Cybersecurity Foundation für IT-Professionals.

Cybersecurity Foundation für IT-Professionals.

Seminar | 5 Termine verfügbar | Teilnahmebescheinigung

Präsenz / Virtual Classroom | 32 Unterrichtseinheiten | Garantietermine vorhanden

Seminarnummer: 31490

Stand: 05.02.2025. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31490

Das Einführungsseminar vermittelt ein grundlegendes Verständnis in den Themengebieten der Cybersicherheit.

Nutzen

Die theoretischen Grundlagen bilden die Betrachtung von historischen Cyberangriffen, aktuellen Industriestandards und der vorhandenen Bedrohungslage. Unser Labor stellt ein Unternehmensnetzwerk nach, mit welchem Ihnen mitunter ein Rollenwechsel ermöglicht wird und Sie als Angreifer typische Techniken und Werkzeuge anwenden können.

Teilnehmer dieses Seminars können in ihrem täglichen Aufgabengebiet sinnvollere Entscheidungen zur effizienten und nachhaltigen Verbesserung der IT-Sicherheit treffen.

Der Workshop grenzt sich durch seine Herstellerunabhängigkeit von anderen Cybersecurity-Trainings ab. Die Industrieerfahrung des Trainers und das praxisrelevante dedizierte Labor gestalten den Workshop zielführend und lebendig. Spezifische Themen wie BSI-Grundschutz und NIS2 werden mitberücksichtigt.

- Sie lernen sinnvolle und nachhaltige Entscheidungen zur effizienten Verbesserung der IT-Sicherheit zu treffen.
- Sie erhalten einen umfassenden Einblick, durch die Orientierung der praktischen Kursinhalte an dem MITRE ATT&CK® Framework.
- Sie lernen die aktuellen Angriffstechniken und Werkzeuge von Cyberkriminellen kennen.
- Sie versetzen sich mittels Laborübungen in die Lage eines Angreifers und verstehen dadurch die kritischen Sicherheitsmaßnahmen für die Netzwerkverteidigung.
- Sie lernen aus dem Erfahrungsschatz eines Consultants, der viele Penetrationstests, forensische Analysen und Incident-Response durchgeführt hat.
- Sie lernen, wie Angreifer moderne Sicherheitstechnologien umgehen.

- Sie verstehen die Bedrohungslage speziell in Deutschland und wenden Compliance-Frameworks wie BSI-Grundschutz zielgerichtet an.
- Sie erhalten einen Einblick in die neue Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS2).

Zielgruppe

Dieser Kurs ist geeignet für Einsteiger in das Cybersecurity-Thema und vermittelt grundlegende Konzepte sowie technische und praktische Kenntnisse.

Angesporchen werden folgende Jobrollen:
- Administratoren (Netzwerk, Windows, Linux, Cloud, DevOps)
- Sicherheitsbeauftragte
- Programmierer
- SOC-Analysts
- Cybersecurity Engineers
- IT-Manager

Voraussetzungen

Allgemeine IT-Admin-Erfahrung, Grundlegendes Verständnis von Netzwerken, Wünschenswert: Kommandozeilenerfahrung

Inhalte des Seminars

Der Kurs lehrt anhand realistischer Übungen die Grundlagen der Cybersicherheit. Die Auswahl des praktischen Kursinhaltes orientiert sich dabei an dem MITRE ATT&CK® Framework. Der theoretische Teil basiert auf Industriestandards wie: BSI-Grundschutz Kompendium, CIS-Benchmarks, OWASP und PTES.

Im Kurs wechseln wir bei jedem Thema konsequent die Perspektive zwischen Angriff und Verteidigung. Dies befähigt die Teilnehmer, Verteidigungsmaßnahmen und Quick-Wins aus den Erfahrungen im Labor abzuleiten.

Der Kurs wird durch fortgeschrittene Themen, wie die Umgehung von Antivirus, WAFs, Intrusion-Protection-Systemen, Firewalls, Spam-Gateways, Proxy-Whitelisting, Sandboxes, EDRs und XSS-Filter abgerundet.

Erster Seminartag
- Cybersicherheitsgrundlagen (2 UE)
  - Was ist Hacking? / Was ist IT-Sicherheit?
  - Angreifertypen, Motivation und Taktiken
  - Allgemeine Begriffsdefinitionen und Metriken

- MITRE ATT&CK® Framework

- Social-Engineering (2 UE)
  - Arten von Social-Engineering
  - Beispiele aus Pentests und aktuellen Kampagnen
  - Phishing erkennen und verhindern
  - E-Mail-Angriffe, Browser-Angriffe
  - Angriffe mit Peripheriegeräten
  - Exploit vs. Social-Engineering
  - Physische Angriffe
- Infrastruktursicherheit (4 UE)
  - Einführung der Angriffskette
  - Footprinting, Discovery
  - Enumeration, Port-Scanning
  - Speicherung von Passwörtern
  - Hashingverfahren
  - Online- / Offline-Bruteforcing
  - Vor- und Nachteile von Passwortrichtlinien
  - Shells
  - Klassifizierung und Bewertung von Verwundbarkeiten
  - Command-Injections
  - Einführung in Metasploit

Zweiter Seminartag

- Linuxsicherheit | Theorie (4 UE)
  - Linux-Grundlagen
  - Linux-Exploitation
  - Lateral Movement und Pivoting
  - Post Exploitation

- Linuxsicherheit | Praxis (4 UE)
  - Fallstudien im Labor

Dritter Seminartag

- Windows-Sicherheit | Theorie und Praxis (6 UE)
  - Windows-Grundlagen
  - Active Directory-Grundlagen
  - IPS-Evasion
  - Pivoting
  - Memory Corruptions, Exploit Mitigations
  - Proxy-Whitelisting-Evasion

- Pass the Hash (PTH), Pass the Ticket (PTT)
- Kerberoasting
- Native Malware, Powershell Malware, .NET Malware, Anti-Virus-Evasion
- Spoofing Angriffe
- Exfiltration und C+C
- Client Side Exploitation
- Mimikatz, Impersonation
- Volatility, Sysinternals Tools

- Post Exploitation (2 UE)
  - Post Exploitation-Übersicht
  - Fortgeschrittene Post Exploitation
  - Native und Meterpreter Befehle für Post Exploitation
  - Living-off-the-Land-Angriffe
  - Fileless-Malware
  - Lateral Movement (RDP, WMI, WinRM, DCOM, RPC)
  - Windowshärtung
  - Keylogging

Vierter Seminartag

- Post Exploitation (1 UE)
  - Lokale Persistenz
  - AD-Persistenz (Golden Tickets, Silver Tickets)

- Defense-in-Depth (1 UE)
  - Einführung in das Konzept Defense-in-Depth
  - Die Kill-Chain und MITRE ATT&CK® Matrix
  - Basis Netzwerkverteidigung
  - Grundlagen der ISMS
  - Fortgeschrittene Netzwerkverteidigung
  - Bedrohungs-Modellierung und Schützen von Kronjuwelen
  - Aufbau und Betrieb von Security-Operation-Centern
  - Incident-Response-Richtlinien
  - Threat-Intelligence

- Ransomware (1 UE)

- Backup-Strategie
- RPO und RTO
- Recovery
- Ransomware-Schutz
- Bezahlen oder nicht?
- Entschlüsselungs-Erwägungen
- Tools

- Websicherheit (2 UE)
  - Einführung Webanwendungen, Dienste und HTTP
  - OWASP TOP 10
  - Kartografieren einer Webseite
  - Umgang mit Intercepting-Proxies
  - Umgang mit Browser-Developer-Tools
  - Web-Verwundbarkeiten serverseitig (SSRF, Command Injections, Deserialisation, SQLi, File Inclusion)
  - Web-Verwundbarkeiten browserunterstützt (XSS, XSRF, etc.)
  - Verwundbarkeiten in Web-Diensten

- Sichere Kommunikation (1 UE)
  - Verschlüsselungsgrundlagen
  - Verschiedene Kryptosuites
  - Public-Key-Infrastrukturen
  - Krypto-Härtung
  - Praktischer Einsatz von Kryptografie
  - Einführung in TLS/SSL
  - TLS/SSL Angriffe und Verteidigung
  - Festplattenverschlüsselung

- Netzwerksicherheit (1 UE)
  - Einführung Wireshark und Scapy
  - Verschiedene Arten von MITM-Angriffen
  - Sniffing und Injektion
  - Switching-Sicherheit
  - Microsegmentation
  - Wifi-Sicherheit Hauptbedrohungen

- Angriffe auf TCP/IP Stack
- TCP-,UDP,IPv4/IPv6-Bedrohungen
- Network Access Control

- Denial-of-Service (1 UE)
  - Arten von Denial-of-Service
  - Motive der Angreifer
  - Memory-Corruption-DoS
  - Fokus auf volumenbasierte DDoS
  - Verteidigung gegen Denial-of-Service
  - Incident-Response bei DoS

Wichtige Hinweise

- Das Seminarskript wird in deutscher Sprache bereitgestellt
- Die Kurssprache ist Deutsch
- Es gibt sowohl englische als auch deutsche Unterlagen (Student Guide und Lab Guide)

Administratorprivilegien werden für die Installation NICHT benötigt, ein normaler Nutzer kann die Software installieren und deinstallieren. Jedoch müssen vereinzelte TCP-Verbindungen für den Client erlaubt sein. Mit unserem Einladungsschreiben erhalten Sie zwei Links, einen fpr den Labguide und einen für den Labzugriff. bitte testen Sie vorab, ob Sie auf die URLs zugreifen können. Zu Beginn des Lehrganges bespricht der Trainer mit Ihnen die Einrichtung und Benutzung im Detail.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31490 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.