CERTIFIED PENETRATION TESTER

CPT

Duration: 5 days; Instructor-led | Virtual Instructor-led

WHAT WILL YOU LEARN

Certified Penetration Tester is a hands-on deep-dive training and certification programme that enables the participants to handle vulnerability assessments and penetration tests for their customers.

- Understand all Latest Attacks and their entry points
- Learn how to conduct vulnerability assessment on networks and systems
- Learn ways to harden networks and systems therefore securing corporate infrastructures
- Learn exploit techniques on Network, Web, WiFi, and Mobile infrastructure
- Prepare and submit Vulnerability Assessment & Pentest reports

OBJECTIVES

- To understand different attacks used by hackers
- To learn how to conduct a vulnerability assessment on the network and systems
- To learn ways to harden the network and systems thus securing the corporate network and systems.
- To prepare and submit Vulnerability
- Assessment & Pentest Reports

PREREQUISITES

A ready-to-learn attitude is a must, and an analytical mind is definitely a huge plus. Network and IT Software systems background would be an advantage.

AUDIENCE

- Network administrators
- Network executives
- Security professionals who insterested in conducting vulnerability assessment and penetration test for their customers.

COURSE CONTENTS

Module 1: Introduction to Vulnerability Assessment & Penetration Testing

- Basics: Vulnerability, Exploit, Payload, Listener, Vulnerability Assessment Vs. Penetration Testing, Types of Vulnerabilities, Vulnerability Research Sources for Penetration Testers, Exploits and tools sources for Penetration Testers, Commercial Tools for Penetration Testers, Penetration Testing Methodologies and Penetration Test Report Template

Module 2: Information Intelligence Techniques

- Passive Information Gathering
- Information intelligence and Map the Customer organization with Maltego
- Information intelligence and Map the infrastructure with FOCA
- Open Source intelligence OSINT on the organisation and its people

Module 3: Scanning & Vulnerability Assessment

- Scanning Types & Scan Options
- NMap Scanning
- NeXpose : Vulnerability Scanning & Reporting
- Network scanning using Rumble
- Multiple scanning techniques and Tools

Module 4: Cracking & Social Engineering

- MiTM Concepts & Attacks
- Password Cracking with tons of powerful tools
- Social Engineering Attacks : Bashbunny, Java Applet Attack Vectors, Infectious Media Generator, Credential Harvester Attack Method, Spear-Phishing Attack Method and many more

Module 5: Exploitation & Pentest

- Metasploit Framework Concepts
- Metasploit Exploitations : Armitage, Dump Password Hash, Capture Screenshots, Capture Keystrokes, Privilege Escalation, Pivoting, ARP Scan, Stdapi and Priv, Persistence and Backdoors (Maintaining Access), Cover Tracks, Post Exploitations.
- Anti-Virus Evasion Frameworks and various techniques
- Pentest Tools Framework (PTF)
- Image Exploitation via Whatsapp
- Netcat Exploitations
- Backdoor using msfvenom & Netcat
- Advanced Exploitations using PowerShell
- Mobile Exploitations
- Rapid 7 Metasploit Pro
- Pentest Reporting

Module 6: PowerShell Exploitation

- PowerShell Basics
- PowerShell Log Analysis

GemRain Consulting Sdn Bhd.
33-5.6, Block C, Jaya One, Jalan Profesor Diraja Ungku Aziz, 46200 Petaling Jaya, Selangor, Malaysia
Contact: (+60)3 7931 3036 | (+60)12 613 3667 | Email: enquiry@gemrain.net | Website: www.gemrain.net

- PowerShell Malwares evading Antivirus and End Point Defenses

Module 7: Web Pentest

- Web Application Basics,
- Web Application Fingerprinting,
- Payment Gateway & Order Tampering,
- Labs on OWASP TOP 10 Vulnerabilities and its sub categories using Mutillidae, DVWA
    - [SQL Injection, Cross Site Scripting, Cross Site Request Forgery, LDAP Injection, Command Injection, Parameter/Form Tampering, Payment Gateway hacking, Improper Error Handling, Directory Traversal, Insecure storage, Information Leakage, Broken Account Management, Denial of Service, Buffer Overflow, Broken Session Management, Session Fixation, Security Misconfiguration, File Upload and Download and many more]
- Pentest Reporting
- Tools Covered : Acunetix, Nexpose, Burp Suite, Kali Linux and tons of scripts

Module 8: Wireless Pentest

- Introduction on WEP, WPA, WPA2
- Wireless cracking with Reaver
- Wireless cracking with Wifi Pineapple
- Uncovering hidden SSIDs
- More Wifi attacks