

Cybersecurity Foundation

An Industry recommended and validated course aligned to SSC NASSCOM Cybersecurity Foundation curriculum

Self Paced Program

Duration:
42+ hours

Price:
INR 11,681
(inclusive of taxes)



Overview

Total Curriculum Duration: **42+ Hours**

Number of Videos: **100+**

Video Duration: **40 hours**

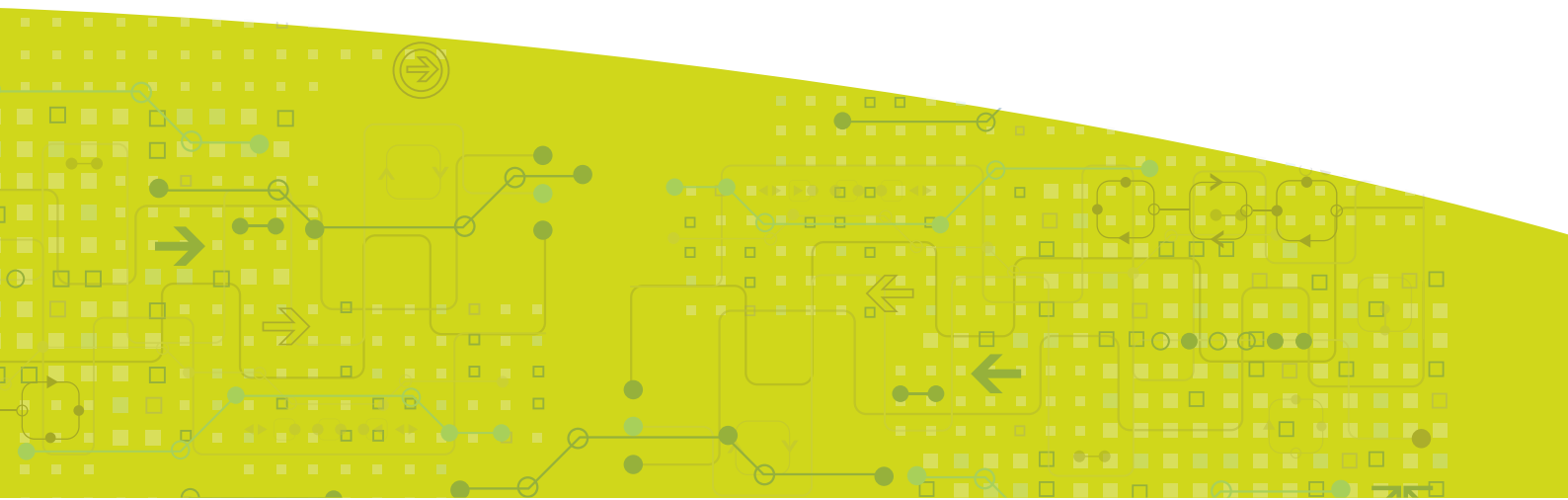
Assignment

- ✓ Number of Auto Graded Assessments: **6 MCQ type**
- ✓ Number of Self Practice Exercises in Videos: **5**

Assignment Duration: **9 hours**

Student Effort: **51+ hours**

Tools Covered: **Kali Linux, nmap, metasploit, wireshark**



Description

Cybersecurity Fundamentals teaches you the foundational concepts, theory, and techniques you need to know to become an effective cybersecurity expert. The course starts by covering fundamentals of cybersecurity, networking and then moves to security testing, incidence management and security operations.

Pearson's Cybersecurity Fundamentals is aligned to the model curriculum designed by NASSCOM- Sector Skills Council for graduates and working professionals. The course is created and taught by globally renowned experts in the field of Cybersecurity ensuring world class content. The self-paced videos cover practical exercises which provide extensive hands-on practice within the course environment. Auto graded MCQ type quizzes are also embedded within the course for regular self-assessment.





Highlights



Leading Instructors: Learn from internationally renowned Cybersecurity experts



Flaunt Your Skills: Receive a certificate from Pearson, the world's leader in professional learning, and showcase your skills



Technology in Action: Concepts are demonstrated with plenty of real-life use cases



Learn Anytime, anywhere: Learn at your pace on any device for minimum disruption to your job and family life

Learning Outcomes

The course is divided into 6 modules covering different levels of cybersecurity fundamentals. These are:

-  **Fundamentals of Cybersecurity:** This module covers the history of cybersecurity, information security and different types of attacks
-  **Fundamentals of Networking:** This module covers basic concepts of networking protocols, devices, firewalls etc.
-  **Basics of Security Testing:** This module covers various security testing techniques and introduction to ethical hacking
-  **Fundamentals of Access Management:** This module covers identity and access management, CIA triad and best practices followed under access management
-  **Fundamentals of Incident Management and Response:** This module covers fundamental concepts of Incidence monitoring, identification, disaster mitigation etc.
-  **Fundamentals of Security Operations:** This module covers fundamentals of security forensics, continuous monitoring, data loss prevention and other tools

Who should take this course:

- ✓ University students enrolled in streams such as Engineering, Computer Science, Sciences or Mathematics
- ✓ Employed professionals who wish to explore their career options and interests with regards to Cybersecurity and Information Security
- ✓ Enthusiasts curious about understanding the hype behind Cybersecurity

Curriculum

Module 1

Fundamentals of Cyber Security

- a) Definition of Cyber Security and its importance in the present scenario
- b) Popular security events in the history of Cyber Security
- c) Different disciplines of Cyber Security (such as application security, network security, data security, end-point security etc.)
- d) Difference between Information Security and Cyber Security
- e) Definition of CIA (Confidentiality, Integrity and Availability) Triad in Information Security
- f) Definition of cyber security threats and their types
- g) Types of malwares (such as Worms, Virus, Trojan Horse, Rootkit, Ransomware, Spyware, Adware, Logic Bomb etc.) and their characteristics
- h) Types of Cyber Security Attacks and their applications (such as DDoS/DoS attack, SQL injection attack, Phishing, Eavesdropping attack etc.)
- i) Basics of enterprise architecture and components (Networks, Security Controls, Servers, etc.)





Fundamentals of Networking

- a) Basic concepts of Networking, Network Ports and Network Protocols
- b) Fundamental concept of OSI (Open System Interconnection) model and TCP/IP (Transmission Control Protocol/Internet Protocol) model
- c) Fundamental concepts of network infrastructure and firewall
- d) Understanding of different types of network devices (such as Modem, Hub, NIC, Switch, Router, Repeater, Bridge etc.)
- e) Basics of Ping and Traceroute
- f) Types of network categories (such as Local Area Network (LAN), Wide Area Network (WAN), Virtual Private Network (VPN) etc.) and their components
- g) Demonstrate how to set up a LAN (Local Area Network) network using a standard router and 3-4 personal computers installed with Windows/ Linux based operating system. Demonstrate how to look for IP Address and MAC addresses of devices connected in the network. Explain how to change the IPv4/IPv6 addresses of devices and systems connected to the network.
- h) Basics definitions of key networking terminologies (such as MAC Address, IP Address, DNS (Domain Name System) etc.)
- i) Types of internet protocols (such as IPv4, IPv6 etc.)
- j) Basics of network sharing and subnetting

Curriculum

Module 3

Basics of Security Testing

- a) Definition of security testing
- b) Importance of security testing and its real world implication
- c) Basics concepts of Security Auditing test and its applications
- d) Types of popular security testing tools and their applications
- e) Basics concepts of Vulnerability Scanning test and its applications
- f) Basics concepts of Security Scanning test and its applications
- g) Basics concepts of Penetration test and its applications
- h) Definition of Ethical Hacking and its application and its applications
- i) Basics concepts of Risk Assessment test and its applications
- j) Basics concepts of Posture Assessment test and its applications
- k) Fundamentals of network monitoring for threats
- l) Demonstrate how to penetrate a dummy website using standard web penetration tool. One can use Vega tool found in Kali Linux for this. Similarly demonstrate how to scan for vulnerabilities in the website using a standard vulnerability assessment tool. One can also use OWASP tool found in Kali Linux for this purpose.





Fundamentals of Access Management

- a) Definition of Identity and Access Management
- b) Importance of Identity and Access Management in Information Security and Cyber Security
- c) Basic understanding of user Identification and Access Management policies
- d) Best practices followed under access management
- e) Demonstrate Identity and Access Management in practise using standards tools provided by a public cloud platform provider (such as AWS, Azure, Google Cloud etc.). Demonstrate how to create access policies and enable or disable access for specific users.
- f) Basic concepts of User Identification, Authentication and Authorization
- g) Basic access control models
- h) Types of security authorizations and encryptions
- i) Basics of Single Sign On (SSO) authentication

Curriculum

Module 5

Fundamentals of Incident Management and Response

- a) Basic understanding of different types of security controls and their applications (such as deterrence, detection, prevention, correction etc.)
- b) Definition of a security policy and security policy frameworks
- c) Basic definitions of Incident management and Incident response
- d) Definition of an incident response plan and incident communications plan
- e) Fundamental concepts of incident monitoring and identification
- f) Definition of a back and recovery plan
- g) Fundamental concepts of disaster mitigation and containment
- h) Basic definitions of Business Continuity Planning and Disaster recovery
- i) Basic concepts of RTO (recovery time objective) and RPO (recovery point objective)
- j) Types of cyber security investigation (such as operational investigation, criminal investigation, civil investigation and regulatory investigation)
- k) Demonstrate how to create a disaster recovery plan for a web application where the database server is affected by a malware. Use standards software, tools and packages such as MySQL, Linux, Apache etc. to create the web application and back-up for the web application's database.





Fundamentals of Security Operations

- a) Fundamentals of security forensics
- b) Types of security forensics (such as System and file forensics, network forensics, software forensics, embedded device forensics etc.)
- c) Understanding of system logging and security monitoring
- d) Fundamentals of continuous security monitoring
- e) Techniques used for continuous security monitoring (such as anomaly analysis, trend analysis, behavioural analysis, availability analysis etc.)
- f) Basics of data loss prevention and its importance
- g) Basic understanding of change and configuration management
- h) Types of tools used for security monitoring
- i) Deploy a standard web application and demonstrate how to monitor different systems (such as network, servers etc.) using standards security information and event management (SIEM) tools. (such as IBM QRadar, Splunk Enterprise Security etc.)

Faculty Details



Sari Greene

Cybersecurity Excellence Award Winner
| Author | Entrepreneur | Educator



Omar Santos

Principal Engineer
Cisco Product Security Incident
Response Team (PSIRT)



Contact us:

ppp.edge@pearson.com

in.pearson.com/ppp

Call us: 0124 – 4185100

Pearson Professional Programs,
Vatika First Indian Place, Tower C,
Ground Floor (Near M.G. Road
Metro Station), Gurugram, India