CompTIA PenTest+ - úvod do penetračného testovania

Kód kurzu: CTPEN

Kurz je určený bezpečnostným špecialistom a administrátorom, ktorí chcú začať s penetračným testovaním alebo chcú poznať problematiku penetračného testovania a zoznámiť sa s postupmi, ktoré používajú etickí hackeri pri penetračných testoch. Kurz je určený aj tým administrátorom, ktorí neplánujú vykonávať penetračné testy, ale chcú veci vidieť aj z druhej strany, aby lepšie chápali opatrenia, ktoré by mali prijímať pri zvyšovaní miery zabezpečenia svojich sietí. Kurz je zároveň prípravou na certifikačnú skúšku CompTIA PenTest+ (nie je súčasťou kurzu).

Pre koho je kurz určený

Najnovšia verzia 5-dňového kurzu CompTIA PenTest+ je súčasťou prípravy na celosvetovo uznávanú certifikačnú skúšku CompTIA PenTest+ (PT0-003), ktorá je dnes štandardom v kybernetickej bezpečnosti. Certifikát PenTest+ je, okrem iného, v súlade s normou ISO 17024 a schválený ministerstvom obrany USA. Certifikácie poskytované spoločnosťou CompTIA sú čoraz populárnejšie aj v Európe.

Veľkou výhodou všetkých kurzov od poskytovateľa certifikácie CompTIA je, že účastníci majú k dispozícii virtuálne prostredie pre praktické cvičenia súvisiace s kurzom. Kurz zahŕňa až 28 labov, kde si účastníci vyskúšajú rôzne nástroje a postupy pri penetračnom testovaní. Laby sú k dispozícii až 1 rok a každý z nich je možné opakovať neobmedzený počet krát. V laboratóriách si účastníci vyskúšajú desiatky nástrojov a postupov používaných pri penetračnom testovaní. Účastníci získajú komplexný prehľad o tom, ako fungujú penetračné testy. Dozvedia sa o jednotlivých fázach penetračného testovania, aké nástroje a postupy použiť a na aký účel.

Pre koho je kurz určený?

Kurz je úvodom do problematiky a je určený pre každého, kto chce vedieť, čo robia penetrační testeri alebo chcú sami vykonávať penetračné testy.

Kurz je určený pre administrátorov a bezpečnostných administrátorov, ktorí chcú vedieť, ako sa penetračné testy vykonávajú, alebo plánujú vykonávať penetračné testy sami. Je určený aj pre členov prevažne "červených tímov", ale výrazne pomôže aj druhej strane, "modrým tímom", lepšie pochopiť, čo sa deje na "druhej strane" v prípade útoku. Kurz je určený pre každého, kto sa chce dozvedieť o etickom hackingu.

Čo vás naučíme

V kurze sa naučíte, ako vykonať penetračný test podľa odporúčaných postupov. Teoretické vysvetlenie a množstvo praktických cvičení vás zoznámia s penetračným testovaním. Naučíte sa používať rôzne nástroje a postupy pri testovaní.

Požadované vstupné znalosti

Účastníci by mali mať znalosti na úrovni certifikácie CompTIA Network+, CompTIA Security+ alebo ekvivalentné praktické skúsenosti so správou sietí a operačných systémov.

Študijné materiály

Okrem laboratórneho prostredia získajú účastníci aj ročný prístup k študijným materiálom, ktoré zahŕňajú elektronickú knihu, niekoľko videí, sady otázok a odpovedí na každú tému a simuláciu certifikačnej skúšky v reálnom svete.

Osnova kurzu

- Penetration Testing: Before You Begin
- Professional Conduct and Penetration Testing
- Collaboration and Communication
- Testing Framework and Methodologies

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Introduction to Scripting for Penetration Testing
- Applying Pre-Engagement Activities
- Define the Scope
- Compare Types of Assessments
- Utilize the Shared Responsibility Model
- Identify Legal and Ethical Considerations
- Reconnaissance and Enumeration
- Information Gathering Techniques
- Host and Service Discovery Techniques
- Enumeration for Attack Planning
- Enumeration for Specific Assets
- Scanning and Identifying Vulnerabilities
- Vulnerability Discovery Techniques
- Analyzing Reconnaissance Scanning and Enumeration
- Physical Security Concepts
- Conducting Pentest Attacks
- Prepare and Prioritize Attacks
- Scripting Automation
- Web-Based Attacks
- Web-Based Attacks
- Cloud-Based Attacks
- Enterprise Attacks
- Perform Network Attacks
- Perform Authentication Attacks
- Perform Host-Based Attacks
- Specialized Attacks
- Wireless Attacks
- Social Engineering Attacks
- Specialized System Attacks
- Performing Penetration Testing Tasks
- Establish and Maintain Persistence
- Move Laterally through Environments
- Staging and Exfiltration
- Cleanup and Restoration
- Reporting and Recommendations
- Penetration Test Report Components
- Analyze Findings and Remediation Recommendations

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk