

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	2
1.5	Pip	3
1.6	Virtualenv	4
2	Network 4 Newbies	5
2.1	Components	5
2.2	Topologies	6
2.3	ISO/OSI Layer Model	7
2.4	Ethernet	8
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	An Example Network	18
2.12	Architecture	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-Attacks	22

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	29
3.7	Modules	32
3.8	Exceptions	33
3.9	Regular Expressions	33
3.10	Sockets	35
4	Layer 2 attacks	37
4.1	Required modules	37
4.2	ARP-Cache-Poisoning	38
4.3	ARP-Watcher	41
4.4	MAC-Flooder	43
4.5	VLAN hopping	44
4.6	Let's play switch	44
4.7	ARP spoofing over VLAN hopping	44
4.8	DTP abusing	45
4.9	Tools	46
4.9.1	NetCommander	46
4.9.2	Hacker's Hideaway ARP Attack Tool	46
4.9.3	Loki	46
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	58
5.10	ICMP-Redirection	60
5.11	RST Daemon	62
5.12	Automatic Hijack Daemon	63
5.13	Tools	67
5.13.1	Scapy	67

6	WHOIS DNS?	71
6.1	Protocol Overview	71
6.2	Required Modules	72
6.3	Questions About Questions	72
6.4	WHOIS	73
6.5	DNS Dictionary Mapper	75
6.6	Reverse DNS Scanner	76
6.7	DNS-Spoofing	79
6.8	Tools	81
6.8.1	Chaosmap	81
7	HTTP Hacks	83
7.1	Protocol Overview	83
7.2	Web Services	87
7.3	Required Modules	87
7.4	HTTP Header Dumper	87
7.5	Referer Spoofing	88
7.6	The Manipulation of Cookies	89
7.7	HTTP-Auth Sniffing	90
7.8	Webserver Scanning	91
7.9	SQL Injection	93
7.10	Command Injection	99
7.11	Cross-Site-Scripting	100
7.12	HTTPS	101
7.13	SSL / TLS Sniffing	104
7.14	Drive-by-Download	106
7.15	Proxy Scanner	107
7.16	Proxy Port Scanner	110
7.17	Tools	111
7.17.1	SSL Strip	111
7.17.2	Cookie Monster	112
7.17.3	Sqlmap	112
7.17.4	W3AF	112
8	Wifi Fun	113
8.1	Protocol Overview	113
8.2	Required Modules	117
8.3	Wifi Scanner	117
8.4	Wifi Sniffer	118
8.5	Probe-Request Sniffer	119
8.6	Hidden SSID	120
8.7	MAC-Address-Filter	121
8.8	WEP	121

8.9	WPA	123
8.10	WPA2	125
8.11	Wifi-Packet-Injection	125
8.12	Playing Wifi Client	126
8.13	Deauth	128
8.14	PMKID	129
8.15	WPS	130
8.16	Wifi Man-in-the-Middle	130
8.17	Wireless Intrusion Detection	135
8.18	Tools	137
8.18.1	KRACK Attack	137
8.18.2	KrØØk attack	137
8.18.3	WiFuzz	137
8.18.4	Pyrit	137
8.18.5	Wifiphisher	138
9	Feeling Bluetooth on the Tooth	139
9.1	Protocol Overview	139
9.2	BLE – Bluetooth Low Energy	141
9.3	Required Modules	142
9.4	Bluetooth-Scanner	143
9.5	BLE-Scanner	143
9.6	GAP	144
9.7	GATT	146
9.8	SDP-Browser	149
9.9	RFCOMM-Channel-Scanner	150
9.10	OBEX	151
9.11	BIAS	152
9.12	KNOB Attack	154
9.13	BlueBorne	155
9.14	Blue Snarf Exploit	156
9.15	Blue Bug Exploit	157
9.16	Bluetooth-Spoofing	158
9.17	Sniffing	159
9.18	Tools	161
9.18.1	BlueMaho	161
9.18.2	BtleJack	162
10	Bargain box Kung Fu	163
10.1	Required Modules	163
10.2	Spoofing e-mail Sender	163
10.3	DHCP Hijack	165
10.4	IP Brute Forcer	167

10.5	Google-Hacks-Scanner	168
10.6	SMB-Share-Scanner	169
10.7	Login Watcher	171
Appendix A Scapy reference		175
Appendix B Secondary links		215
Index		217