IT Security Grundlagen

Agenda für den CSP Jahrgang 10

Tom Gries | Berlin | Oktober 2023

Dokumenten URL: http://docs.tx7.de/TT-CSP
Autor: Tom Gries <TT-CSP@tx7.de>
@tomo@chaos.social

Version: 7.0.0 vom 20.10.2023

Zielgruppe:

Dieses Training richtet sich hauptsächlich an Teilnehmer des Cyber Security Professional Programms (CSP). Ziel dieses Trainings ist es, den Teilnehmern einen Überblick über die für dieses Programm benötigten Skills und Impulse zur Bildung von Lerngruppen zu geben.

Die Teilnehmer haben die Möglichkeit, selber einfache Angriffe auszuprobieren, wie zum Beispiel Cracken von passwortgeschützten ZIP-Archiven, überwinden des Windows Zugangsschutzes, Passwort-Cracking mit John the Ripper sowie SQL-Injection.

Was müsst ihr mitbringen:

Für die praktischen Teile wird ein Laptop mit Internetzugang und einem aktuellen Browser auf einem beliebigen Betriebssystem benötigt. Netzwerktechnisch werden die Ports HTTP:80, HTTPS:443 sowie HTTPS:8006 benötigt. Zum Testen können folgende Adressen verwendet werden:

- http://training.tx7.de => [einfache Testseite]
- https://training.tx7.de => [einfache Testseite]
- https://training.tx7.de:8006 => [Proxmox Startseite]

Die Adresse training.tx7.de kann in restriktiven Umgebungen zum Whitelisting verwendet werden.

Themen des Kurses

A - Grundlagen des Internets und Internet Technologien - Die Basics

01 History of the Internet - Wie alles begann

02 "Wie funktioniert das Internet?" Eine Erklärung mit der Maus

03 Internet Organisationen und Standards

04 Adressierung (Verzeichnisbäume, URLs, IP-Adressen, MAC-Adressen und DNS)

05 Sicherheitsaspekte in der Adressierung (Spoofing, Verschleierung)

B - Hardware, Software, Skript- und Programmiersprachen

01 Netzwerkkomponenten: Hub, Bridge, Switch, Router, Firewalls, IDS/IPS, Load-Balancer etc.

02 Betriebssysteme (Windows, macOS, Unix/Linux), Virtualisierung und Tools (WSL, Terminal etc.)

03 Wesentliche Programmier- und Skriptsprachen

Themen des Kurses

C – Wesentliche Dienste und Internet Protokolle

01 TCP/IP – Das OSI und DoD Schichtenmodell, ICMP, TCP/UDP und Ports

02 Standardprotokolle für die Dateiübertragung – HTTP(S) und FTP(S)

03 Mail Protokolle – SMTP, POP3, IMAP4 und Spoofing mit Telnet

04 Technologien in Heimnetzwerken (VPN, Proxy, PAT, NAT, DynDNS und das TOR Netzwerk)

D – Security Technologien und Konzept

01 Grundlagen der Kryptologie

02 Codes und Datenintegrität

Themen des Kurses

X - Security Deep Dive und Live-Demonstrationen

01 Social Engineering - Hoaxe (Fake News), Malware und CEO-Fraud

02 Passwortgeschütztes ZIP-Archiv und Passwort Hashe cracken

03 Security in Datenbanken - SQL-Injection

04 Windows Zugangsschutz überwinden und lokale Passwörter aufdecken

05 P4wnP1 A.L.O.A. - Passworthashe stehlen und HOSTS-Datei manipulieren

Anmerkungen oder Fragen?