Zielgruppe

IT-Sicherheitsbeauftragte und Systemadministratoren. Dieses Seminar richtet sich an Teilnehmer, die selbst keine Hacker im eigentlichen Sinne sind, aber die Methoden der Eindringlinge kennenlernen wollen, um die eigene EDV auf Schwachstellen zu testen und zu optimieren.

Verpflichtungserklärung

Vor Kursantritt unterzeichnen die Teilnehmenden eine Erklärung, mit welcher sie sich verpflichten, die neu erworbenen Fähigkeiten keinesfalls für illegale oder böswillige Angriffe zu verwenden und diese auch keinesfalls einsetzen werden, um Computersysteme zu schädigen.

Dauer / Termin

5 Tage. Bitte erfragen Sie den nächsten Starttermin bei uns unter 04421/9785-0 oder informieren Sie sich unter **www.tbg-schortens.de**.

Lehrgangsgebühren

Dieser Zertifizierungsworkshop bietet ein erstklassiges technisches Training nach EC Council Konzept und eine Zertifikatsvorbereitung. Die Investition beträgt 3 200 € plus MwSt. und und beinhaltet den Zugang zu den aktuellsten CEH v10-Kursmaterialien und einen Prüfungsgutschein 312-50 v10.

Testcenter direkt vor Ort!

Die Seminarabsolventen können die CEH-Zertifizierungsprüfung direkt im Testcenter der TBG vor Ort ablegen!

Zu schulen ist seit über 25 Jahren unsere Lieblingsbeschäftigung!

Und es gelingt uns immer wieder Trainer-Koryphäen für Spezialthemen zu engagieren: wie z.B. für Datenbanken & Exchange, Virtualisierung, Sharepoint, Citrix, VMware, Linux uvm.

Nutzen Sie die Gelegenheit und informieren Sie sich bei uns!
04421/9785-0 oder www.tbg-schortens.de

TBG Technologie & Bildung GmbH

Olympiastraße 1, Gebäude 1 (TCN Tor 2) in 26419 Schortens
Telefon: (0 44 21) 97 85-0, tbg@tbg-schortens.de

Microsoft Partner

CompTIA AUTHORIZED PARTNER

TÜVRheinland ZERTIFIZIERT
ISO 9001:2008 Zugelassener Träger nach §2 AZAV
www.tuv.com ID 9105037446

Das Seminar für Sicherheitsexperten: CEHv10 – Certified Ethical Hacker

TBG Technologie & Bildung GmbH

C|EH™ Certified Ethical Hacker

Certified Ethical Hacker

Neue Version!

Stand 08/18

Sie glauben, dass Ihr IT-Netzwerk optimal gesichert ist????

Spionage, Sabotage, Datendiebstahl:
Der deutschen Wirtschaft entsteht jährlich ein Schaden von 55 Milliarden Euro!

Jedes zweite Unternehmen wurde in den vergangenen beiden Jahren angegriffen und nur jedes dritte Unternehmen meldet Attacken, denn die Sorge vor Imageschäden schreckt ab...

Nach dem Besuch dieses Kurses werden die Teilnehmenden die Sicherheit ihres Netzwerkes in einem ganz anderen Licht sehen und haben nicht nur gelernt, die Schwachstellen ihres Netzwerks zu erkennen, sondern es auch optimal gegen Angriffe zu sichern!

Um einen Dieb zu fangen, muss man wie ein Dieb denken!

EC-Council

EC Council ist eine Organisation von Sicherheitsexperten, die von Mitgliedern der Geschäftsführung von Unternehmen wie Microsoft, Cisco Systems, Hewlett Packard, Oracle, Symantec und vielen anderen gegründet wurde. EC Council bietet herstellerunabhängige Workshops und Zertifizierungen im Bereich Security an.

Die CEH v10 Seminarinhalte reichen von digitalen Fußspuren (Footprinting) über Trojaner & Viren, Hintertüren im System (Backdoors), Übernahme von Webservern und -applikationen (Hijacking), WLAN-Hacking und Verschlüsselung (Cryptography) bis zum simulierten Angriff (Penetration Testing).

Die Absolventen sind nach dem Kurs in der Lage, Gefahren zu erkennen und IT-Systeme möglichst „wasserdicht" zu sichern.

Das sind die Neuerungen im praxisorientierten CEHv10 - Certified Ethical Hacker-Seminar:

Neues Modul zur Internet of Things (IoT) Sicherheit

Als Reaktion auf die wachsende Sicherheitsbedrohung durch ungesicherte IoT Geräte und entsprechende Hackerangriffe, wie den Mirai-Botnet Angriff in 2017, führt CEH v10 ein neues Modul zur Internet of Things (IoT) Sicherheit ein. Abgedeckt werden Kenntnisse, die zum Testen, Einsatz und Management der Sicherheit von IoT Geräten notwendig sind.

Upgrade der Materialien zum Vulnerability Assessment

Die Beurteilung von Schwachstellen ist ein kritisches Element im Hacking Lifecycle - im CEH v10 wird daher die Anwendung von Schwachstellenanalysen in Real-World Umgebungen vertieft. Es werden Hacker-Tools zum Zugriff auf Systeme behandelt und vermittelt, wie Schwachstellen behoben werden können.

Cloud Angriffsvektoren, AI und Machine Learning

Der Fokus auf die sicherheitsrelevanten Bereiche Cloud Technologien, Künstliche Intelligenz (AI) und Machine Learning wird erhöht. Der CEH v10 integriert außerdem einen Malware-Analyseprozess zur Beurteilung der Funktion, Herkunft und Auswirkungen von Malware.

Im Kurs verwenden die Teilnehmenden eine interaktive Hacking-Umgebung und erlangen die Kenntnisse, die eigenen Systeme zu scannen, zu testen, zu hacken und zu sichern. Sie lernen, die gleichen Attacken auszuführen wie ein Hacker mit kriminellen Absichten - und erfahren so, wie sie sich gegen verschiedene Arten von Cyberbedrohungen verteidigen können:

- ✓ Trojaner, Viren und Würmer
- ✓ SQL Injection
- ✓ MAC und DHCP Attacken
- ✓ Direct-Denial-of-Service (DDoS) Attacken