

Kapitel 12: Mit Malware das System übernehmen

12.1 Malware-Grundlagen

12.1.1 Typische Malware-Kategorien

12.1.2 Wie gelangt Malware auf das Opfer-System?

12.1.3 Eine selbst erstellte Malware

12.2 Viren und Würmer

12.2.1 Was ist ein Computervirus?

12.2.2 Was ist ein Computerwurm?

12.2.3 Einen Makro-Virus erstellen

12.3 Trojanische Pferde in der Praxis

12.3.1 Trojaner-Typen

12.3.2 Einen Trojaner selbst bauen

12.3.3 Viren- und Trojaner-Baukästen

12.4 Malware tarnen und vor Entdeckung schützen

12.4.1 Grundlagen der Tarnung von Payload

12.4.2 Encoder einsetzen

12.4.3 Payload mit Hyperion verschlüsseln

12.4.4 Das Veil-Framework

12.4.5 Shellter AV Evasion

12.4.6 Fileless Malware

12.5 Rootkits

12.5.1 Grundlagen der Rootkits

12.5.2 Kernel-Rootkits

12.5.3 Userland-Rootkits

12.5.4 Rootkit-Beispiele

12.5.5 Rootkits entdecken und entfernen

12.6 Covert Channel

12.6.1 ICMP-Tunneling

12.6.2 NTFS Alternate Data Stream (ADS)

12.7 Keylogger und Spyware

12.7.1 Grundlagen

12.7.2 Keylogger und Spyware in der Praxis

12.8 Advanced Persistent Threat (APT)

12.8.1 Wie funktioniert ein APT?

- 12.8.2 Ablauf eines APT-Angriffs
- 12.8.3 Zielgruppen von APT-Angriffen
- 12.9 Schutzmaßnahmen gegen Malware
- 12.10 Zusammenfassung und Prüfungstipps
 - 12.10.1 Zusammenfassung und Weiterführendes
 - 12.10.2 CEH-Prüfungstipps
 - 12.10.3 Fragen zur CEH-Prüfungsvorbereitung

Kapitel 13: Malware-Erkennung und -Analyse

- 13.1 Grundlagen der Malware-Analyse
 - 13.1.1 Statische Malware-Analyse
 - 13.1.2 Dynamische Malware-Analyse
- 13.2 Verdächtiges Verhalten analysieren
 - 13.2.1 Virencheck durchführen
 - 13.2.2 Prozesse überprüfen
 - 13.2.3 Netzwerkaktivitäten prüfen
 - 13.2.4 Die Windows-Registrierung checken
 - 13.2.5 Autostart-Einträge unter Kontrolle
 - 13.2.6 Windows-Dienste checken
 - 13.2.7 Treiber überprüfen
 - 13.2.8 Integrität der Systemdateien prüfen
 - 13.2.9 Datei-Integrität durch Prüfsummen-Check
 - 13.2.10 System-Integrität mit Tripwire sichern
- 13.3 Sheep-Dip-Systeme
 - 13.3.1 Einführung
 - 13.3.2 Aufbau eines Sheep-Dip-Systems
- 13.4 Schutz durch Sandbox
 - 13.4.1 Sandboxie
 - 13.4.2 Cuckoo
- 13.5 Aufbau einer modernen Anti-Malware-Infrastruktur
 - 13.5.1 Relevante Komponenten
 - 13.5.2 Komponenten der Anti-Malware-Infrastruktur
- 13.6 Allgemeine Schutzmaßnahmen vor Malware-Infektion
- 13.7 Zusammenfassung und Prüfungstipps

- 13.7.1 Zusammenfassung und Weiterführendes
- 13.7.2 CEH-Prüfungstipps
- 13.7.3 Fragen zur CEH-Prüfungsvorbereitung

Kapitel 14: Steganografie

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

Kapitel 15: Spuren verwischen

- 15.1 Auditing und Logging
 - 15.1.1 Die Windows-Protokollierung
 - 15.1.2 Die klassische Linux-Protokollierung
- 15.2 Spuren verwischen auf einem Windows-System
 - 15.2.1 Das Windows-Auditing deaktivieren
 - 15.2.2 Windows-Ereignisprotokolle löschen
 - 15.2.3 Most Recently Used (MRU) löschen
 - 15.2.4 Zeitstempel manipulieren
 - 15.2.5 Clearing-Tools
- 15.3 Spuren verwischen auf einem Linux-System
 - 15.3.1 Logfiles manipulieren und löschen
 - 15.3.2 Systemd-Logging in Journald

- 15.3.3 Zeitstempel manipulieren
- 15.3.4 Die Befehlszeilen-Historie löschen
- 15.4 Schutz vor dem Spuren-Verwischen
- 15.5 Zusammenfassung und Prüfungstipps
 - 15.5.1 Zusammenfassung und Weiterführendes
 - 15.5.2 CEH-Prüfungstipps
 - 15.5.3 Fragen zur CEH-Prüfungsvorbereitung

Teil IV: Netzwerk- und sonstige Angriffe

Kapitel 16: Network Sniffing mit Wireshark & Co.

- 16.1 Grundlagen von Netzwerk-Sniffern
 - 16.1.1 Technik der Netzwerk-Sniffer
 - 16.1.2 Wireshark und die Pcap-Bibliotheken
- 16.2 Wireshark installieren und starten
 - 16.2.1 Installation unter Linux
 - 16.2.2 Installation unter Windows
 - 16.2.3 Der erste Start
- 16.3 Die ersten Schritte mit Wireshark
 - 16.3.1 Grundeinstellungen
 - 16.3.2 Ein erster Mitschnitt
- 16.4 Mitschnitt-Filter einsetzen
 - 16.4.1 Analyse eines TCP-Handshakes
 - 16.4.2 Der Ping in Wireshark
 - 16.4.3 Weitere Mitschnittfilter
- 16.5 Anzeigefilter einsetzen
 - 16.5.1 Eine HTTP-Sitzung im Detail
 - 16.5.2 Weitere Anzeigefilter
- 16.6 Passwörter und andere Daten ausspähen
 - 16.6.1 FTP-Zugangsdaten ermitteln
 - 16.6.2 Telnet-Zugangsdaten identifizieren
 - 16.6.3 SSH – sicherer Schutz gegen Mitlesen
 - 16.6.4 Andere Daten ausspähen
- 16.7 Auswertungsfunktionen von Wireshark nutzen

- 16.8 Tcpcdump und TShark einsetzen
 - 16.8.1 Tcpcdump – der Standard-Sniffer für die Konsole
 - 16.8.2 TShark – Wireshark auf der Konsole
- 16.9 Zusammenfassung und Prüfungstipps
 - 16.9.1 Zusammenfassung und Weiterführendes
 - 16.9.2 CEH-Prüfungstipps
 - 16.9.3 Fragen zur CEH-Prüfungsvorbereitung

Kapitel 17: Lauschangriffe & Man-in-the-Middle

- 17.1 Eavesdropping und Sniffing für Hacker
 - 17.1.1 Eavesdropping und Wiretapping
 - 17.1.2 Sniffing als Angriffsvektor
- 17.2 Man-in-the-Middle (MITM)
 - 17.2.1 Was bedeutet Man-in-the-Middle?
 - 17.2.2 Was erreichen wir durch einen MITM-Angriff?
- 17.3 Active Sniffing
 - 17.3.1 Mirror-Ports: Ein Kabel mit drei Enden
 - 17.3.2 Aus Switch mach Hub – MAC-Flooding
 - 17.3.3 Auf dem Silbertablett: WLAN-Sniffing
 - 17.3.4 Weitere physische Abhörmöglichkeiten
- 17.4 Die Kommunikation für MITM umleiten
 - 17.4.1 Physische Umleitung
 - 17.4.2 Umleitung über aktive Netzwerk-Komponenten
 - 17.4.3 Umleiten mit ARP-Spoofing
 - 17.4.4 ICMP-Typ 5 Redirect
 - 17.4.5 DNS-Spoofing oder DNS-Cache-Poisoning
 - 17.4.6 Manipulation der hosts-Datei
 - 17.4.7 Umleiten via DHCP-Spoofing
- 17.5 Die Dsniff-Toolsammlung
 - 17.5.1 Programme der Dsniff-Suite
 - 17.5.2 Abhören des Netzwerk-Traffics
 - 17.5.3 MITM mit arpspoof
 - 17.5.4 Die ARP-Tabelle des Switches mit macof überfluten
 - 17.5.5 DNS-Spoofing mit dnspooft
 - 17.5.6 Dsniff