INFOSECTRAIN

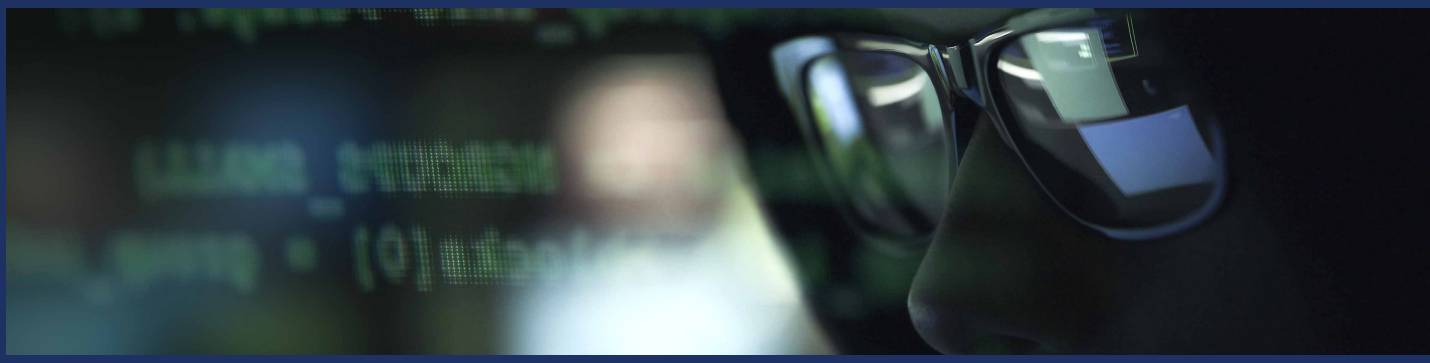
Pentest Tester Combo

TRAINING & CERTIFICATION

Pentest Tester Combo

- CEH
- Bug Bounty
- Red Team

www.infosectrain.com | sales@infosectrain.com



Course description

The Pentest Tester Combo Training course from InfosecTrain incorporates three important aspects of cybersecurity that is CEH training, Bug bounty training, and Red Team training.

The EC-Council Certified Ethical Hacker is one of the most highly regarded security certifications in the world. The Certified Ethical Hacker training course improves your awareness of key security concepts and confirms your ability to spot vulnerabilities in an organization's network architecture, allowing you to successfully battle cyber-at-tacks.

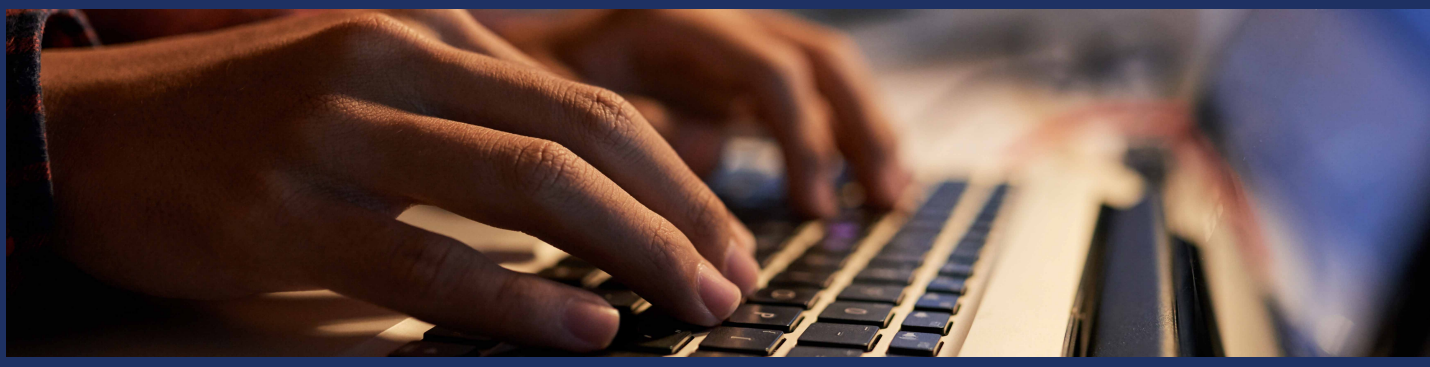
This course is the second in EC-new Council's Vulnerability Assessment and Penetration Testing (VAPT) Track. EC-Council has updated the document to include new themes and concepts in light of current breakthroughs in the realm of cybersecurity. The course will teach you about the most recent commercial hacking tools, practices, and methodologies used by real-world hackers.

Any organization's cybersecurity teams are made up of several teams, and the Red Team is an important aspect of that structure. We provide you with hands-on experience of reliable red teaming strategies including identifying, preventing, and mitigating attack vulnerabilities. You'll learn how to adopt a hacker's mindset and abuse/violate IT systems and infrastructure that are exposed to a future cyber-at-tack/threat.

Our Red Team Training course includes a number of practical sessions that are meant to establish a learning and application environment in order to develop a solid upskilling process with an effective learning methodology. For aspiring Red Teamers, the course was established, planned, and approved by certified cybersecurity experts and Red Team certified professionals. Our course includes everything you'll need to get started on your path to becoming a qualified Red Team cyber security specialist.

The bug bounty training course will help you in identifying the security vulnerabilities and loopholes in an organization's security infrastructure or applications. A bug bounty is a monetary payment provided to ethical hackers who find and disclose a vulnerability or flaw in a program to the developer. Bug bounty schemes enable businesses to use the hacker community to continually enhance the security posture of their systems.

By delivering an all-in-one platform for ongoing and thorough security testing, we will assist you in keeping the organization safe. The technology employs a simplified method to finding and fixing flaws, with everything from disclosure to compensation managed through a single dashboard.



Target Audience

- Ethical hackers
- System Administrators
- Network Administrators
- Engineers
- Web managers
- Auditors
- Red Teamers
- Bug Bounty Hunters
- Security Analysts
- Vulnerability Managers
- Penetration Testers
- IT Security Professionals
- Security Consultants
- Anyone who wants to learn the Offensive side of Cyber Security
- People with an interest in finding bugs

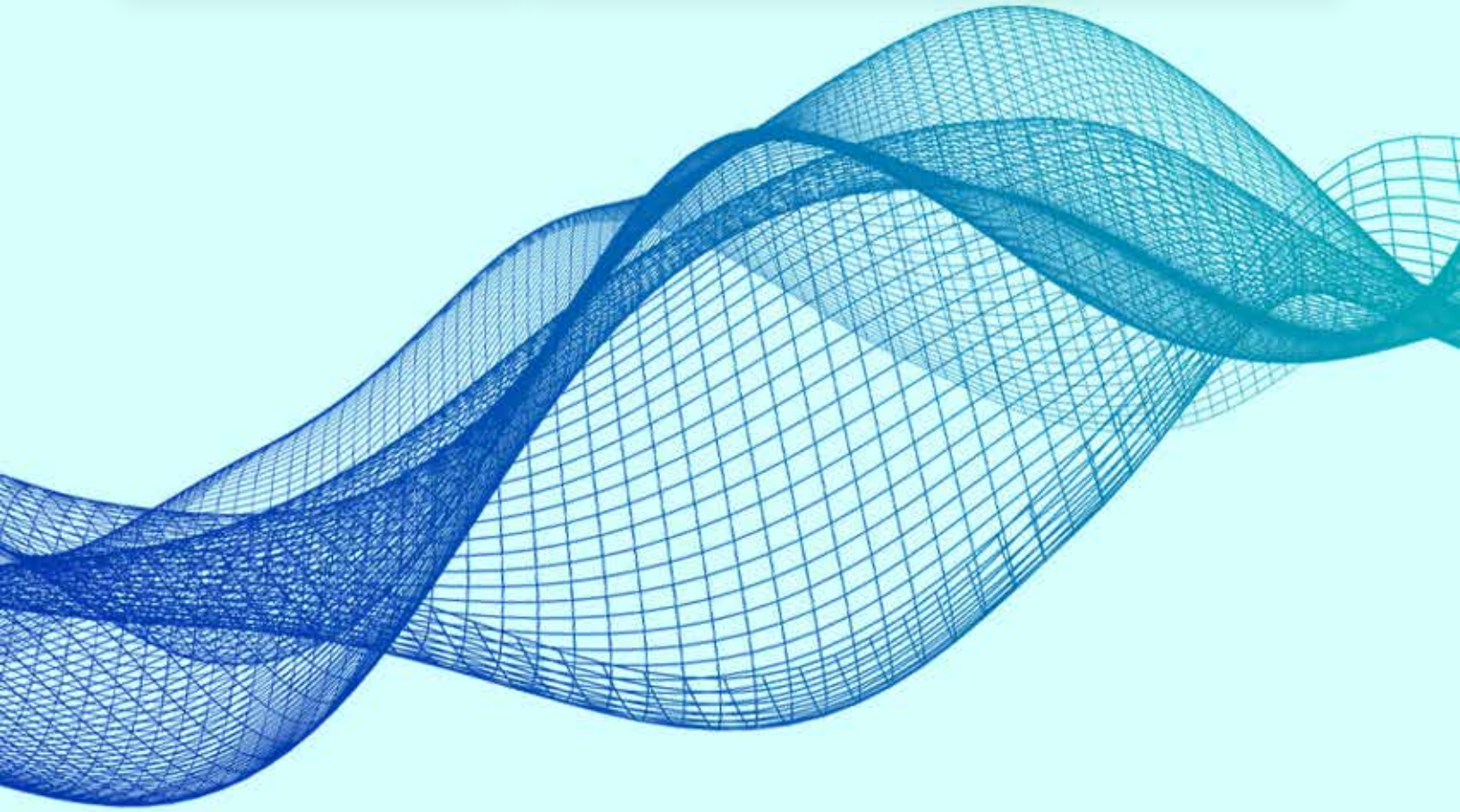
Prerequisites

- It is recommended to have a basic understanding of network essentials, core concepts including server and network components.
- A thorough understanding of Penetration Tests and Security Assessments
- Prior knowledge on OWASP TOP 10
- Understanding & Navigating Different OSes like Windows, Linux
- Knowledge of Active Directory
- Networking Basics
- Familiarity with PowerShell Scripts

INFOSECTRAIN

Why Infosec Train?

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- 4 hrs/day in Weekend/ Weekday



Course Content

INFOSECTRAIN

Module 01

Introduction to Ethical Hacking: This module introduces you to the basic concepts of hacking, what is hacking, who are hackers, their intent, and other related terminologies. The next modules dive deeper into the various phases of hacking, which would help you in thinking with the mindset of a hacker.

Module 02

Footprinting and Reconnaissance: Gathering information from various sources using footprinting tools and how to defend against the same.

Module 03

Scanning Networks: Different techniques to identify and scan the network, host, and port discovery by utilizing various scanning tools.

Module 04

Enumeration: Finding detailed information about the hosts and ports discovered during scanning. This module now includes sub-domains like NFS enumeration and related tools, DNS cache snooping, and DNSSEC Zone walking, along with the countermeasures.

Module 05

Vulnerability Analysis: It introduces the concepts of vulnerability assessment, its types, along with a hands-on experience of tools that are currently used in the industry.

Module 06

System Hacking: It focuses on the “how” part. How to gain access to the system, how to escalate privileges, how to maintain access, and how to clear your tracks. The next modules help to develop a deeper understanding of various defense and attack methodologies and concepts that aid the process of hacking.

Module 07

Malware Threats: Malware threat terminologies, viruses, worms, trojans, their analysis, and countermeasures to prevent data loss. The introduction and analysis of malware like, Emotet and fileless that are gaining popularity have been updated under this section. APT concepts have also been added.

Module 08

Sniffing: Packet sniffing techniques, associated tools, and related defensive techniques.

Module 09

Social Engineering: Since humans are the most significant vulnerability for any organization, it becomes essential to understand how attackers use them for their purpose for carrying out attacks like identity theft, impersonation, insider threat, and how to defend against such social engineering attacks.

Module 10

Denial-of-Service: As DoS and DDoS are some of the most common purposes of attackers, this module talks about these attacks, use cases, and the related attack and defense tools.

Module 11

Session Hijacking: To provide a deeper understanding of the technique, its purpose, tools used along with countermeasures.

Module 12

Evading IDS, Firewalls, and Honeypots: Understand the terminologies and working of these inline defenses and techniques to learn how to evade these while performing an attack.

Module 13

Hacking Web Servers: Web servers based attacks, methodologies, tools used, and defense

Module 14

Hacking Web Applications: Web application-based attacks, techniques, and mitigation.

Module 15

SQL Injection: An in-depth understanding of the top OWASP top 10 web app vulnerability, its working, and the mitigation.

Module 16

Hacking Wireless Networks: Wireless encryption, wireless hacking, and Bluetooth hacking-related concepts

Module 17

Hacking Mobile Platforms: Management of mobile devices, mobile platform attack vectors, and vulnerabilities related to Android and iOS systems

Module 18

IoT Hacking: Recognizing the vulnerabilities in IoT and ensuring the safety of IoT devices. Operational Technology (OT) essentials, introduction to ICS, SCADA, and PLC, threats, attack methodologies, and attack prevention. The concept of OT is a new addition.

Module 19

Cloud Computing: Cloud computing, threats, and security. Additionally, the essentials of container technology and serverless computing have been added.

Module 20

Cryptography: Encryption algorithms, Public Key Infrastructure (PKI), cryptographic attacks, and cryptanalysis.

Introduction to Pen-Testing

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

Hands On with Linux

- 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
- Backgrounding Processes (bg)
- Jobs Control
- Process Control
- File and Command Monitoring
- Downloading Files
- Persistent Bash Customization

Scripting Skills

- 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 Red Team's Plan and Execution

- What is Red Teaming?
- Red Team Attack Lifecycle (Phases)
- Red Team Infrastructure
- Enterprise Environment Overview
- Technologies Exploitation in Red Teaming
  - Web Technology
  - Network Technology
  - Physical Red Teaming
  - Cloud Technology
  - Wireless
- Why organizations need Red Team?
- Red Team Exercise Execution

Information Gathering & Enumeration

- Types of Information Gathering
- OSINT: Case Study
- Extensive OSINT 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

Red Team Kill Chain

- Initial Access & Delivery
- Weaponization
- Command & Control
- Credentials Dumping
- Lateral Movement
- Establishing Persistence
- Data Exfiltration

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)

Binary Analysis and Exploitation

- WinDbg and x86 Architecture
- Introduction to x86 Architecture
- Introduction to Windows Debugger
- Accessing and Manipulating Memory from WinDbg
- Introduction to IDA Pro

- Static-Dynamic Analysis Synchronization
- Double Pivoting
- Windows Defender Exploit Guard
- Binary diffing with BinDiff 5
- Visualizing code changes and identifying fixes
- Reversing 32-bit and 64-bit applications and modules

The Metasploit Framework

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

Exploiting Overflows - Linux & Windows

- 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

Privilege Escalation

- Windows Privilege Escalation
  - Understanding Windows Privileges and Integrity Levels
  - User Account Control (UAC) Bypass: fodhelper.exe Case Study
  - Insecure File Permissions: Servio Case Study
  - Leveraging Unquoted Service Paths
  - Windows 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

Lateral Movement & Pivoting Techniques

- Lateral Movement and Network Pivoting
- File-Less Lateral Movement Methodologies
- Understand Local, Remote Port Forwarding Using Chisel, various proxies etc
- Multi-level in-depth network pivoting in Windows & Linux OS
- Lateral Movement with SSH
- SSH Hijacking Using SSH-Agent and SSH Agent Forwarding

Advanced 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

Introduction to Wireless Security

- Cracking Wireless Encryptions
- Cracking WEP
- Cracking WPA, WPA2 & WPA3
- WIFI-Phishing
- Dos Attack: WIFI Jamming
- Securing WAP
- Auditing and Reporting

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.

Mitre ATT&CK Red Teaming

- Follow Mitre ATT&CK Framework
- Playing with Mitre
- Testing with Caldera
- Atomic Red Team Test for MITRE-ATT&CK
- Utilizing LOLBAS for stealth persistence & Data Exfiltration

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 | sales@infosectrain.com