INFOSECTRAIN

PRICE
~~$ 199~~
FREE
BOOTCAMP

CYBERSECURITY
FOUNDATION COURSE

A Social Endeavour to Make These Tough Times Easier

GAIN THE MOST WANTED SKILLS THAT ARE TOO TOUGH TO IGNORE BY EMPLOYERS

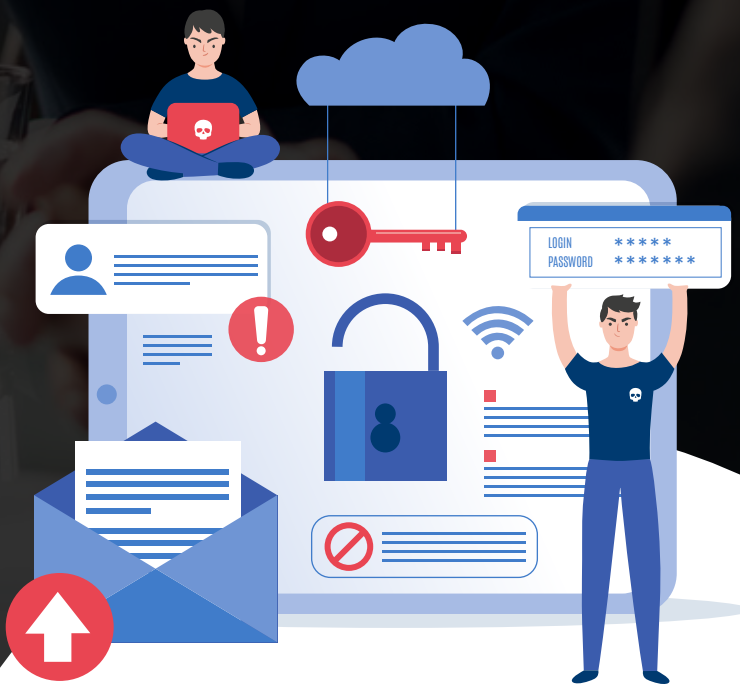
FREE BOOTCAMP | 64 HOURS | 32 DAYS

HIGHLIGHTS

64 Hours
of instructor-led training

Get 20 CPE
Certificate

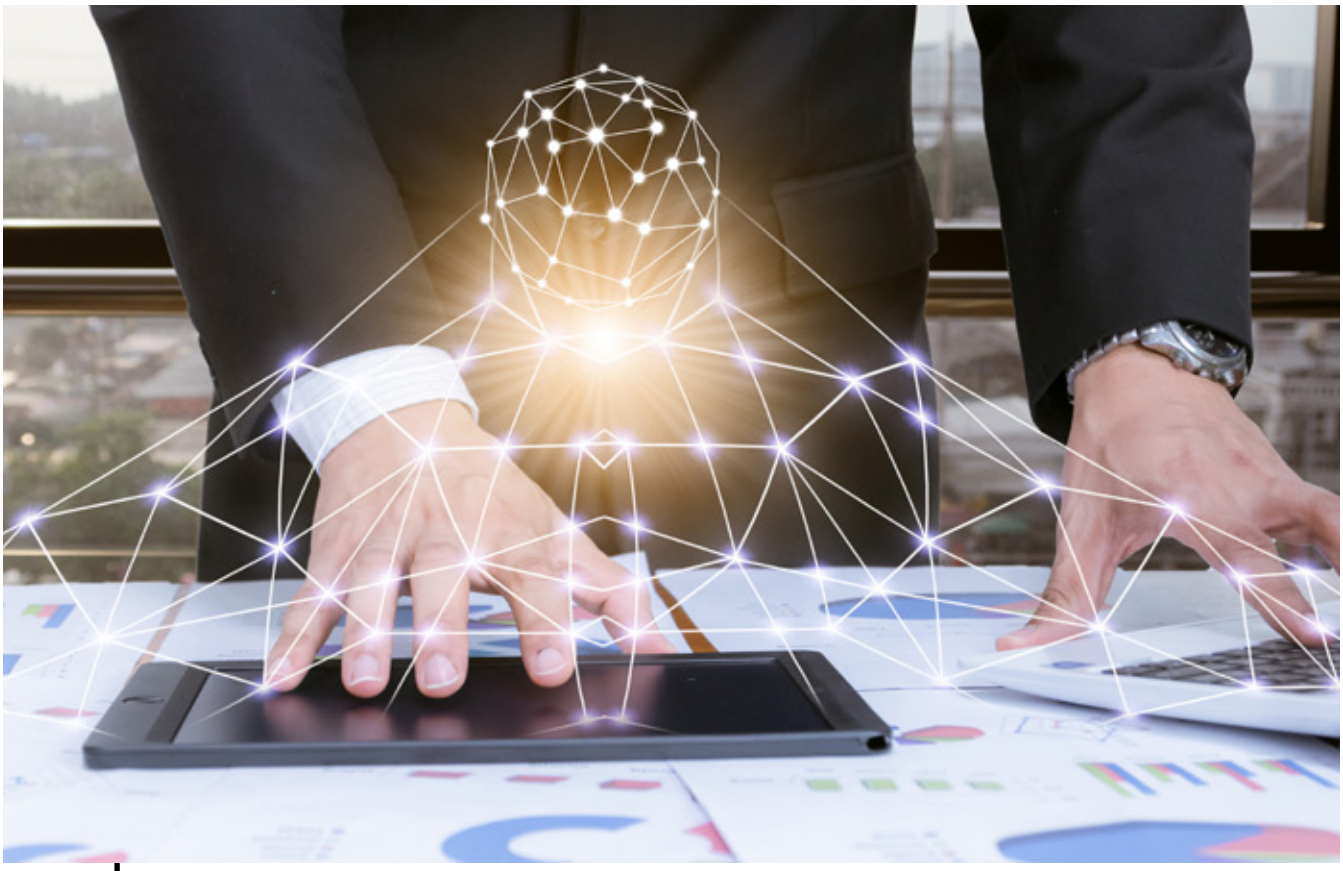
Certified & Experienced
Instructors



www.infosectrain.com

INFOSECTRAIN

COURSE TOPICS & SCHEDULE



NETWORKING BASICS

DAY 01

- What is Network?
- Network types
- Networking Models
- Methods of data transmission

DAY 02

- Introduction of OSI model
- Understanding the flow of data through every layer
- Protocols in every layer of OSI model

DAY
03

- Types of network Media
- Network topologies
- Networking devices
- TCP/IP protocol suite
- IPv4 Addressing
- IPv6 Introduction

DAY
04

- Routing and Switching
  - Dynamic and static routing
  - Types of switching – circuit switching, packet switching, message switching
  - Protocols in routing and switching

DAY
05

- Basics of WAN
- WAN transmission technologies
- Network Troubleshooting tools
- Overview of SDN

DEFENSIVE SECURITY BASICS

DAY 06

- Cybersecurity vs Information security vs Privacy
- CIA triad
- Basic terminologies in security
- Hackers and their types
- Teams in Cybersecurity

DAY 07

- Social Engineering
- Types of social engineering attacks
- Vulnerability Assessment
- Types of Vulnerability Scanning

DAY 08

- Cryptography an introduction
- Basic terminologies in cryptography
- Encryption and its types
- Encodings
- Digital signature
- Digital Certificates
- Public Key Infrastructure introduction
- Certification authorities and certificate types
- Certificate chaining

DAY 09

- Network security Appliances
- Firewall and its types
- Security monitoring
- SIEM summary
- What is endpoint security
- Endpoint security technologies – (EDR, XDR, MDR)

DAY 10

- Introduction to packet analysis
- Analyzing traffic using Wireshark
- Mobile device security
- Mobile device management and policies
- Safety measures to follow for mobile device security

DAY 11

> What is data privacy?
> Types of data
> Data privacy controls
> Data privacy laws

DAY 12

> Digital forensics introduction
> Chain of custody
> Order of volatility
> Evidence Acquisition
> Tools used in Digital Forensics

DAY 13

> How Redundancy can increase availability?
> Fault tolerance vs redundancy
> Power redundancy
> Disk Redundancy
> Network redundancy
> Backups and its types

> Physical security in an Enterprise
> Physical security controls
> Air gaps
> Safes and vault
> HVAC, hot aisle and cold aisle

OFFENSIVE SECURITY BASICS

DAY 15

> Introduction to Attacks
> Introduction to penetration testing
> Penetration testing methodologies
> Why penetration testing is important for an organization?

DAY 16

> Reconnaissance through search engines
> Website Reconnaissance
> The OSINT Framework
> Introduction to scanning
> Tools of scanning (nmap,nessus)

DAY 17

> Working with nmap
> Finding open ports, services running and service version with nmap
> Banner grabbing
> Scan beyond IDS and Firewall

DAY 18

> Enumeration introduction
> Introduction to the Metasploit framework
> Enumerating different services using the Metasploit framework
> Exploiting vulnerabilities to gain access

DAY 19

> Privilege escalation introduction
> Methods to escalate privileges
> Covering the tracks by clearing logs
> Covering tracks by Clearing the history
> Clearing logs by removing log directory

DAY
20

> Introduction to malware
> Types of malware
> Creating a malware
> Intro to malware analysis

DAY
21

> Sniffing
> Types of Sniffing
> Sniffing Techniques

DAY
22

> Denial of Service attacks
> Categories of DOS and DDOS
> DDOS and bot-nets
> DOS Tools
> Countermeasures of DOS attack

> Introduction to Wireless networks
> Types of Wireless Encryption
> Wireless hacking tools

> Web application Basics
> OWASP Top 10 2021 Introduction
> Exploiting vulnerabilities of web application
> Countermeasures of vulnerabilities
> Secure coding practices

INFOSECTRAIN

BASICS OF CLOUD COMPUTING

DAY
25

- Introduction to Cloud computing
- Advantages of cloud over on-premises
- Limitations of cloud
- Service models
- Deployment models

DAY
26

- Virtualization in cloud
- Types of Hypervisors
- Docker vs Container
- Cloud service providers
- Types of services provided by cloud
- Get acquainted with cloud environment

- Cloud storage security
- Cloud networking security
- VPC and Transit gateways
- Introduction to AWS infrastructure
- Security groups in AWS
- Serverless architecture
- EC2
- S3 buckets
- AWS Infrastructure

INFOSECTRAIN

INFORMATION SECURITY MANAGEMENT

DAY
28

> Introduction to Information Security Management
> Access Controls
> Security Policies

DAY
29

> Overview of Incident Response Process
> Risk Management

ISO 27001

DAY 30

> What is ISO?
> The ISO/IEC 27000 family of standards
> Advantages of ISO/IEC 27001

DAY 31

> Certification process
> Certification bodies
> Fundamental concepts and principles of information security

DAY 32

> Interview Preparation