daemon	65
5.13	Tools	68
5.13.1	Scapy	68
6	WHOIS DNS?	73
6.1	Protocol Overview	73
6.2	Required Modules	74
6.3	Questions About Questions	74
6.4	WHOIS	75
6.5	DNS Dictionary Mapper	76
6.6	Reverse DNS Scanner	77
6.7	DNS-Spoofing	80

6.8	Tools	83
6.8.1	Chaosmap	83
7	HTTP Hacks	85
7.1	Protocol Overview	85
7.2	Web Services	88
7.3	Required Modules	88
7.4	HTTP Header Dumper	89
7.5	Referer Spoofing	89
7.6	The Manipulation of Cookies	90
7.7	HTTP-Auth Sniffing	91
7.8	Webserver Scanning	92
7.9	SQL Injection	95
7.10	Command Injection	101
7.11	Cross-Site-Scripting	102
7.12	SSL Sniffing	103
7.13	Proxy Scanner	107
7.14	Proxy Port Scanner	109
7.15	Tools	111
7.15.1	SSL Strip	111
7.15.2	Cookie Monster	111
7.15.3	Sqlmap	112
7.15.4	W3AF	112
8	Wifi Fun	113
8.1	Protocol Overview	113
8.2	Required Modules	115
8.3	Wifi Scanner	116
8.4	Wifi Sniffer	117
8.5	Probe-Request Sniffer	118
8.6	Hidden SSID	119
8.7	MAC-Address-Filter	120
8.8	WEP	120
8.9	WPA	122
8.10	WPA2	124
8.11	Wifi-Packet-Injection	124
8.12	Playing Wifi Client	125
8.13	Deauth	127
8.14	Wifi Man-in-the-Middle	128
8.15	Wireless Intrusion Detection	133
8.16	Tools	134
8.16.1	WiFuzz	134
8.16.2	Pyrit	135
8.16.3	AirXploit	135

9	Feeling Bluetooth on the Tooth	137
9.1	Protocol Overview	137
9.2	Required Modules	138
9.3	Bluetooth-Scanner	139
9.4	SDP-Browser	140
9.5	RFCOMM-Channel-Scanner	140
9.6	OBEX	142
9.7	Blue Snarf Exploit.....	143
9.8	Blue Bug Exploit	144
9.9	Bluetooth-Spoofing	145
9.10	Sniffing	146
9.11	Tools	148
	9.11.1 BlueMaho	148
10	Bargain Box Kung Fu	149
10.1	Required Modules	149
10.2	Spoofing E-mail Sender.....	149
10.3	DHCP Hijack	150
10.4	IP Brute Forcer	154
10.5	Google-Hacks-Scanner.....	155
10.6	SMB-Share-Scanner	156
10.7	Login Watcher	157
A	Scapy Reference	161
A.1	Protocols	161
A.2	Functions	162
B	Secondary Links	173
	Index	175



<http://www.springer.com/978-3-662-44436-8>

Understanding Network Hacks

Attack and Defense with Python

Ballmann, B.

2015, XIV, 178 p. 26 illus., Hardcover

ISBN: 978-3-662-44436-8