

System and Web Penetration Testing

Duration 4 Days

COURSE DESCRIPTION

This course provides penetration techniques to examine system and web applications.

COURSE OBJECTIVE

After completed this course, the participants will be able to

- understand techniques and tools for gathering useful information of system and web application
- understand the vulnerability assessment and exploitation process of system and web application
- understand web application protocol and technology, and how to identify vulnerability
- understand attacking techniques in web application

COURSE OUTLINE

- Information Gathering, OSINT, Vulnerability Assessment, System Exploitation, Password Cracking Techniques and Tools, Privilege Escalation Techniques, System Backdoor, Mobile Payload, Lab Exercises and Challenges.
- Web Application Protocol and Technology, Web Vulnerability Identification, OWASP Top 10 Web Application Vulnerabilities such as Command Injection, SQL Injection, Broken Authentication and Authorization, Cross-site Scripting (XSS) and Cross-site Request Forgery (CSRF), XML External Entity (XXE), Web Backdoor and Payload, Lab Exercises and Challenges.

PREREQUISITES

- General knowledge of computer and network system.
- Some experience in computer programming languages.
- Background in network and security tools such as nmap, Burp suite.
- Some basic of Linux command.

WHO SHOULD ATTEND

A system administrator, a security analyst, and an IT auditor with some background in conducting system vulnerability assessment, computer and network security, network protocols, and web services and applications

SKILL LEVEL

Intermediate.