11.3.2 Bereitstellung eines Post-Exploits . . . 428
11.3.3 Mit Metasploit-Multi-Handler zur Root-Shell . . . 431
11.4 Meterpreter – die Luxus-Shell für Hacker . . . 432
11.4.1 Exploits und Payload . . . 433
11.4.2 Einführung in Meterpreter . . . 433
11.4.3 Meterpreter-Shell in der Praxis . . . 435
11.4.4 Eine Meterpreter-Shell für Windows erstellen . . . 437
11.4.5 Externe Module in Meterpreter laden . . . 440
11.5 Empire – Das Powershell-Post-Exploitation-Framework . . . 442
11.5.1 Das Szenario . . . 442
11.5.2 Bereitstellung von Empire . . . 443
11.5.3 Grundlagen: Listener, Stager, Agents . . . 444
11.5.4 Empire in Aktion: Module nutzen . . . 447
11.6 Verteidigungsmaßnahmen gegen Privilegien-Eskalation . . . 449
11.7 Zusammenfassung und Prüfungstipps . . . 450
11.7.1 Zusammenfassung und Weiterführendes . . . 450
11.7.2 CEH-Prüfungstipps . . . 451
11.7.3 Fragen zur CEH-Prüfungsvorbereitung . . . 451

12 Mit Malware das System übernehmen . . . 453
12.1 Malware-Grundlagen . . . 454
12.1.1 Typische Malware-Kategorien . . . 454
12.1.2 Wie gelangt Malware auf das Opfer-System? . . . 456
12.1.3 Eine selbst erstellte Malware . . . 458
12.2 Viren und Würmer . . . 459
12.2.1 Was ist ein Computervirus? . . . 459
12.2.2 Was ist ein Computerwurm? . . . 461
12.2.3 Einen Makro-Virus erstellen . . . 462
12.3 Trojanische Pferde in der Praxis . . . 466
12.3.1 Trojaner-Typen . . . 466
12.3.2 Einen Trojaner selbst bauen . . . 468
12.3.3 Viren- und Trojaner-Baukästen . . . 471
12.4 Malware tarnen und vor Entdeckung schützen . . . 473
12.4.1 Grundlagen der Tarnung von Payload . . . 473
12.4.2 Encoder einsetzen . . . 476
12.4.3 Payload mit Hyperion verschlüsseln . . . 479
12.4.4 Das Veil-Framework . . . 480
12.4.5 Shellter AV Evasion . . . 480
12.4.6 Fileless Malware . . . 481
12.5 Rootkits . . . 483
12.5.1 Grundlagen der Rootkits . . . 483
12.5.2 Kernel-Rootkits . . . 484
12.5.3 Userland-Rootkits . . . 484
12.5.4 Rootkit-Beispiele . . . 485
12.5.5 Rootkits entdecken und entfernen . . . 485

12.6 Covert Channel . . . 486
12.6.1 ICMP-Tunneling . . . 487
12.6.2 NTFS Alternate Data Stream (ADS) . . . 490
12.7 Keylogger und Spyware . . . 492
12.7.1 Grundlagen . . . 492
12.7.2 Keylogger und Spyware in der Praxis . . . 492
12.8 Advanced Persistent Threat (APT) . . . 497
12.8.1 Wie funktioniert ein APT? . . . 497
12.8.2 Ablauf eines APT-Angriffs . . . 498
12.8.3 Zielgruppen von APT-Angriffen . . . 498
12.9 Schutzmaßnahmen gegen Malware . . . 499
12.10 Zusammenfassung und Prüfungstipps . . . 499
12.10.1 Zusammenfassung und Weiterführendes . . . 499
12.10.2 CEH-Prüfungstipps . . . 500
12.10.3 Fragen zur CEH-Prüfungsvorbereitung . . . 500

13 Malware-Erkennung und -Analyse . . . 503
13.1 Grundlagen der Malware-Analyse . . . 503
13.1.1 Statische Malware-Analyse . . . 504
13.1.2 Dynamische Malware-Analyse . . . 507
13.2 Verdächtiges Verhalten analysieren . . . 507
13.2.1 Virencheck durchführen . . . 508
13.2.2 Prozesse überprüfen . . . 512
13.2.3 Netzwerkaktivitäten prüfen . . . 515
13.2.4 Die Windows-Registrierung checken . . . 520
13.2.5 Autostart-Einträge unter Kontrolle . . . 524
13.2.6 Windows-Dienste checken . . . 526
13.2.7 Treiber überprüfen . . . 528
13.2.8 Integrität der Systemdateien prüfen . . . 530
13.2.9 Datei-Integrität durch Prüfsummen-Check . . . 531
13.2.10 System-Integrität mit Tripwire sichern . . . 533
13.3 Sheep-Dip-Systeme . . . 534
13.3.1 Einführung . . . 534
13.3.2 Aufbau eines Sheep-Dip-Systems . . . 535
13.4 Schutz durch Sandbox . . . 536
13.4.1 Sandboxie . . . 536
13.4.2 Cuckoo . . . 538
13.5 Aufbau einer modernen Anti-Malware-Infrastruktur . . . 539
13.5.1 Relevante Komponenten . . . 540
13.5.2 Komponenten der Anti-Malware-Infrastruktur . . . 540
13.6 Allgemeine Schutzmaßnahmen vor Malware-Infektion . . . 542
13.7 Zusammenfassung und Prüfungstipps . . . 543
13.7.1 Zusammenfassung und Weiterführendes . . . 543
13.7.2 CEH-Prüfungsgstipps . . . 544
13.7.3 Fragen zur CEH-Prüfungsvorbereitung . . . 545

14 Steganografie ... 547
14.1 Grundlagen der Steganografie ... 547
14.1.1 Wozu Steganografie? ... 547
14.1.2 Ein paar einfache Beispiele ... 548
14.1.3 Klassifikation der Steganografie ... 549
14.2 Computergestützte Steganografie ... 553
14.2.1 Daten in Bildern verstecken ... 553
14.2.2 Daten in Dokumenten verstecken ... 558
14.2.3 Weitere Cover-Datenformate ... 559
14.3 Steganalyse und Schutz vor Steganografie ... 560
14.3.1 Methoden der Steganalyse ... 560
14.3.2 Steganalyse-Tools ... 561
14.3.3 Schutz vor Steganografie ... 561
14.4 Zusammenfassung und Prüfungstipps ... 562
14.4.1 Zusammenfassung und Weiterführendes ... 562
14.4.2 CEH-Prüfungstipps ... 563
14.4.3 Fragen zur CEH-Prüfungsvorbereitung ... 563

15 Spuren verwischen ... 565
15.1 Auditing und Logging ... 565
15.1.1 Die Windows-Protokollierung ... 566
15.1.2 Die klassische Linux-Protokollierung ... 568
15.2 Spuren verwischen auf einem Windows-System ... 571
15.2.1 Das Windows-Auditing deaktivieren ... 571
15.2.2 Windows-Ereignisprotokolle löschen ... 573
15.2.3 Most Recently Used (MRU) löschen ... 575
15.2.4 Zeitstempel manipulieren ... 578
15.2.5 Clearing-Tools ... 582
15.3 Spuren verwischen auf einem Linux-System ... 583
15.3.1 Logfiles manipulieren und löschen ... 583
15.3.2 Systemd-Logging in Journald ... 586
15.3.3 Zeitstempel manipulieren ... 586
15.3.4 Die Befehlszeilen-Historie löschen ... 588
15.4 Schutz vor dem Spuren-Verwischen ... 589
15.5 Zusammenfassung und Prüfungstipps ... 590
15.5.1 Zusammenfassung und Weiterführendes ... 590
15.5.2 CEH-Prüfungstipps ... 591
15.5.3 Fragen zur CEH-Prüfungsvorbereitung ... 591

Teil IV Netzwerk- und sonstige Angriffe ... 595

16 Network Sniffing mit Wireshark & Co. ... 599
16.1 Grundlagen von Netzwerk-Sniffern ... 599
16.1.1 Technik der Netzwerk-Sniffer ... 599

16.1.2 Wireshark und die Pcap-Bibliotheken . . . 601
16.2 Wireshark installieren und starten . . . 601
16.2.1 Installation unter Linux . . . 601
16.2.2 Installation unter Windows . . . 602
16.2.3 Der erste Start . . . 603
16.3 Die ersten Schritte mit Wireshark . . . 604
16.3.1 Grundeinstellungen . . . 604
16.3.2 Ein erster Mitschnitt . . . 606
16.4 Mitschnitt-Filter einsetzen . . . 607
16.4.1 Analyse eines TCP-Handshakes . . . 608
16.4.2 Der Ping in Wireshark . . . 609
16.4.3 Weitere Mitschnittfilter . . . 610
16.5 Anzeigefilter einsetzen . . . 611
16.5.1 Eine HTTP-Sitzung im Detail . . . 612
16.5.2 Weitere Anzeigefilter . . . 614
16.6 Passwörter und andere Daten ausspähen . . . 615
16.6.1 FTP-Zugangsdaten ermitteln . . . 616
16.6.2 Telnet-Zugangsdaten identifizieren . . . 617
16.6.3 SSH – sicherer Schutz gegen Mitlesen . . . 619
16.6.4 Andere Daten ausspähen . . . 621
16.7 Auswertungsfunktionen von Wireshark nutzen . . . 622
16.8 Tcpdump und TShark einsetzen . . . 624
16.8.1 Tcpdump – der Standard-Sniffer für die Konsole . . . 624
16.8.2 TShark – Wireshark auf der Konsole . . . 627
16.9 Zusammenfassung und Prüfungstipps . . . 629
16.9.1 Zusammenfassung und Weiterführendes . . . 629
16.9.2 CEH-Prüfungstipps . . . 629
16.9.3 Fragen zur CEH-Prüfungsvorbereitung . . . 630

17 Lauschangriffe & Man-in-the-Middle . . . 633
17.1 Eavesdropping und Sniffing für Hacker . . . 633
17.1.1 Eavesdropping und Wiretapping . . . 634
17.1.2 Sniffing als Angriffsvektor . . . 634
17.2 Man-in-the-Middle (MITM) . . . 635
17.2.1 Was bedeutet Man-in-the-Middle? . . . 636
17.2.2 Was erreichen wir durch einen MITM-Angriff? . . . 637
17.3 Active Sniffing . . . 637
17.3.1 Mirror-Ports: Ein Kabel mit drei Enden . . . 638
17.3.2 Aus Switch mach Hub – MAC-Flooding . . . 638
17.3.3 Auf dem Silbertablett: WLAN-Sniffing . . . 640
17.3.4 Weitere physische Abhörmöglichkeiten . . . 641
17.4 Die Kommunikation für MITM umleiten . . . 641
17.4.1 Physische Umleitung . . . 641
17.4.2 Umleitung über aktive Netzwerk-Komponenten . . . 642
17.4.3 Umleiten mit ARP-Spoofing . . . 643

17.4.4 ICMP-Typ 5 Redirect 643
17.4.5 DNS-Spoofing oder DNS-Cache-Poisoning 644
17.4.6 Manipulation der hosts-Datei 646
17.4.7 Umleiten via DHCP-Spoofing 647
17.5 Die Dsniff-Toolsammlung 648
17.5.1 Programme der Dsniff-Suite 648
17.5.2 Abhören des Netzwerk-Traffics 649
17.5.3 MITM mit arpspoof 650
17.5.4 Die ARP-Tabelle des Switches mit macof überfluten 653
17.5.5 DNS-Spoofing mit dnspoof 653
17.5.6 Dsniff 656
17.6 Man-in-the-Middle-Angriffe mit Ettercap 657
17.6.1 Einführung in Ettercap 657
17.6.2 DNS-Spoofing mit Ettercap 659
17.7 Schutz vor Lauschangriffen & MITM 667
17.8 Zusammenfassung und Prüfungstipps 669
17.8.1 Zusammenfassung und Weiterführendes 669
17.8.2 CEH-Prüfungstipps 670
17.8.3 Fragen zur CEH-Prüfungsvorbereitung 670

18 Session Hijacking 673
18.1 Grundlagen des Session Hijackings 673
18.1.1 Wie funktioniert Session Hijacking grundsätzlich? 674
18.1.2 Session-Hijacking-Varianten 674
18.2 Network Level Session Hijacking 675
18.2.1 Die TCP-Session im Detail 676
18.2.2 Entführen von TCP-Sessions 678
18.2.3 Eine Telnet-Session entführen 680
18.2.4 Weitere Hijacking-Varianten auf Netzwerk-Ebene 685
18.3 Application Level Session Hijacking 686
18.3.1 Die Session-IDs 686
18.3.2 Die Session-ID ermitteln 687
18.3.3 Sniffing/Man-in-the-Middle 688
18.3.4 Die Session-ID erraten – das Prinzip 688
18.3.5 WebGoat bereitstellen 689
18.3.6 Die Burp Suite – Grundlagen und Installation 692
18.3.7 Burp Suite als Intercepting Proxy 693
18.3.8 Der Burp Sequencer – Session-IDs analysieren 697
18.3.9 Entführen der Session mithilfe der Session-ID 700
18.3.10 Man-in-the-Browser-Angriff 707
18.3.11 Weitere Angriffsformen 709
18.4 Gegenmaßnahmen gegen Session Hijacking 711
18.4.1 Session Hijacking entdecken 711
18.4.2 Schutzmaßnahmen 712