INFOSECTRAIN

Network Security

Fundamentals & Essentials

TRAINING PROGRAM

www.infosectrain.com | sales@infosectrain.com

INFOSECTRAIN

Course Overview

Network Security is one of the most significant parts of any information security process due to overreliance on various verticals for business and personal communication. Companies of all scales and sizes should have proper strategies and mitigation processes to secure their networks to ensure optimum digital security and compliance. Although there are no networks that are completely secured from cyber threats, an efficient and reliable network security system can ensure that essential security is maintained throughout the network system of the business.

This course is designed to help you build your fundamental basics of understanding the working of Networks and their various components. The course extensively covers a wide range of concepts like Networks and Networking basics, IP Addressing, threats targeting Network security, network security fundamentals, routers, firewalls, malware, and much more!

This course will also help you build your base as a cybersecurity professional as Network security is a significant part of the same. This network security training program will help you identify and mitigate various types of Network Security threats and attacks that plague Network security systems like Sniffing, DoS & DDoS attacks, Fraggle and Smurf attacks, DNS poisoning, etc. Take advantage of this best network security training from InfoSecTrain and help yourself jumpstart a lucrative Cybersecurity career.

Target Audience

- Anyone who is interested to explore network security in-depth and gain essential skills for their cybersecurity career.
- IT security enthusiasts looking to build a career in the same
- Analysts and Junior engineers looking to build a career in cybersecurity

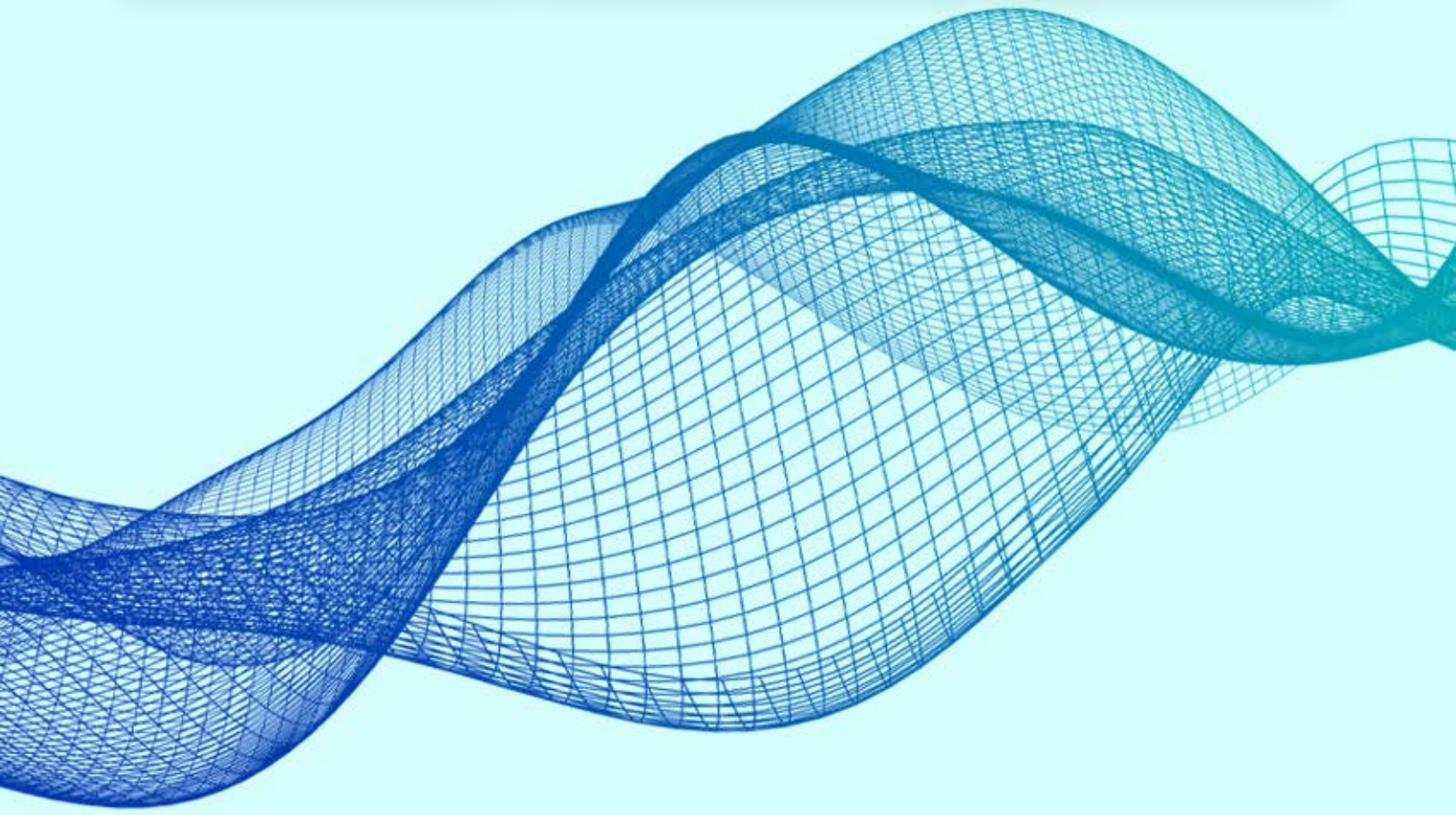
Prerequisites

- Basic knowledge of Network and Networking concepts like TCPs, DNS, IPs, Ports, etc.
- Linux Basics/ fundamentals and scripting in Linux OS
- Computing fundamentals and Internet working methodology
- Computer Science fundamentals/ background

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

Network Security Introduction Module

- What is Network Security
- Fundamentals of Networks
- IP Addressing
- Threats that impact network security & their types
- What are Cyber Controls
- Introducing ISO-27001 & PCI-DSS

Understanding of Router & Hands-on practice on Vulnerability Scanning

- Understanding of Router & End Points
- Network Discovery using hping3, arp-scan, Angry IP Scanner
- Finding Open Ports using Nmap
- Scanning for Vulnerabilities
- Vulnerability Scanners including OpenVAS, Nessus, Nmap

Firewalls & its Types

- Understanding Firewall
- Host Based Firewall
- Network Based Firewall
- Linux – iptables & Configurations
- Windows Firewall
- Windows Firewall Control (WFC)
- Network Based Firewall - pfSense
- Configuring & Detection using Snort

Network Attacks - The Reason for Network Security

- Introduction to network-based attacks, now and then.
- Practical Demonstrations – Man in the middle, SSL Stripping, ARP & DNS Spoofing
- Sniffing concepts
- DoS & DDoS Attack
- Fraggle and Smurf Attack
- DNS Poisoning & Ping of Death Attack
- Firewalking
- Perform Privilege Escalation to Gain Higher Privileges - Practical
- Maintain Remote Access and Hide Malicious Activities
- Reconnaissance
- Introduction to IoT & ICS
- Challenges of IoT
- Coding Errors (Buffer Overflow)
- Lack Of Security & Privacy
- Extensive use of clear text protocols & unnecessary open ports.
- IoT Security Problems
- OWASP Top 10 IoT Threats

Malwares

- Introducing Malwares
- Types of Malwares – Virus, Keyloggers, Worms, Trojan, Rootkits, Spyware, Adware
- Functionalities of Malwares
- Ransomware – Myths/Facts
- Working of Ransomwares
- Ransomware Deliveries
- Prevention against Ransomwares (Corporate Best Practices)

Understanding of Wireless and Wi-fi Security

- What is a Wireless Network?
- Wi-Fi Standards
- Wi-Fi Encryptions – WEP, WPA, WPA2, WPA3
- Wi-Fi Weaknesses
- Wi-Fi Attack – Practical
- Wireless Security
- Fundamentals of LiFi
- Zigbee for IoT

Network Monitoring – Fundamentals

- Introduction to Wireshark
- Using filters of Wireshark
- Network Packet Analysis - Practical
- Detecting malwares using Wireshark - Practical

Browser Security - Learning tools and their usage

- Minimize Browser Attacking Surface
- Browser Hacking - Practical
- Browser Hardening - Firefox
- Firefox Security, Privacy & Tracking
- HTTP Filters, ad and blockers
- Disconnect, Ghostery, Request Policy - HTTP Filters, ad and blockers
- ABP, Privacy badger - HTTP Filters, ad and blockers
- uMatrix and others - HTTP Filters, ad and blockers
- History, Cookies
- Fingerprinting Browser

Learning Authentication & Why it is Important

- Understanding Authentication
- Multi-Factor Authentication (MFA)
- Something You Know
- Something You Have
- Something You Are
- Choosing a Method of Multi-Factor Authentication
- MFA - Strength & Weakness
- Password Cracking
- Password Managers - KeePass
- Strong Password Creation & Necessity

INFOSECTRAIN

A Cryptography Primer

- Cryptography description
- Symmetric/Asymmetric Cryptography
- Hashing
- Encoding/Decoding
- Digital Signatures
- PKI – Practical

www.infosectrain.com | sales@infosectrain.com