INFOSECTRAIN

# Advanced Penetration Testing

## Course Agenda

sales@infosectrain.com | www.infosectrain.com

## Course Objectives

- Introduction to Linux
- Intelligence Gathering
- Scanning and Enumeration
- What is hashing?
- Scripting
- Exploitation
- The Metasploit Framework
- Post -Exploitation
- Wireless Exploitation and Wireless auditing
- Web Application Penetration Testing
- Data Collection ,Evidence Management and Reporting

## Introduction to Linux

- Installing Linux distribution for Pen testing
- Configuring Distribution
- Introduction to Bash Environment

  a. Intro to Bash Scripting

  Practical bash usage - Example 1

  Practical bash usage - Example 2

## Intelligence Gathering

- Online Sources
- Active Information Gathering

## Scanning and Enumeration

- SMB Enumeration
- SMTP Enumeration
- SNMP Enumeration
- FTP Enumeration
- Retina
- Open-Vas
- Nessus
- Nikto

## What is hashing?

- Hashing Concepts
- Kerberos Authentication
- Windows, Linux cracking
- Reverse Hashing

## Scripting

## Exploitation

- Windows and Linux
- Using Custom Exploits
- Buffer Overflows

## The Metasploit Framework

a. Setting up Metasploit

Exploring the Metasploit Framework

Using Metasploit Auxiliary

b. Using Exploits Modules

c. Exercises

### Metasploit Payloads

a. Staged and Non-staged Payloads

b. Working with Meterpreter Session

c. Working with Multi Handler

d. Executable Payloads

e. Exercises

## Post-Exploitation

- System command Privilege Escalation
- Configuration files
- Sudors priviledge
- Kernel exploits
- Backdoor
- Linux post Exploitation
- Windows post Exploitation

## Wireless Exploitation and Wireless auditing

- Introduction to Wireless Security
- Cracking Wireless Encryptions
- Cracking WEP
- Cracking WPA and WPA2
- WIFI-Phishing
- Halting Wireless Network Through Dos Attack
- Restricting Wireless Access Through Wireless Jammer
- Securing Wireless Access Points
- Auditing and Reporting

## Web Application Penetration Testing

- Introduction to Web Application Vulnerabilities
- Introduction to BurpSuite Proxy
- Cross Site Scripting (XSS)
- IFRAME Injection
- Cookie Stealing
- Session Hijacking
- Cross Site Request Forgery (CSRF)
- LFI and RFI
- Hacking database using SQL injection
- Enumerating Database
- SQL Injection with Automated Tools
- Web Application Assessment and Exploitation with Automated Tools
- DOS Attack

## Data Collection ,Evidence Management and Reporting

- Type of Report
- Presentation Report
- Post Testing Procedure

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com