CompTIA

PUBLIC SECTOR NETWORK

Certified B Corporation

CompTIA PenTest+ Certification Course

TRAINING

Secure Your Future: Elevate Your Career

Online

Monday - Friday, November 18 - 22, 2024 | 9AM - 5PM EST

Overview

In an age where cyber threats evolve with alarming speed, the ability to not only defend but proactively attack these threats through ethical hacking and penetration testing has become invaluable. The CompTIA PenTest+ certification empowers IT professionals with the advanced skills and knowledge needed to conduct effective penetration testing and vulnerability assessment across a variety of systems, all while ensuring the resilience of networks against cyber threats.

Designed to bridge the gap between foundational cybersecurity knowledge and the hands-on application of penetration testing skills, CompTIA PenTest+ equips candidates with the ability to identify, exploit, report, and manage vulnerabilities on a network. This certification goes beyond traditional penetration testing to include management skills necessary for planning, scoping, and managing weaknesses, not just exploiting them.

Key aspects covered in the PenTest+ certification include understanding legal and compliance requirements, conducting penetration tests and vulnerability assessments using the latest tools and techniques, and effectively communicating findings to stakeholders. PenTest+ prepares cybersecurity professionals to step into roles that directly influence the protection and defence mechanisms of their organisations.

Earning the CompTIA PenTest+ certification positions you as a leader in the cybersecurity field, capable of addressing complex security vulnerabilities with proficiency and confidence. Whether you're aspiring to become a penetration tester, security consultant, or any role requiring deep security knowledge, PenTest+ is your next step towards mastering the art of ethical hacking and network defence.

Who Attends

Advisor, Principal, Consultant, Lead and Officers of:

- Security consultant
- Cloud security specialist
- Network & security specialist
- Information security engineer
- Security analyst
- Cyber security engineer
- Application security engineer
- Cyber security operations analyst
- Technology security
- Cyber protective security
- Cyber security response

Skills You Will Learn

Planning and Scoping: updated techniques emphasising governance, risk, and compliance concepts, scoping and organisational/customer requirements, and demonstrating an ethical hacking mindset.

Information Gathering and Vulnerability Scanning: performing vulnerability scanning and passive/active reconnaissance, vulnerability management, as well as analysing the results of the reconnaissance exercise.

Attacks and Exploits: approaches to expanded attack surfaces, researching social engineering techniques, performing network attacks, wireless attacks, application-based attacks and attacks on cloud technologies, and performing post-exploitation techniques.

Reporting and Communication: the importance of reporting and communication in an increased regulatory environment during the pen testing process through analysing findings and recommending appropriate remediation within a report.

Tools and Code Analysis: concepts of identifying scripts in various software deployments, analysing a script or code sample, and explaining use cases of various tools used during the phases of a penetration test–scripting or coding is not required.

Explore the Key Sessions

This program will be delivered across 5 days from November 18 - 22, 2024, 9am to 5pm EST with breaks for morning tea, lunch and afternoon tea.

CompTIA PenTest+ Modules Breakdown:

Planning and Scoping

- Understand legal and regulatory implications to ensure compliance during penetration testing.
- Define the scope and objectives of penetration tests, including identifying key stakeholders and establishing communication protocols.
- Evaluate governance, risk, and compliance (GRC) concepts relevant to penetration testing and organisational security.
- Demonstrate an ethical hacking mindset with a focus on integrity, confidentiality, and availability of data.
- Prepare engagement contracts that define the boundaries and limitations of the penetration test.

Information Gathering and Vulnerability Scanning

- Perform passive and active reconnaissance to gather information on targets without being detected.
- Utilise various vulnerability scanning tools and techniques to identify vulnerabilities within systems and networks.
- Analyse the output from reconnaissance and vulnerability scans to prioritise targets for further exploitation.
- Understand the role of vulnerability management programs in identifying and mitigating vulnerabilities.
- Conduct social engineering tests to gather additional information or gain access to systems.

Attacks and Exploits

- Execute network-based attacks, including exploiting misconfigurations and vulnerabilities in network services.
- Conduct wireless and application-based attacks to penetrate Wi-Fi networks and web applications.
- Utilise social engineering techniques for manipulation and gaining unauthorised access.
- Perform post-exploitation techniques to maintain access, escalate privileges, and gather more sensitive information.
- Explore vulnerabilities in cloud technologies and execute attacks tailored to cloud-based environments.

Pricing for Public Courses

Early Bird 1	Early Bird 2	Standard
$2,590 CAD	$2,790 CAD	$2,990 CAD

Reporting and Communication

- Analyse penetration testing findings to identify critical vulnerabilities and the impact on the organisation.
- Develop comprehensive penetration testing reports that detail the findings, methodologies, and outcomes of the test.
- Communicate effectively with stakeholders, including technical staff and senior management, to explain the risks and necessary remediations.
- Recommend remediation strategies for identified vulnerabilities to improve the organisation's security posture.
- Address legal and compliance issues in reports to ensure the organisation understands its regulatory obligations.

Tools and Code Analysis

- Identify and use various tools and technologies throughout the phases of a penetration test, including reconnaissance, scanning, exploitation, and post-exploitation.
- Analyse scripts and code samples for malicious content or vulnerabilities that could be exploited.
- Understand the applications and limitations of penetration testing tools to select the most effective ones for each phase of the test.
- Explain the use cases for scripting in automation of tasks during a penetration test.
- Evaluate the security of scripts and coded applications as part of the overall security assessment of an organisation.