INFOSECTRAIN

Become the Guardian of Cyber-Galaxy

Cyber Security Expert Training

Course Highlights

- Learn with Practical Approach
- 52-Hrs of Instructor-Led Training

www.infosectrain.com

INFOSECTRAIN

YOUR LEARNING PATH

Course 1
Hands-on SOC Expert

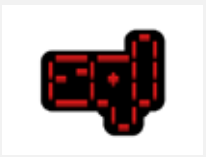
Course 2
Hands-on Penetration Testing

Expert 's Certificate
You will get certificate by Infosectrain

TOOLS COVERED







MANY MORE...

INFOSECTRAIN

COURSE DESCRIPTION OVERVIEW

The Cyber Security Expert training course offered by InfosecTrain is a comprehensive program that integrates SOC and Penetration Testing domains. It provides a comprehensive introduction to the fundamentals of Ethical Hacking and Penetration Testing. Throughout the course, participants will gain theoretical knowledge and practical skills by engaging in hands-on activities and using various tools and techniques. They will learn about different types of hackers, the importance of security, and the CIA Triad. The course also focuses on understanding network protocols, OSI model, IP addressing, operating systems, information gathering, blue team operations, threat intelligence, incident response, and so much more.

INFOSECTRAIN

WHY CYBER SECURITY EXPERT TRAINING COURSE WITH INFOSECTRAIN?

InfosecTrain is a leading IT security training and consulting organization offering best-in-class yet cost-effective, customized training programs to enterprises and individuals across the globe. We offer role-specific certification training programs and prepare professionals for the future. Our Cyber Security Expert training course will equip you with a comprehensive overview of essential topics in the field of cyber security.

Here's what you get when you choose InfosecTrain as your learning partner:

- **Flexible Schedule:** Training sessions to match your schedule and accommodate your needs.
- **Post Training Support with No Expiry Date:** Ongoing assistance and support until the learners achieve their certification goals.
- **Recorded Sessions:** Access to LMS or recorded sessions for post-training reference.
- **Customized Training:** A training program that caters to your specific learning needs.
- **Knowledge Sharing Community:** Collaborative group discussions to facilitate knowledge sharing and learning.
- **Certificate:** Each candidate receives a certificate of participation as a testament to their accomplishment.
- **Expert Career Guidance:** Free Career Guidance and support from industry experts.

INFOSECTRAIN

TARGET AUDIENCE

- System Administrators
- Network Administrators
- Penetration Testers
- IT Security Professionals
- Security Consultants
- SOC Analysts (L1 & L2)
- Cyber Security Analysts

PRE-REQUISITES

- Prior knowledge of networking fundamentals, OS basics, and troubleshooting
- A basic understanding of Penetration Testing and Security Assessments
- Understanding of different Operating Systems like Windows, Linux, etc.

INFOSECTRAIN

COURSE OBJECTIVES

You will be able to:

1. Understand cybersecurity concepts and penetration testing techniques
2. Learn about types of hackers, types of attacks, and ethical hacking phases
3. Understand the difference between ethical and malicious hacking
4. Learn footprinting techniques, scanning concepts, and vulnerability assessment
5. Understand the functions and role of a Security Operations Center (SOC)
6. Gain knowledge of SIEM systems, specifically Splunk
7. Understand vulnerability analysis and classification
8. Explore system hacking techniques and threat intelligence
9. Understand social engineering techniques and phishing attacks
10. Gain basic knowledge of incident response and digital forensics
11. Explore web application threats, including OWASP Top 10 Vulnerabilities
12. Learn about mobile platform security and vulnerabilities
13. Understand cloud computing and set up AWS for penetration testing
14. Gain knowledge of cryptography and encryption algorithms

INFOSECTRAIN

COURSE CONTENT

- **Module 1:** Security Terminologies, OS Basics and Network Fundamentals **[Theory]**
- **Module 2:** Introduction to Pen-Testing **[Theory]**
- **Module 3:** Linux Operating System Fundamentals **[Practical]**
- **Module 4:** Information Gathering / Footprinting
- **Module 5:** Scanning
- **Module 6:** Enumeration
- **Module 7:** Vulnerability Analysis
- **Module 8:** System Hacking
- **Module 9:** Windows Operating System Fundamentals **[Practical]**
- **Module 10:** Blue Team Operations Architecture
- **Module 11:** SIEM - Nervous System of SOC
- **Module 12:** Importance of Threat Intelligence
- **Module 13:** Social Engineering
- **Module 14:** Basics of Incident Response & Forensics
- **Module 15:** Web Application Threats and Concepts
- **Module 16:** Cryptography

INFOSECTRAIN

MODULE 1:

SECURITY TERMINOLOGIES, OS BASICS AND NETWORK FUNDAMENTALS [THEORY]

- Why do we need Security?
- Information Security vs. Cybersecurity
- CIA Triad
- Authentication, Authorization, and Accounting (AAA)
- Hacking Concepts

- **TYPES OF HACKERS**
  - » Black Hat
  - » White Hat
  - » Gray Hat
  - » Suicide Hacker
  - » Script Kiddies
  - » Hacktivist

- **DOMAINS OF CYBERSECURITY**
  - » Offensive Security
  - » Defensive Security

- **ETHICAL HACKING PHASES**

INFOSECTRAIN

- **TYPES OF ATTACKS**
  - » Phishing
  - » Vishing
  - » Smishing
  - » DoS
  - » Malware
  - » Man in the Middle Attack
  - » Insider Threat

- **NETWORK FUNDAMENTALS**
  - » OSI Model
  - » TCP/IP
  - » Network Protocols
  - » IP Addressing

INFOSECTRAIN

MODULE 2:

INTRODUCTION TO PEN-TESTING [THEORY]

- What is Penetration Testing?
- Difference between Ethical Hacking and malicious activities
    - White-Hat Hacker vs. Black-Hat Hacker
- Need for Penetration Testing
- Vulnerability Assessment vs. Penetration Testing
- Overview of Penetration Testing Process
- **TYPES OF PENETRATION TESTING**
    - Web Application Penetration Testing
    - Mobile Application Penetration Testing
    - Cloud Penetration Testing
- **VARIOUS METHODOLOGIES OF PENETRATION TESTING**
    - Black box testing
    - Gray box testing
    - White box testing
- **IMPORTANCE OF REPORTING IN PENETRATION TESTING PROCESS**

INFOSECTRAIN

MODULE 3:

LINUX OPERATING SYSTEM FUNDAMENTALS [PRACTICAL]

- Linux Directory Services
- The most useful Linux Commands in SOC
- Events Logs in Linux
- Linux System Services

MODULE 4:

INFORMATION GATHERING/FOOTPRINTING

- Footprinting Concepts
- Footprinting through a Search Engine **[Practical]**
    - » Using Google Dorks
    - » Understanding Title, Text, and URL in Dorks
    - » Shodan
    - » Censys
- **FOOTPRINTING THROUGH TOOLS [Practical]**
    - » Spiderfoot
    - » Netcraft
    - » Harvester
    - » MxToolbox
    - » Eagle OSINT

INFOSECTRAIN

- **DIFFERENT TECHNIQUES FOR WEBSITE FOOTPRINTING**
  - » Wappliyzer
  - » Whois
  - » Netcraft
  - » crt.sh
  - » DNS Dumpster

MODULE 5:

SCANNING

- SCANNING CONCEPTS
  - » Steps of Scanning
  - » Installation of Nessus
  - » Working with Nessus
  - » Working of Nmap
- SCANNING TECHNIQUE FOR PORT AND SERVICE DISCOVERY
  - » Various Switches of Nmap

INFOSECTRAIN

MODULE 6:

ENUMERATION

» Enumeration concepts

» Different techniques for Enumeration **[Practical]**

MODULE 7:

VULNERABILITY ANALYSIS

• Vulnerability assessment concepts

• Vulnerability classification and assessment types

MODULE 8:

SYSTEM HACKING

• Password cracking and gaining access techniques **[Practical]**

• Privilege escalation technique **[Practical]**

INFOSECTRAIN

MODULE 9:

WINDOWS OPERATING SYSTEM FUNDAMENTALS

[PRACTICAL]

- INVESTIGATING WINDOWS OPERATING SYSTEM
  - » Reliability Monitor
  - » Task manager CLI view
  - » Temp and Prefetch
- UNDERSTANDING WINDOWS EVENT LOGS
  - » Event Viewer
- Understanding Windows Registry
- Scheduled Tasks
- File Analysis
- SysInternals Suite
- Command Prompt

INFOSECTRAIN

MODULE 10:

BLUE TEAM OPERATIONS ARCHITECTURE

- What is SOC?
- Why do we need SOC?
- Functions of SOC
- Security Operation Center Models & Types
- Security Operation Center SOC Teams & Roles
- Incidents vs Events
- True vs False Incident Categories
- Concept of Logging
- Log Management & Log Analysis

MODULE 11:

SIEM - NERVOUS SYSTEM OF SOC

- Why do we need SIEM?
- What is SIEM?
- SIEM guidelines and architecture
- SIEM Capabilities: Aggregation, Correlation, Reporting, Storage, Alerts, etc
- Using Splunk **[Practical]**
    - Splunk setup
    - Working of Splunk
    - UI Navigation

- Search Queries using SPL
- Creating Alerts & Dashboard
- Adding logs
- Analyzing logs

MODULE 12:

IMPORTANCE OF THREAT INTELLIGENCE

- What is a threat?
- Why do we need intelligence?
- Introduction to Threat Intelligence
- Threats, Threat Actors, APTs & Global Campaigns
- Indicator of compromise vs Indicator of Attack precursors
- Collecting Threat Intelligence **[Practical]**
- Enhanced Detection with Threat Intelligence

MODULE 13:

SOCIAL ENGINEERING

- Social engineering concepts and phases
- Social engineering techniques
- Phishing email attack **[Practical]**

INFOSECTRAIN

MODULE 14:

BASICS OF INCIDENT RESPONSE & FORENSICS

- Incident Response Lifecycle
- Incident detection and mitigation **[Practical]**
- Forensics Fundamentals
- Email Forensics
- Analyzing Phishing Emails **[Practical]**
- Lockheed Martin Cyber Kill Chain
- MITRE ATT&CK Framework **[Practical]**

MODULE 15:

WEB APPLICATION THREATS AND CONCEPTS

- What is a web application?
- How Web Application works
- Understanding HTTP headers and status codes
- OWASP Top 10
    - Broken Access Control **[Practical]**
    - Cryptographic Failures
    - Injection **[Practical]**
    - Insecure Design
    - Security Misconfiguration **[Practical]**
    - Vulnerable and Outdated Components

- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery **[Practical]**

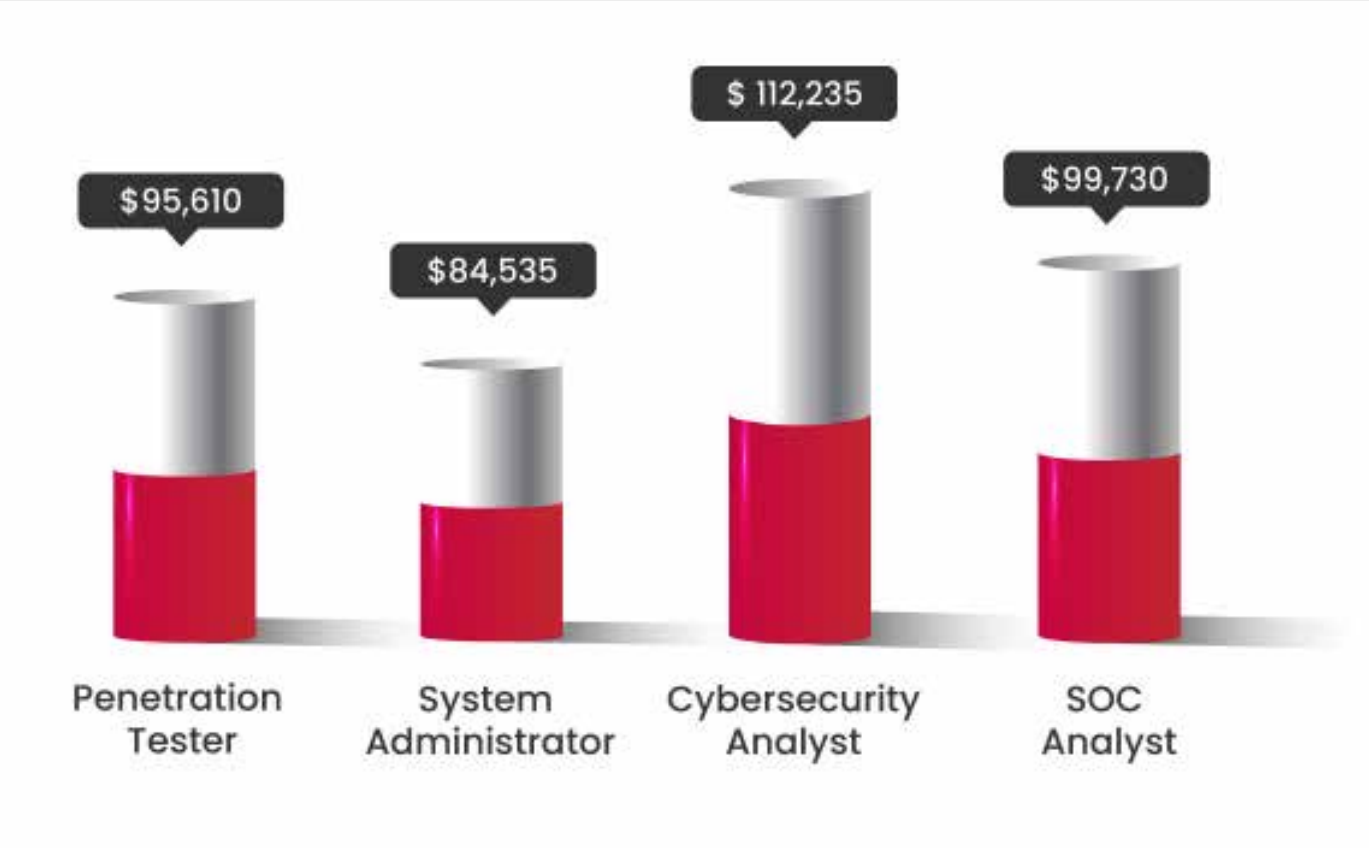
MODULE 16:

CRYPTOGRAPHY

- Introduction and history of Cryptography
- Different encryption algorithms
    - Symmetric Encryption
    - Asymmetric Encryption
- Application of cryptography
    - PKI (Public Key Infrastructure)
    - Digital certificate
    - Digital signature
    - Steganography **[Practical]**
- Cryptanalysis **[Practical]**

INFOSECTRAIN

COURSE BENEFITS



Hiring Companies

wipro HCL IBM cognizant

Source: Glassdoor

www.infosectrain.com I sales@infosectrain.com