
Inhalt

1	Einführung	1
2	Ihre Python-Umgebung einrichten	3
2.1	Kali Linux installieren	3
2.2	WingIDE	5
3	Das Netzwerk: Grundlagen	11
3.1	Python-Networking – kurz und knapp	11
3.2	TCP-Client	12
3.3	UDP-Client	13
3.4	TCP-Server	13
3.5	Netcat ersetzen	15
3.6	Einen TCP-Proxy entwickeln	22
3.7	SSH mit Paramiko	28
3.8	SSH-Tunneling	32
4	Das Netzwerk: Raw Sockets und Sniffing	37
4.1	Ein UDP-Host-Discovery-Tool entwickeln	37
4.2	Paket-Sniffing unter Windows und Linux	38
4.3	Decodierung der IP-Schicht	40
4.4	ICMP decodieren	44
5	MIT SCAPY das Netzwerk übernehmen	51
5.1	E-Mail-Passwörter stehlen	51
5.2	ARP-Cache-Poisoning mit Scapy	54
5.3	PCAP-Verarbeitung	59

6	Hacking im Web	65
6.1	Die Socket-Bibliothek für das Web: urllib2	65
6.2	Open-Source-Webanwendungen	66
6.3	Brute-Forcing von Verzeichnissen und Dateien	69
6.4	Brute-Forcing der HTML-Formular-Authentifizierung	73
7	Den Burp-Proxy erweitern	81
7.1	Setup	81
7.2	Burp Fuzzing	83
7.3	Bing für Burp	93
7.4	Website-Inhalte in Passwort-Gold verwandeln	99
8	Command and Control per Github	107
8.1	Einen GitHub-Account einrichten	107
8.2	Module anlegen	109
8.3	Trojaner-Konfiguration	110
8.4	Einen GitHub-fähigen Trojaner entwickeln	111
9	Typische Trojaner-Aufgaben unter Windows	117
9.1	Keylogging	117
9.2	Screenshots	120
9.3	Shellcode ausführen	122
9.4	Sandbox-Erkennung	124
10	Hacking-Spaß mit dem Internet Explorer	129
10.1	Eine Art Man-in-the-Browser-Angriff	129
10.2	Daten ausschleusen per IE-COM	134
11	Windows-Rechte ausweiten	143
11.1	Voraussetzungen schaffen	144
11.2	Einen Prozessmonitor entwickeln	144
11.3	Windows-Token-Rechte	148
11.4	Das Rennen gewinnen	150
11.5	Code-Injection	154

12	Offensive Forensik automatisieren	157
12.1	Installation	157
12.2	Profile	158
12.3	Passwort-Hashes abgreifen	158
12.4	Direkte Code-Injection	162