INFOSECTRAIN

NETWORK SECURITY

ONLINE TRAINING

COURSE OVERVIEW

Companies of all scales and sizes want to have proper strategies and mitigation processes to secure their networks. 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. The Network Security Training course from Infosectrain is designed to help you build a basic understanding of Networks and their various components. The course extensively covers a wide range of concepts along with tools used to secure networks. This 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.

WHY **NETWORK SECURITY** ONLINE TRAINING COURSE WITH **INFOSECTRAIN**?

InfosecTrain is a proficient technology and security training and consulting organization across the globe, specializing in various IT security courses and services. Our Network Security training aims to develop advanced skills required to secure networks. You can leverage the following benefits with InfosecTrain:

- We provide hands-on experience with our lab sessions.
- We can help you present your qualifications and work experience for the designated profile.
- We provide a flexible training schedule.
- We provide recorded videos after the session to each participant.
- We provide post-training assistance.
- We also provide a certificate of participation to each candidate.

TOOLS COVERED
IN THIS COURSE


Nmap


VELOCIRAPTOR


Metasploit


Wireshark


Nessus


Nslookup


OpenVAS


MEDUSA

Aircrack-ng

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.

Pre-Requisites

- 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 background

Course Content

Network Fundamentals

> Computer Network
> Types of Networks
> Major Network Topologies

Network Components

> Network Interface Card (NIC)
> Repeater
> Hub
> Switches
> Router
> Bridges
> Gateways

TCP/IP Networking Basics

> Standard Network Models: OSI Model
> Standard Network Models: TCP/IP Model
> Comparing OSI and TCP/IP

TCP/IP Protocol Stack

- Domain Name System (DNS)
- DNS Packet Format
- Transmission Control Protocol (TCP)
  - TCP Header Format
  - TCP Services
  - TCP Operation
  - Three-way handshake
- User Datagram Protocol (UDP)
  - UDP Operation
- IP Header
  - IP Header: Protocol Field
  - What is Internet Protocol v6 (IPv6)?
  - IPv6 Header
- Internet Control Message Protocol (ICMP)
  - Format of an ICMP Message
- Address Resolution Protocol (ARP)
  - ARP Packet Format
  - Ethernet
  - Fiber Distributed Data Interface (FDDI)
  - Token Ring
- IP Addressing
  - Classful IP Addressing
  - Address Classes
  - Reserved IP Address
  - Subnet Masking
  - Subnetting
  - Supernetting

TCP/IP Protocol Stack

> IPv6 Addressing

- Difference between IPv4 and IPv6
- Configuring static and dynamic IP in windows and linux
- IPv4 compatible IPv6 Address

Operating System basics

> Understanding the basic of Windows

> Installing windows in Vmware

> Basic Windows Commands -> assoc,chkntfs,call,break,color,endlocal,clip, icacls,label,ping,mkdir,verify,wmic,compact,chkdsk,cipher

> Understanding the Architecture of Linux

> Installing Linux in Vmware

> Installing kali Linux in virtual Environment

> Most useful and powerful commands of Linux -> Shred , more , head, less,dig,ssh,ps ,fg ,grep,sed,awk,cut,gzip,chmod,rm , netstat,lsof.

Security Fundamentals

> Cybersecurity vs Information security vs Privacy

> Pillars of Security

> Basic terminologies in security

> Hackers and their types

> Teams in Cybersecurity

> Phases of hacking

> Introduction to Cyber threat intelligence

> Introduction to Threat Modelling

Introduction to Attacks

Reconnaissance Attacks

> Reconnaissance Attacks: ICMP Scanning (Hands-On using nmap)

> Reconnaissance Attacks: Ping Sweep (Hands-On using nmap)

> Reconnaissance Attacks: DNS Footprinting (Hands-On using nmap)

> Reconnaissance Attacks: Network Range Discovery (Hands-On arp-scan , nmap)

> Reconnaissance Attacks: Network Topology Identification

> Reconnaissance Attacks: Network Information Extraction using Nmap Scan (Hands-On)

> Reconnaissance Attacks: Port Scanning (Hands-On using nmap)

> Reconnaissance Attacks: Network Sniffing using wireshark and tcpdump(Hands-On)

How an Attacker Hacks the Network Using Sniffers

Network Access Attacks

> Password Attacks (Hands On using hydra , ncrack, medusa)

> Password Attack Techniques

- Dictionary Attack
- Brute Forcing Attacks
- Hybrid Attack
- Birthday Attack
- Rainbow Table Attack

> Man-in-the-Middle Attack
> Replay Attack
> Smurf Attack
> Spam and Spim
> Xmas Attack
> Pharming
> Privilege Escalation (Hands On)
> DNS Poisoning (hands on lab creation in linux)
> DNS Cache Poisoning (Hands on in ubuntu)
> ARP Poisoning
> DHCP Starvation Attacks (Hands On using yersinia)
> DHCP Spoofing Attack (Hands on using own dhcp server)
> Switch Port Stealing
> Spoofing Attacks
> MAC Spoofing/Duplicating (Hands on using MAC changer)
> Denial of Service (DoS) Attacks (Hands On using script)
> Distributed Denial-of-Service Attack (DDoS) (Creating a C2)
> Malware Attacks (Hands On)

Network Security Policy, Protocols and Controls

> What is Security policy
> Steps to create and Implement security policy
> Various policies in Enterprise
> Network security protocols

- IPSec
- SSL/TLS
- Kerberos
- SNMPv3
- SSH
- PPTP
- L2TP

> Network Security Controls
  - Access Control Principles
  - Access Control System: Administrative Access Control
  - Access Control System: Physical Access Controls
  - Access Control System: Technical Access Control
  - Discretionary Access Control
  - Mandatory Access Control
  - Role based access control

Network Security Appliances

> Network Access Control
> Configuring NAC Packet Fence (Hands-On)
> Firewalls
> DMZ
> VPN
> IDS
> IPS

Network Protocol Analyzer

> How it Works
> Advantages of using Network Protocol Analyzer
> Network Protocol Analyzer Tool like Wireshark and TCP Dump (Hands on)

Internet Content Filter

> Advantages of using Internet Content Filters
> Internet Content Filters
> Integrated Network Security Hardware

Network Security Protocols

> Transport Layer

> Network Layer

> Application Layer

> Data Link Layer

Implementation of Network Security Devices in Virtual Lab

> Firewall

- What Firewall does
- Types of Firewall
- How Firewall Works
- Firewall rules (Hands on)
- Configuring pfsense firewall (Hands on)
- Firewall Topologies
- Anti-Evasion Techniques
- Why are Firewalls bypassed

> IDS/IPS

- IDS Function in Network Defense
- Working of IDS
- Components of IDS
- Types of alerts
- Types of implementations
- Configuring Snort (Hands-On)
- IPS working
- How it is Different from IDS
- Types of IPS

> Antivirus
- Understanding the Working of Antivirus
- Bypassing Antivirus techniques (Hands on)

> Endpoint Detection and Response
- What is EDR?
- How EDR works
- Configuring EDR velociraptor (Hands-On)
- Introduction to XDR

> VPN Configuration and Management
- What is VPN?
- Configuring VPN functionality of your router. (Hands On)
- Working of VPN
- Why to use VPN?
- VPN Components
- VPN Types
- Common Flaws in VPN
- VPN Security

Network Traffic Monitoring and Analysis

> Monitoring and Analysis techniques
> Network Traffic Signatures
> Using Packet sniffer : Wireshark and tcpdump (hands on)
> Detecting OS Fingerprinting Attempts
> Detecting Passive OS Fingerprinting Attempts
> Detecting Active OS Fingerprinting Attempts
- Detecting ICMP Based OS Fingerprinting
- Detecting TCP Based OS Fingerprinting

- Examine Nmap Process for OS Fingerprinting
- Detecting PING Sweep Attempt
- Detecting ARP Sweep/ ARP Scan Attempt
- Detecting TCP Scan Attempt
  - TCP Half Open/ Stealth Scan Attempt
  - TCP Full Connect Scan
  - TCP Null Scan Attempt
  - TCP Xmas Scan Attempt
- Detecting SYN/FIN DDOS Attempt
- Detecting UDP Scan Attempt
- Detecting Password Cracking Attempts
- Detecting FTP Password Cracking Attempts
- Detecting Sniffing (MITM) Attempts
- Detecting the Mac Flooding Attempt
- Detecting the ARP Poisoning Attempt

Introduction to Zero Trust

- What is Zero Trust Network
- Pillars of Zero trust network
- Architecture of zero trust network
- Application Deployment

Securing the Wireless infrastructur

- Wireless Terminologies
- Wireless Networks
  - Advantages of Wireless Networks
  - Disadvantages of Wireless Networks

> Wireless Standard

> Wireless Topologies

> Components of Wireless Network

- Access Point
- Wireless Cards (NIC)
- Wireless Modem
- Wireless Bridge
- Wireless Repeater
- Wireless Router
- Wireless Gateways
- Wireless USB Adapter

> WEP (Wired Equivalent Privacy) Encryption

> WPA (Wi-Fi Protected Access) Encryption

> WPA2 Encryption

> WEP vs. WPA vs. WPA2

> Wi-Fi Authentication Method

- Open System Authentication
- Shared Key Authentication

> Wireless Attacks (Hands on using Wifi exploitation Framework)

- War Driving
- Client Mis-association
- Unauthorized Association
- HoneySpot Access Point (Evil Twin) Attack
- Rogue Access Point Attack (hands on)
- Misconfigured Access Point Attack
- Ad Hoc Connection Attack
- AP MAC Spoofing
- Denial-of-Service Attack
- WPA-PSK Cracking
- RADIUS Replay
- ARP Poisoning Attack

- WEP Cracking (hands on)
- Man-in-the-Middle Attack (Hands on)
- Fragmentation Attack
- Jamming Signal Attack

> Applying Mitigations of Network based attack to Virtual Lab (Hands on)

> Pentesting the Lab (Hands On)

.> Conclusion

www.infosectrain.com | sales@infosectrain.com