IT Security Grundlagen

Agenda für den Workshop

Dokumenten URL:	http://docs.tx7.de/TT-C11
Autor:	Tom Gries <TT-C11@tx7.de>
	@tomo@chaos.social
Lizenz:	Creative Commons BY-NC-ND
Version:	7.1.0 vom 20.10.2024

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

Die Adressen porttest.tx7.de und training.tx7.de müssen in restriktiven Umgebungen zur Whitelist hinzugefügt werden.

Themen des Kurses

Tag 1

01 History of the Internet - Wie alles begann

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

03 Internet Organisationen und Standards

04 Ein Spiel mit Quadraten ...

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

06 Sicherheitsaspekte in der Adressierung (Spoofing, Verschleierung)

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

08 Wesentliche Programmier- und Skriptsprachen

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

10 Einführung in Proxmox

11 Security in Datenbanken - SQL-Injection

Themen des Kurses

Tag 2

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

02 Wesentliche Protokolle - HTTP(S), FTP(S), DHCP, SMTP, POP4, IMAP4 und Spoofing mit Telnet

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

04 Codes und Datenintegrität

05 Grundlagen der Kryptologie

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

07 Passwortgeschütztes ZIP-Archiv und Passwort Hashe cracken

08 Benchmarks mit John the Ripper und Hashcat

09 Windows Zugangsschutz überwinden und lokale Passwörter aufdecken

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

11 Zusammenfassung