CyberSecurity MALAYSIA

MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

nexagate

NETWORK PENETRATION TESTING AND DEFENSE FOR SYSTEM & NETWORK ADMINISTRATORS

This course introduces network penetration testing techniques and mechanism/tools to defend against it.

FEE : RM3,500.00
(subject to 6% SST)

TARGET PARTICIPANTS

Network Administrators, System Administrator, Blue team, Red Team

OBJECTIVE

1. Understand the definition, scope, purpose and the benefits from network penetration testing.
2. Understand different techniques to approach the network via network penetration testing.
3. Learn mechanisms and methods on how to protect the network and perform hardening to avoid from the attacks..
4. Hands-on experience via interacting with the relevant tools.

AGENDA

Module 1: Overview of Penetration Testing

- Introduction
- Methodology
- Type of penetration Testing

Module 2: Target Enumerations and Port Scanning

- Host Discovery
- Scanning for open ports
- Identifying running Services
- OS Detection
- Various port-scanning techniques

Module 3: Vulnerability Assessment

- Introduction
- Vulnerability Assessment with NMAP
- Vulnerability Assessment with Nessus

Module 4: Penetration testing with Metasploit

- Introduction
- Searching for exploits
- Exploiting windows with Metasploit
- Exploiting linux with Metasploit

Module 5: Password Cracking

- Introduction
- Types of password cracking techniques
- Password cracking with Hydra
- Generating custom password dictionaries

GET IN TOUCH

☎ 03 - 8800 7999 ✉ training@cybersecurity.my ⌂ www.cyberguru.my