AISECT LEARN
Better Education. Better Careers.

LIVE + SELF-PACED

NETWORK SECURITY PROFESSIONAL CERTIFICATE COURSE

COURSE OVERVIEW

The Network Security Professional Certificate course is designed to provide participants with a comprehensive understanding of the principles, concepts, and techniques related to securing computer networks. This course focuses on equipping individuals with the knowledge and skills necessary to protect network infrastructure, data, and communication channels from unauthorized access, threats, and attacks.

COURSE OBJECTIVE

This course aims to equip learners with advanced knowledge and techniques to secure computer networks from modern threats.

WHAT YOU WILL LEARN

In the Network Security Professional Certificate course, participants will learn about various aspects of securing computer networks. They will develop an understanding of network infrastructure security, including configuring and managing firewalls, intrusion detection systems, and secure wireless networks. Participants will also explore network protocols and services security, learning how to protect against common network-based attacks. Additionally, they will gain knowledge in network access control, network monitoring, and incident response, and the fundamentals of cryptography. By the end of the course, participants will be equipped with the skills to identify network security risks, implement preventive measures, and respond to security incidents effectively.

COURSE SKILL SET

- Understanding the importance of cybersecurity
- Knowledge of different types of cyber threats and attack methods
- Familiarity with security policies and procedures
- Ability to design and implement secure architectures for systems and networks
- Understanding network protocols, OSI layers, and IP addressing
- Knowledge of common hacking methodologies and techniques
- Familiarity with incident management and response processes
- Understanding and implementing cybersecurity controls and frameworks

- Conducting penetration testing and vulnerability assessments
- Knowledge of computer forensics principles and investigation techniques
- Understanding the role and configuration of firewalls
- Awareness of web application security vulnerabilities and mitigation techniques
- Familiarity with risk management principles and methodologies
- Knowledge of network security controls and intrusion detection systems
- Understanding the legal and regulatory aspects of cybersecurity.

PROGRAM HIGHLIGHTS

Instructor- Ajay Gautam | Cyber Security Expert
Duration- 2 Months
Eligibility- Any graduate with a Science stream
No. of Modules – 15 Modules
Language - English
Shareable certificate- Yes

CURRICULUM

Module 1 Introduction to Cybersecurity

session 1.1 Why Cyber Security is Important?
session 1.2 Role of cyber security enginner
session 1.3 CIA Triad
session 1.4 The Hacking Methodology
session 1.5 The WhoIS Query
session 1.6 Social Engineering
Live Session
session 1.7 Brute Force Attacks
session 1.8 Phishing
session 1.9 Bots and Botnets
session 1.10 DoS and DDoS
session 1.11 Pings
session 1.12 Man in the Middle Attacks (MITM)
Live Session

Module 2 Cyber Security Building blocks

session 2.1 Malicious Codes and Terminologies
session 2.2 Cybersecurity Breaches
session 2.3 Penetration Testing and Methodologies
session 2.4 Frameworks and Standards for Cybersecurity
Live Session

session 2.5 Hardware and Software Elements of Computer Systems
session 2.6 Introduction to Networks and Reference Models
session 2.7 OSI layers
session 2.8 Network Protocol
session 2.9 IP Address and Subnet Classes
session 2.10 Network Devices
Live Session

Module 3 Basic concepts of Vulnerability

session 3.1 Types of Hackers & Hacktivism
session 3.2 Understanding Terminologies
session 3.3 Vulnerability & Pentesting
session 3.4 Cyber Security Controls
session 3.5 Cyber Security Policies
session 3.6 CVE & CVSS
Live Session

Module 4 Security Basics

session 4.1 What is Cyber Kill Chain?
session 4.2 Reconnaissance & Weaponization
session 4.3 Delivery & Exploitation
session 4.4 Installation, Command and control (C2) & Actions on Objectives
Live Session

Module 5 Python Scripting Project1 - Port Scanner
Live Session

Module 6 Architecture and Design

session 6.1 Compare and Contrast Cryptographic Ciphers
session 6.2 Cryptographic Modes of Operation
session 6.3 Manage Certificates and Certificate Authorities -Part 1
session 6.4 Manage Certificates and Certificate Authorities -Part 2
session 6.5 Implement PKI Management -Part 1
session 6.6 Implement PKI Management -Part 2
session 6.7 Summarize Authentication Design Concepts -Part 1
session 6.8 Summarize Authentication Design Concepts -Part 2

session 6.9 Implement Knowledge-Based Authentication
session 6.10 Implement Authentication Technologies (JWT, SAML, OAUTH)
session 6.11 Summarize Biometrics Authentication Concepts
session 6.12 Identify Management Controls
session 6.13 Implement Account Policies
session 6.14 Implement Authorization Solutions - Part 1
session 6.15 Implement Authorization Solutions - Part 2
session 6.16 Importance of Personnel Policies - Part 1
session 6.17 Importance of Personnel Policies - Part 2
session 6.18 Importance of Personnel Policies - Part 3
Live Session

Module 7 Cyber Security Frameworks

session 7.1 Introduction to NIST Framework
session 7.2 Using NIST Framework
session 7.3 Real World Case Studies
session 7.4 Introduction To Cobit Framework
session 7.5 Principles
session 7.6 Cobit - Governance and Managing Objectives
session 7.7 Business cases
session 7.8 ISO Standard
session 7.9 Implementation Over IT
session 7.10 Fundamentals of PCI-DSS
session 7.11 PCI DSS History
session 7.12 Anatomy Of Payment Flow
session 7.13 Payment Attacks - Indian Perspective
Live Session

Module 8 Network Security Introduction to network attack

session 8.1 ARP poisoning
session 8.2 ARP Poisoning with ARPspoof & Ettercap
session 8.3 ARP Poisoning with Berrtercap
session 8.4 DNS spoofing
session 8.5 Introduction to Sniffing
session 8.6 Sniffing tools & Countermeasures
session 8.7 Session Hijacking
session 8.8 Introduction to DOS & DDOS Attacks
session 8.9 Introduction to Firewalls
session 8.10 Intrusion Detection systems

Module 9 Computer Forensics

session 9.1 Computer Forensics investigation process
session 9.2 Data Acquisition & Duplication
session 9.3 Introduction to Windows Forensics
session 9.4 Lab: Capturing Windows Memory
session 9.5 Browser Forensics using Encase
session 9.6 Lab: WebHistorian
session 9.7 Memory Forensics
session 9.8 Lab: Analysing USB data
session 9.9 Lab: Analysing Malware using Volatility
session 9.10 Introduction to Indian Cyber Law
Live Session

Module 10 Case study and application in industries
Live Session

Module 11 Virtual private network (VPN)

session 11.1 Introduction
session 11.2 Why VPN, Analogy and tunneling
session 11.3 IP tunneling
session 11.4 TUN/TAP Virtual Interface
session 11.5 Create TUN/TAP Interface - Part 1
session 11.6 Create TUN/TAP Interface - Part 2
session 11.7 How Packets Return
Live Session

Module 12 BGP and Attacks

session 12.1 Introduction
session 12.2 Autonomous Systems and Peering
session 12.3 How BGP Works
session 12.4 Path Selection
session 12.5 IBGP and IGP
session 12.6 Overlapping Routes
session 12.7 IP Anycast
session 12.8 BGP Tools and Utilities
session 12.9 BGP Attacks
session 12.10 Case Studies of BGP Attacks
Live Session

Module 13 Firewalls

session 13.1 Firewalls – Host-based, network-based and virtual
session 13.2 Netfilter
session 13.3 Comodo Firewall
session 13.4 Building a simple firewall
session 13.5 Windows - Host Based Firewalls - Windows Firewall
session 13.6 Windows - Host Based Firewalls - Windows Firewall Control (WFC)
session 13.7 Windows - Host Based Firewalls - Third Party
session 13.8 Linux - Host Based Firewalls - iptables
session 13.9 Linux - Host Based Firewalls - UFW, gufw & nftables
session 13.10 Use iptables to Build Source NAT
session 13.11 Use iptables to Build Destination NAT
session 13.12 Using iptables' Match and Target Extensions
session 13.13 Mac - Host based Firewalls - Application Firewall & PF
session 13.14 Mac - Host based Firewalls - pflist, Icefloor & Murus
session 13.15 Mac - Host based Firewalls - Little Snitch
session 13.16 Network based firewalls - Routers - DD-WRT
session 13.17 Network based firewalls - Hardware
session 13.18 Network based firewalls - pfSense, Smoothwall and Vyos
session 13.19 Stateful Firewall and Connection Tracking
session 13.20 Bypassing Firewalls Using SSH and VPN Tunnels
Live Session

Module 14 Wireless and Wi-Fi security

session 14.1 Introduction
session 14.2 Wi-Fi Weaknesses - WEP, WPA, WPA2, TKIP and CCMP
session 14.3 Wi-Fi Weaknesses - Wi-Fi Protected Setup WPS, Evil Twin and Rouge AP
session 14.4 Wi-Fi Security Testing
session 14.5 Wireless Security - Secure Configuration and Network Isolation
session 14.6 Wireless security - RF Isolation and Reduction
session 14.7 Wireless security - Who is on my Wi-Fi Network?
Live Session

Course 15 Job roles

session 15.1 Engineer Trainee
session 15.2 Security Analyst
Live Session

AISECT LEARN
Better Education. Better Careers.

Sign up for

Webinars, Free courses and Paid Courses

starting from ₹**499/-** onwards only

Contact Us

+91 9111177800

learn@aisectlearn.com

www.courses.aisectlearn.com