INFOSECTRAIN

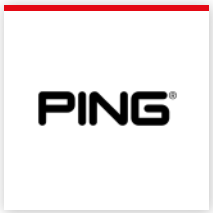
APT

Advanced Penetration Testing

Training Course

INFOSECTRAIN

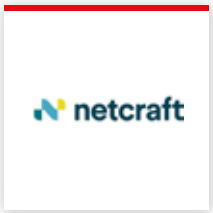
Tools Covered



Ping

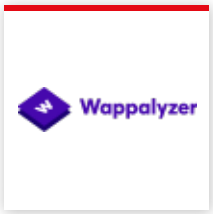
hPing

shodan

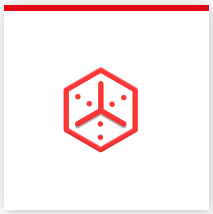


netcraft

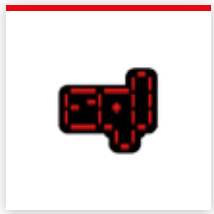
waybackmachine



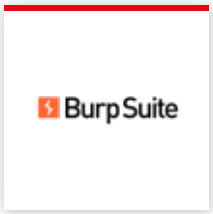
wappalyzer



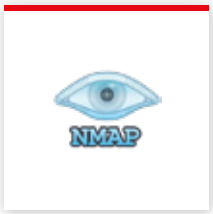
theHarvester



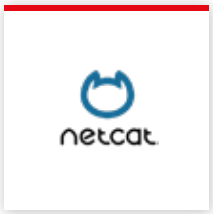
sqlmap



Burpsuite

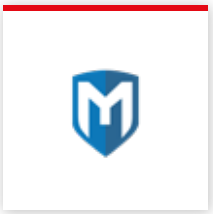


Nmap

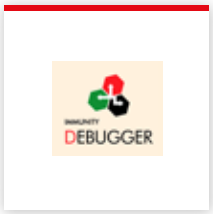


Netcat

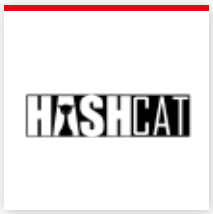
Wireshark



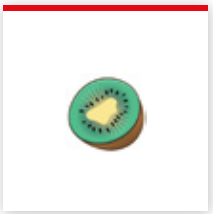
metasploit framework



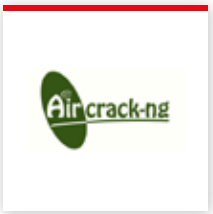
immunity debugger



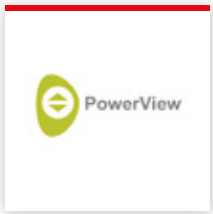
hashcat



kiwi

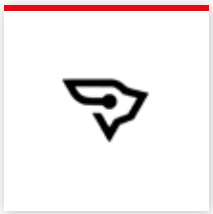


Aircrack-ng

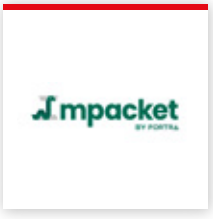


powerview

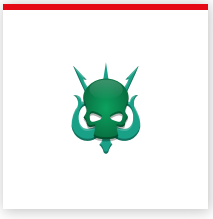
bloodhound



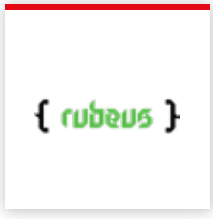
sharphound



Impacket

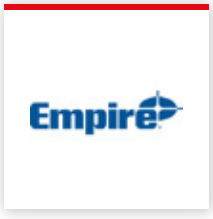


crackmapexec



Rubeus

PowerupSQL



Empire Framework

INFOSECTRAIN

Course Highlights

- **40-Hour LIVE** Instructor-led Training
- Highly Customized Program
- Scenario-based Learning on Latest Tools
- Interactive sessions with Q&A rounds
- Career Guidance and Interview Prep
- Post Training Support
- Access to Recorded Sessions
- Hands-on exposure to diverse vulnerabilities

INFOSECTRAIN

About Course

The Advanced Penetration Testing with Kali Linux is an all-embracing course that expertly explains how to optimize Kali Linux and its powerful tools for advanced wired and wireless networks. The course focuses on demonstrating advanced techniques to perform penetration testing. You learn to use Metasploit Framework and practices used in exploiting Windows and Unix platforms. Vulnerability scanning forms 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.

INFOSECTRAIN

Course Objectives

- Learn Kali Linux installation with lab setup
- Understand Reconnaissance types, Vulnerability analysis, classification, and identification
- Practice SQLMap, Metasploit, Tomcat Manager and other tools for identifying exploitation and attacks
- Learn advanced level exploitation such as exploiting vulnerable services in Windows and Unix
- Understand Spoofing, spinning and access maintenance, social engineering and BeFF
- Report writing and pen testing process

INFOSECTRAIN

Target Audience

- Middle and advanced level penetration testers
- Security enthusiasts
- Aspiring penetration testers
- Security professionals intending to upskill for
- compliance based penetration testing

Pre-requisites

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

INFOSECTRAIN

Our Expert Instructor

Ashish Dhyani

10+ Years of Experience

Network+ | Security+| Pentest+ | CEH | CND | ECSA | CCNA | ECDE

10+ years of experience as a Network Security Expert in delivering training to government and non-government organizations around the globe on different cyber security verticals and Network Security.

Ashish has provided training and consultancy to learners as well as organizations on the latest networking and security technologies available in the market today. He is proficient in tailoring course curricula to ensure courses and skills are up to date with current standards.

INFOSECTRAIN

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

INFOSECTRAIN

OSINT & Analysis

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

INFOSECTRAIN

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**
- → Leveraging Unquoted Service Paths
- → 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

- 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

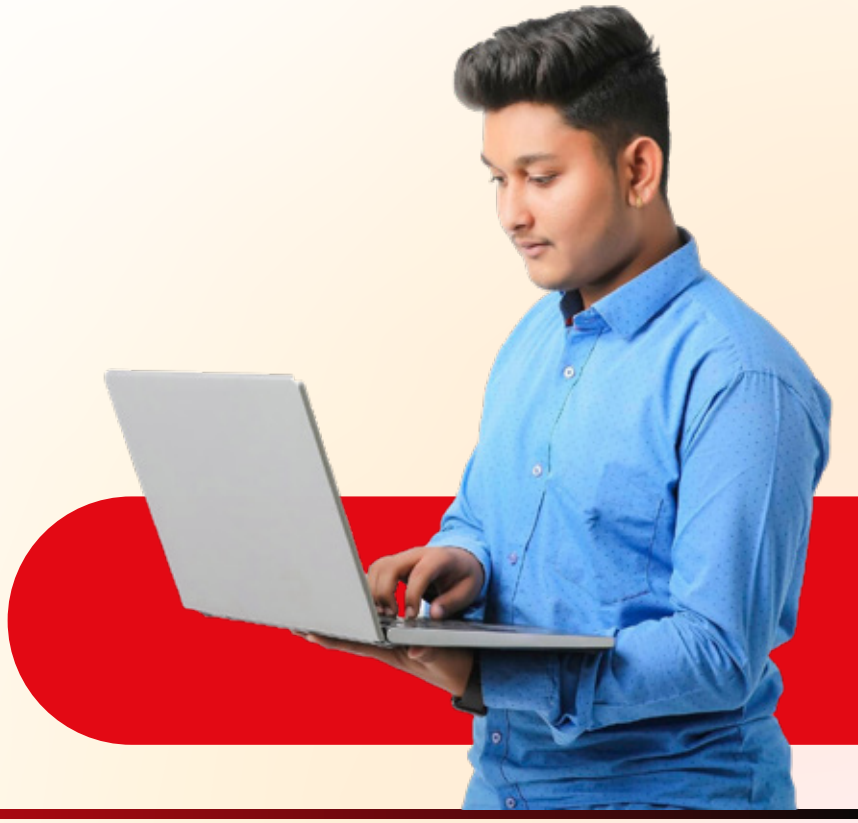
INFOSECTRAIN

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



INFOSECTRAIN

Testimonials

Senthil Kumar

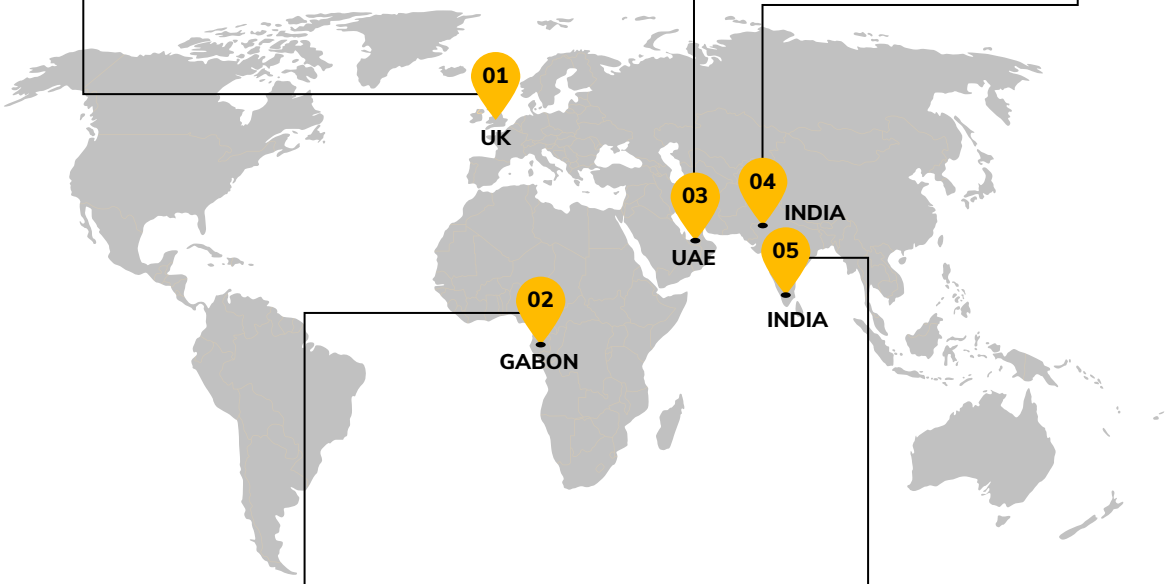
The trainer was very patient while answering all our questions. He is a very knowledgeable person, and I am glad to attend this course with InfosecTrain. Thanks a lot.

Shomayle Faruqui

I completed the APT course at InfosecTrain and I must say it was a very good training. I will definitely take up more courses in the future.

Vinit Jhalani

It was a good course. The trainer had great knowledge and made us understand the course in the best possible way. Thanks a lot for such an insightful training.



Moussodji Ikapi valery

I would like to thank InfosecTrain for the valuable course with experience and skills from the trainer. It was a very well-structured course. I learned very professional tools in the cyber security field through this course.

Sadashivuni Sushant

The course gave me a really good understanding of the cybersecurity domain and understanding of tools needed for testing. It was a great course.

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on