Cybersecurity, Ethical Hacking & Pentesting

mITSM Munich Institute for IT Service Management GmbH

mITSM
Wir verändern durch Wissen.

20. bis 23. April 2026 (Online-Durchführung)
10. bis 13. August 2026 (Online-Durchführung)
7. bis 10. Dezember 2026 (Online-Durchführung)

Strukturiertes Penetration Testing kennenlernen

In diesem viertägigen Kurs lernen Sie strukturierte Vorgehensweisen für das Penetration Testing kennen. In unserem ITSec Labor erleben und erlernen Sie die zielgerichteten Angriffstechniken der Hacker. Wenn Sie Techniken und Angriffspunkte von Cyberattacken kennen, sind Sie in der Lage, Schwachstellen zu erkennen und so die IT-Sicherheit in der Organisation zu stabilisieren.

Zertifizierung

Nach erfolgreicher Prüfung in Theorie und Praxis erhalten Sie das Zertifikat „ITSec Penetration Tester“.

CHF 2'490.00

Mehr Informationen und Anmeldung

Zusätzliche Infos zur Veranstaltung

Zertifikat/Bestätigung

Zertifikat

Veranstalter

mITSM Munich Institute for IT Service Management GmbH

Beschreibung

Inhalt der Schulung

- Einführung in die Cybersecurity und die Bedeutung von Ethical Hacking
- Überblick über die verschiedenen Arten von Angriffen und Schwachstellen
- Grundlagen der Netzwerktechnologie und -sicherheit
- Scanning- und Enumeration-Techniken
- Angriffsmethoden wie Denial-of-Service (DoS), Man-in-the-Middle (MitM), Social Engineering und Malware
- Grundlagen der Kryptografie und Verschlüsselung
- Prinzipien des Penetration Testings und der Penetration-Testing-Lebenszyklus
- Durchführung von Penetrationstests und Ethical Hacking-Übungen
- Berichterstattung über Sicherheitslücken und Schwachstellen und Empfehlungen zur Behebung

Zielgruppe

Es wird erwartet, dass die Teilnehmer bereits ein grundlegendes Verständnis von Netzwerk- und Informationssicherheit haben.

- IT-Administratorinnen und -Administratoren
- IT-Sicherheitsbeauftragte
- Netzwerk- und Systemingenieurinnen und -ingenieure
- Pentester
- Sicherheitsberaterinnen und -berater
- Sicherheitsanalystinnen und -analysten
- Andere IT-Fachleute, die sich für Cybersecurity und Ethical Hacking interessieren

Nutzen der Schulung

- Verbesserung des Verständnisses für Cybersecurity und Hacking
- Erwerb von Kenntnissen und Fähigkeiten im Bereich Ethical Hacking und Pentesting
- Verbesserung der Fähigkeiten zur Identifizierung von Schwachstellen und zur Durchführung von Penetrationstests
- Erhöhung der Sicherheit von IT-Systemen durch proaktive Massnahmen
- Erhöhung der Kenntnisse über aktuelle Bedrohungen und Angriffsmethoden
- Verbesserung der Fähigkeiten zur Erstellung und Umsetzung von Sicherheitsrichtlinien
- Erhöhung der Sensibilisierung für IT-Sicherheit in Unternehmen und Organisationen

Durch die Schulung erlangen Sie ein tieferes Verständnis für die Bedrohungen und Herausforderungen im Bereich der IT-Sicherheit und lernen, wie Sie diese effektiv bekämpfen können. Dies kann dazu beitragen, dass Unternehmen und Organisationen besser geschützt sind und das Risiko von

Cyberangriffen reduzieren.

Agenda

Die Weiterbildung Cybersecurity, Ethical Hacking & Pentesting dauert fünf Tage und wird mit einem entsprechenden Zertifikat abgeschlossen.

1. Tag: 9:00 bis ca. 16:30 Uhr

2. Tag: 9:00 bis ca. 16:30 Uhr

3. Tag: 9:00 bis ca. 16:30 Uhr

4. Tag: 9:00 bis ca. 16:30 Uhr (inklusive Prüfungsvorbereitung)

Kernpunkte der Schulung

- Wiederholung der Cybersecurity & Hacking Basics Inhalte
- Vorbereitung und Durchführung eines Penetrationstests
  - Organisatorische, personelle, technische und ethische Voraussetzungen
  - Wesentliche Vertragsbedingungen zwischen Penetrationstester und Auftraggeber
  - Die 5 Phasen des Penetrationstests
- Grundlagen der Kryptologie – Passwörter und Hashes knacken
- Einführung in die gängigen Werkzeuge eines Penetrationstester unter Kali Linux
  - Grundlagen im Umgang mit Tools wie Metasploit, nmap, Burp Suite, uvm.
  - Optional: Linux Grundlagen im Selbststudium über unser Online-Lab
- Penetrationstests und Angriffe auf Netwerkebene
  - Von A wie ARP Spoofing bis hin zu TCP-Session Hijacking
  - Angriffe und Ausnutzung von Schwachstellen in Diensten wie Samba, IRC oder FTP
- Penetrationstests auf Betriebssystemebene
  - Priviledge Escalation unter Linux
  - Angriffe auf Kerberos (Golden- / Silver-Ticket)
  - Backdoors unter Windows ausnutzen
  - Optional: Powershell Grundlagen im Selbststudium über unser Online-Lab
- Penetrationstest auf Applikationsebene
  - Vorstellung verschiedener Methodiken (Leitfäden) zur strukturierten Durchführung von Penetrationstests
  - Vorstellung OWASP Top 10 inkl. praktischer Übungen (SQL Injection, Cross-Site-Scripting)
  - Buffer Overflow Angriffe verstehen und anwenden
- Grundlagen des Social Engineering und Nutzung von Open-Source Intelligence (OSINT)

Zu allen Themen gibt es praxisnahe Übungen im Online Hacking Lab von TryHackme. Optional stehen noch weitere knifflige Herausforderungen bereit. In sogenannten Captuer-the-Flag-(CTF)-Übungen, können Sie das erlernte Wissen auf die Probe stellen. Sie benötigen nur ein Laptop mit aktuellem Webbrowser und Sie haben die Möglichkeit, alle Werkzeuge und vorgestellten Angriffe gefahrlos auszuprobieren. Auch noch nach dem Kurs behalten Sie den Zugang zum Online Lab. Manche der Übungen erfordern allerdings eine kostenpflichtige Mitgliedschaft, die Sie aber im Rahmen der Schulung für einen Monat kostenlos zur Verfügung gestellt bekommen.

Mehr Informationen und Anmeldung