CyberSecurity MALAYSIA

MINISTRY OF DIGITAL

CYBERTRONIUM

Certification

Certified Penetration Tester is 5 days hands-on training and certification programmes that enable the participants handle the vulnerability assessment and penetration test for their customers.

Terminal 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

Target Participants

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

Accredited by:

GLOBAL ACE CERTIFICATION

Certified Penetration Tester (CPT)

Certified Examination

The CPT examination is certified by the Global ACE Certification. The examination framework is designed to align with a set of relevant Knowledge, Skills and Attitudes (KSA) that are necessary for an Information Security Awareness Manager. Candidates will be tested via a combination of either continual assessment (CA), multiple choice (MC), theory/ underpinning knowledge assessment (UK), practical assessment (PA), assignments (AS) and case studies (CS) as required.

Candidates can take the examination at authorized examination centres in participating scheme member countries. Candidates who have successfully passed the CPT examination will be eligible to apply as an associate or professional member by fulfilling the membership criteria defined under the Global ACE Scheme.

Program Outline

1. Introduction to Vulnerability Assessment & Penetration Testing

- 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
- Latest Attacks – Demos

2. Information Intelligence Techniques

- Passive Information Gathering
- Information intelligence and Map the Customer organization
- Information intelligence and Map the infrastructure of the Target

3. Scanning & Vulnerability Assessment

- Scanning Types & Scan Options
- NMap Scanning
  - Ninja & Non-Ninja Scan types
  - Multiple IP Addresses scanning
  - Host Discovery
  - Ping & Port Scanning
  - OS Fingerprinting & Service Enumerations
  - NMap Scripts
  - Host Scanning : Bypassing Firewalls
  - Decoys
- ZenMap
- Netcat Fingerprinting
- Nessus : Vulnerability Scanning & Reporting
- NeXpose : Vulnerability Scanning & Reporting
- OpenVAS

4. Cracking & Social Engineering

- MiTM Concepts & Attacks
- Password Cracking
  - Brute Force Tools : Hydra, Medusa
  - Crunch Password generator
  - FTP Credential cracking
  - Telnet Brute Force
  - SSH Login Brute Force Attack
  - Password cracking with John the Ripper
- Social Engineering Attacks : Java Applet Attack Vectors, Infectious Media Generator, Credential Harvester Attack Method, Spear-Phishing Attack Method and many more

5. Exploitation & Pentest

- Metasploit Framework Concepts
- Metasploit Community & Armitage
- Metasploit Exploitations : 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 Framework and Methods
- Netcat Exploitations
- Backdoor using msfvenom & Netcat
- Advanced Exploitations using PowerShell
- USB Based exploitation on Win 7 & Win 10
- Pentest Reporting

6. PowerShell Exploitation

- PowerShell Basics
- PowerShell Log Analysis
- PowerShell Malwares to evade Defenses

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, Informa- tion Leakage, Broken Account Management, Denial of Service, Buffer Overflow, Broken Session Management, Session Fixation, Security Misconfigura- tion, File Upload and Download and many more]
- Pentest Reporting

8. Wireless Pentest

- Introduction on WEP, WPA, WPA2
- Wireless cracking with Reaver
- Uncovering hidden SSIDs
- WiFi Twining Attacks
- WiFi Pineapple based attacks

CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia

Tel: +603 8800 7999 **Fax:** +603 8008 7000
Email: info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
Website: www.cybersecurity.my