INFOSECTRAIN

# ADVANCED
## PENETRATION TESTING
## TRAINING COURSE

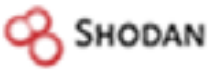
# COURSE DESCRIPTION

The Advanced Penetration Testing with Kali Linux is an all-embracing course that expertly explains to optimize Kali Linux and its powerful tools for advanced wired and wireless networks and mobile security. The course focuses to demonstrate advanced techniques to perform penetration testing. You learn to use Metasploit Framework and practices used in exploiting Windows and Unixplatforms. Vulnerability scanningforms an integral part of this comprehensive training and demonstrates how a system is targeted and exploited. The training also empowers you with detailed understanding of diverse post-exploitation techniques and modernistic techniques to evade antivirus while understanding the customization of attacks.

# TOOLS COVERED

INFOSECTRAIN























INFOSECTRAIN

# WHY ADVANCED PENETRATION TESTING TRAINING ?

## The advanced penetration testing training course helps you gain upper hand in:

- Setting up lab and installing Kali Linux
- Understanding types of reconnaissance including active and passive
- Analyzing vulnerabilities and using SSL Scan to fetch SSL and TLS information
- Finding vulnerabilities with automated scanners
- Understanding core fundamentals of exploitation
- Understanding how to exploit Windows and Unix vulnerable services
- Understanding how to perform DNS spoofing, redirecting traffic and maintaining access
- Using PINGtunnel and HTTPtunnel for protocol spoofing
- Understanding client side attacks and social engineering
- Managing network security and securing traffic
- Working with various security tools
- Setting up and hacking a wireless network

  Hacking of mobile platforms
- Mitigating OWASP vulnerabilities
- Perform penetration testing and documenting reports

# COURSE OBJECTIVES

INFOSECTRAIN

This advanced Penetration training imbibes across the board understanding of:

- Kali Linux installation with lab setup
- Reconnaissance types
- Vulnerabilityanalysis, classification, and identification
- Monitoring the network security with Security Onion
- Vulnerability scanning using OWASP ZAP, w3af, Wapiti, Vega scanner, Metasploit's Wmap and using Lynis for hardening
- SQLMap, Metasploit, Tomcat Manager and other tools to find exploitation and attacks
- Advanced level exploitation
- Exploiting vulnerable services in Windows and Unix
- Spoofing, spinning and access maintenance
- Social engineering and BeFF
- Implementing network security
- Security tools including Squid proxy, Port Sentry, Network Security Toolkit (NST), OSSEC, Tripwire and many more
- Denial of Service (DoS) attacks and wireless network hacks
- Mobile platform hacking
- Top vulnerabilities of OWASP and mitigation
- Report writing and pen testing process

# TARGET AUDIENCE

INFOSECTRAIN

- Middleand advance level penetration testers
- Security enthusiasts
- Aspiring penetration testers pen-testing
- Compliance based penetration testing

## PRE- REQUISITES

- Basic understanding of networking and servers
- Understanding of a programming language like Python recommended

# COURSE CONTENT

# NETWORK AND SYSTEM SECURITY TESTING

## Linux for Testing

- The Linux Filesystem
- Basic Linux Commands
- Finding Files in Linux
- Managing Linux Services
- Searching, Installing, and Removing Tools
- The Bash Environment
- Piping and Redirection
- Text Searching and Manipulation
- Background Processes (bg)
- Jobs Control
- Process Control
- File and Command Monitoring
- Downloading Files
- Persistent Bash Customization

# Scripting for Pen-Testers

## Introduction to Shell

- Script Basics
- Global Declarations
- Variable basics
- Escape characters
- Basic redirection and pipe
- Understanding Conditions
- Understanding Loops
- Recursion and Nested Functions
- Function Attributes
- The Linux Execution Environment with Scripts
- Restricted Shells

## Introduction to Python

- What is Python?
- Python: Favourite of Hackers
- Data Types and variables
- Control Flow and Data structure
- Functions, Functional Programming and File Handling
- Exception Handling
- Creating Managing File and Directory Access
- Raw Socket basics
- Socket Programming with Python

- Servers and Clients architecture
- Creating Sniffers (wired and wireless)
- Creating packet injector

## Introduction to Pen-Testing

- Penetration Testing Benefits
- Types of  Penetration Testing
- Penetration Testing  Methodologies
- Law & Compliance
- Planning, Managing & Reporting

## OSINT & Analysis

- Foundation of OSINT
- Goals of OSINT Collection
- Core OSINT Skills
- Leveraging Search Engines
- File Metadata Analysis
- Reverse Image Searching
- OSINT for Business
- People Investigations
- SOCMINT
- Finding Email Addresses
- Domain & IP Investigations
- Dark Web OSINT
- What is TOR?
- Capture the Flag Exercises for OSINT

## Reconnaissance & Enumeration

- Types of Information Gathering
- Reconnaissance vs Enumeration
- Google Search
- Google Hacking
- User Enumeration & Phishing
- Forward Lookup Brute Force
- Reverse Lookup Brute Force
- DNS Zone Transfers
- Port Scanning
- Null Sessions
- Enum4Linux
- VRFY Script
- Python Port

## The Exploit Framework

- Exploring Metasploit Framework
- Using Metasploit Auxiliary
- Using Exploit Modules
- Staged and Non-Staged Payloads
- Working with Multi Handler
- Working with Meterpreter Session

## Bypassing Security

- Antivirus Evasion using Encoder
- Creating the shellcode with Msfvenom
- Bypassing Network Filters
- Understanding and bypassing pfsense firewall
- Bypassing IDS and IPS demo on snort

## Overflow to Attack

- Stack Overflows Introduction
- A Word About DEP, ASLR, and CFG
- Replicating the Crash
- Controlling EIP
- Stack Overflows and ASLR Bypass
- ASLR Introduction
- ASLR Implementation
- ASLR Bypass Theory
- Windows Defender Exploit Guard and ASLR
- Understanding SEH
- Exploiting SEH Overflows
- Understanding the low fragmentation heap
- Heap Overrun/Overflow

# Advanced Windows Exploitation

- Operating System and Programming Theory
- Win32 APIs
- Windows Registry
- What are Macros?
- Creating Dangerous Macros using Empire
- Microsoft Office Phishing using Macros
- Executing Shellcode in Word Memory
- PowerShell File Transfers
- VBA Shellcode Runner
- PowerShell Shellcode Runner
- Reflection Shellcode Runner in PowerShell
- Client-Side Code Execution with Windows Script Host
- Credential Replay Attacks
- Credential Discovery

## Hashing Concept

- Pass the Hash (PTH)
- Kerberoasting and AS-REP Roasting
- Pass the Ticket (PTT)

## Exploiting Latest Vulnerabilities

- FOLLINA
- Log4j
- Spring4Shell


# Privilege Escalation & Persistence

## Windows Privilege Escalation

- Understanding Windows Privileges and Integrity Levels
- User Account Control (UAC) Bypass: fodhelper. exe Case Study
- Insecure File Permissions: Serviio Case Study
- Kernel Vulnerabilities: USBPcap Case Study

## Linux Privilege Escalation

- Understanding Linux Privileges
- Insecure File Permissions: Cron Case Study
- Insecure File Permissions: /etc/passwd Case Study
- Kernel Vulnerabilities: Case Study

# THE WEB ATTACKS

INFOSECTRAIN

- OWASP Standards
- Broken Web Application
- ATutor & JuiceShop
- Web Traffic Inspection using Burpsuite
- Atmail Mail Server Appliance: from XSS to RCE
- Session Hijacking
- Session Riding
- Authentication Bypass and RCE
- Injection Attacks
- ATutor LMS Type Juggling Vulnerability
- Attacking the Loose Comparison
- Magic Hashes
- JavaScript Injection Remote Code Execution
- Cookie Deserialization RCE
- Server-Side Template Injection
- XSS and OS Command Injection
- Advanced XSS Exploitation
- RCE Hunting

## AWS PEN TESTING

- Building and setup AWS pen testing Environment
- Exploiting S3
- Understanding and exploiting Lambda Services
- Testing IAM privileges
- Case study For Capital One Attack

## DELIVERABLES – REPORT WRITING

- Defining Methodology
- Types of Reports
- Executive Summary
- Detailed Reports
- Adding Proof of Concept
- Creating Drafts
- Risk Rating Factors
- Automating Reports
- Report Writing Tools


www.infosectrain.com I sales@infosectrain.com