Ethical Hacking Essentials.

Einführung in die Themen Ethical Hacking und Penetration-Testing.

Seminar	Zurzeit keine Termine	Teilnahmebescheinigung
Präsenz / Virtual Classroom	16 Unterrichtseinheiten	

Seminarnummer: 31774

Stand: 21.11.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31774

"Ethical Hacking Essentials" ist ein Einführungskurs in die Cybersicherheit, der grundlegende Aspekte des Ethical Hackings sowie des Penetrationstests abdeckt und die Teilnehmer auf eine Karriere in der Cybersicherheitsbranche vorbereitet. Dieser Kurs vermittelt den Lernenden Konzepte der Computer- und Netzwerksicherheit, wie z.B. Bedrohungen und Schwachstellen, Passwort-Cracking, Angriffe auf Webanwendungen, Angriffe auf IoT und OT, Cloud Computing, Grundlagen des Penetrationstests und vieles mehr.

Nutzen

- Grundlegende Herausforderungen in der Welt der Informationssicherheit sowie Gesetze und Standards der Informationssicherheit
- Grundlagen des Ethical Hacking
- Bedrohungen und Schwachstellen in der Informationssicherheit
- Verschiedene Arten von Malware
- Verschiedene Techniken zum Knacken von Passwörtern und Gegenmaßnahmen
- Social-Engineering-Techniken, Insider-Bedrohungen, Identitätsdiebstahl und Gegenmaßnahmen
- Angriffe auf Netzwerkebene (Sniffing, Denial-of-Service und Session Hijacking) und Gegenmaßnahmen
- Angriffe auf Anwendungsebene (Webserver-Angriffe, Angriffe auf Webanwendungen und SQL-Injection) und Gegenmaßnahmen
- Verschlüsselung in drahtlosen Netzwerken, Bedrohungen für drahtlose Netzwerke und Gegenmaßnahmen
- Angriffsvektoren auf mobilen Plattformen, Verwaltung mobiler Geräte, Sicherheitsrichtlinien für mobile Geräte und Sicherheitstools
- Konzepte, Angriffe und Gegenmaßnahmen im Bereich IoT (Internet of Things) und OT (Operational Technology)

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- Cloud-Computing-Technologien, Bedrohungen und Angriffe im Cloud-Computing sowie Sicherheitstechniken
- Grundlagen von Penetrationstests

Zielgruppe

- Studenten, junge Absolventen, Berufstätige, Karriereeinsteiger und -wechsler sowie IT-/Technologie-/Cybersicherheitsteams mit wenig oder keiner Berufserfahrung.
- Jeder, der seine Karriere im Bereich Cybersicherheit starten und die Grundlagen der Online-Sicherheit beherrschen möchte.
- Jeder, der sich auf eine Karriere in der Cybersicherheit vorbereiten und seine IT-Ausbildung unterstützen möchte.
- Fachleute, die in den Bereich der Cybersicherheit einsteigen möchten, aber unsicher sind, wo sie ihre Ausbildung beginnen sollen.

Voraussetzungen

Die Kursunterlagen stehen ausschließlich in englischer Sprache zur Verfügung. Daher empfehlen wir solide Englischkenntnisse aus dem IT-Umfeld.

Inhalte des Seminars

Modul 01: Information Security Fundamentals

Modul 02: Ethical Hacking Fundamentals

Modul 03: Information Security Threats & Vulnerability Assessment

Modul 04: Password Cracking Techniques & Countermeasures

Modul 05: Social Engineering Techniques & Countermeasures

Modul 06: Network Level attacks & Countermeasures

Modul 07: Web application & Countermeasures

Modul 08: Wireless Attacks Countermeasures

Modul 09: Mobile Attacks & Countermeasures

Modul 10: IoT + OT Attacks & Countermeasures

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Modul 11: Cloud Computing threats & Countermeasures

Modul 12: Penetration Testing & Countermeasures

Wichtige Hinweise

Der Kurs wird in deutscher Sprache gehalten.

Die Kursunterlagen werden in englischer Sprache zur Verfügung gestellt.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31774 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.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.