edureka!
Discover Learning

Cybersecurity Certification Course

Course Curriculum : Your 8 module Learning Plan

https://www.edureka.co/cybersecurity-certification-training

About Edureka

Edureka is a leading e-learning platform providing live instructor-led interactive online training. We cater to professionals and students across the globe in categories like Big Data & Hadoop, Business Analytics, NoSQL Databases, Java & Mobile Technologies, System Engineering, Project Management and Programming. We have an easy and affordable learning solution that is accessible to millions of learners. With our students spread across countries like the US, India, UK, Canada, Singapore, Australia, Middle East, Brazil and many others, we have built a community of over 1 million learners across the globe.

About Course

Learn Cybersecurity concepts from scratch with Edureka's Cybersecurity Certification Course. Throughout the course, you will learn important concepts such as ethical hacking, cryptography, computer networks & security, application security, idAM (identity & access management), vulnerability analysis, malware threats, sniffing, SQL injection, DoS, session hijacking, and various security practices for businesses along with hands-on demonstrations. Join this Cybersecurity Certification course and get certified as Cybersecurity Expert.

Curriculum

Introduction to Cybersecurity & Ethical Hacking

Learning Objective: In this module, you will learn about the essential building blocks and basic concepts around cybersecurity such as Confidentiality, Integrity, Availability, Security Architecture, Security Policies, and so on. In addition to these concepts, you will also explore the core topics such as Security Governance, Audit, Compliance and Security Architecture.

Topics:

- Need of Cybersecurity
- CIA Triad
- Security Architecture
- Security Governance
- Security Auditing
- Regulations & Frameworks
- Ethical Hacking
- Types of Hackers
- Phases of Ethical Hacking
- Penetration Testing
- Types of Penetration Testing
- Footprinting
- Objectives of Footprinting
- Types of Footprinting
- Footprinting Techniques

Hands-On/Demo:

- Footprinting a website using Whois Lookup, netcraft, and shodan
- Gathering information about Domain through Reon-ng Tool in Kali Linux

- Gathering information about Domain through Maltego Tool
- Gathering information about Sub-domain through Sublist3r and dnsmap tool in Kali linux
- Email Footprinting using eMail Tracker Pro
- DNS Footprinting using DNS Interrogation Tools

Cryptography

Learning Objective: In this module, you will learn various forms of cryptographic techniques, their pragmatic relevance & weaknesses. You will learn how cryptography, its components, methods, and its usage are employed in the enterprise to store and transmit messages safely.

Topics:

- Types of cryptography
- Symmetric cryptography
- Asymmetric cryptography
- Hash functions
- Digital signatures
- Public Key Infrastructure (PKI)
- Attacks on cryptosystems

Hands-On/Demo:

- Generating and identifying hashes
- Signing a file with digital signatures

Computer Networks & Security

Learning Objective: In this module, you will glance over various aspects related to computer networks and in-parallel delve into understanding the weaknesses & concepts around securing the networks.

Topics:

- Introduction to Computer Network
- Computer Networks - Architecture
- Layered architecture
- Open Systems Interconnect (OSI) Model
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Network Scanning
- Enumeration
- Common Network Threats/Attacks

Hands-On/Demo:

- Identify the Network Routes in the System
- DNS lookup and reverse lookup
- Network Path tracing
- Network Analysis
- Network scanning
- Enumeration

Application and Web Security

Learning Objective: In this module, you will learn the importance of Application-level security. You will also explore various known application weaknesses, techniques to attack them, and various controls/solutions to these vulnerabilities. You will also get an overview of countermeasures that can be employed to protect from different threats.

Topics:

- Web server architecture
- Web server attacks

- Countermeasures and patch management
- Web application architecture
- Web application attacks

Hands-On/Demo:

- Capturing session ID with Burp Suite
- Local File Inclusion on bWAPP

IdAM (Identity and Access Management)

Learning Objective: In this module, you will learn about the aspects related to the principle of Identity & Access Management. This module covers various intricacies around concepts of authorization, authentication, identity & access management, and its benefits to an enterprise.

Topics:

- Authentication and authorization
- Authentication and authorization principles
- Regulation of access
- Access administration
- IdAM
- Password protection
- Identity theft

Hands-On/Demo:

- Adding and granting permissions to users in Linux
- Identifying phishing websites

Vulnerability Analysis & System Hacking

Learning Objective: In this module you will learn how to analyze a system for various vulnerabilities. You will also learn various strategies and methodologies to gain access to the system.

Topics:

- Vulnerability Analysis
- Types of Vulnerability Analysis
- Vulnerability Assessment Lifecycle
- Vulnerability Assessment Tools
- Vulnerability Scoring Systems
- Vulnerability Assessments Report
- System Hacking
- Password Cracking
- Privilege escalation
- Executing Applications
- Hiding Files
- Clearing Logs

Hands-On/Demo:

- Find the vulnerabilities of the host/website using the Nessus tool
- Find the vulnerabilites on target website/ host using Nikto scanner
- Password Breaking – Ophcrack
- Password Breaking - Konboot Tool
- Install keyloggers and configure the victim PC to monitor the system on keystrokes and screenshots

Sniffing and SQL Injection

Learning Objective: In this module, you will learn concept of malwares, its propagation techniques, its types, concept of sniffing, types of sniffing attacks, SQL injection & its types, and SQL injection methodologies.

Topics:

- Malware and its propagation ways
- Malware components
- Types of malware
- Concept of sniffing
- Types of sniffing
- Types of sniffing attacks
- SQL injection
- Types of SQL injection
- SQL injection Methodologies

Hands-On/Demo:

- Create a trojan by using msfvenom
- Sniff network packets Using Wireshark
- MAC Flooding Using macof
- DHCP attack using Yersinia
- Bypass Authentication using SQL Injection
- Determine how the hackers may get the database of a website and steal the credentials of users from website vulnerability

DoS and Session Hijacking

Learning Objective: In this module, you will gain an overview of DoS and DDoS attacks, session

hijacking and its types, working of the intrusion detection system, and the concept of honeypots.

Topics:

- DoS attack
- DDoS attack
- Common symptoms of DoS/DDoS attack
- Categories of DoS/DDoS Attack Vectors
- DoS/DDoS detection techniques
- Session hijacking
- Application level session hijacking
- Network level session hijacking
- Intrusion Detection System (IDS)
- Types of Intrusion Detection Systems
- Introduction to Firewalls
- Types of Firewalls
- Introduction to Honeypots
- Evading IDS

Hands-On/Demo:

- DoS Attack using LOIC Tool
- Cross-site Scripting attack
- Demonstration on cookie stealing

Project

What are the system requirements for this Cybersecurity Course?

The system requirement for this course is:

- System with an Intel i3 processor or above
- Minimum 4GB RAM
- Operating system can be of 32bit or 64 bit

How will I execute the Practicals in this Cybersecurity Certification Training?

- The practicals will be executed on Kali and Windows VM. A step by step installation guide is provided on the LMS for setting up the environment.

Which Demos will be part of this course?

- Footprinting a website using Whois Lookup, netcraft, shodan, Reon-ng, Maltego, Sublist3r and more
- Identifying hashes and signing a file with digital signatures
- Network Scanning
- Enumeration
- Access management of users on Linux
- Finding vulnerabilities using Nessus and Nikto
- Password cracking using Ophcrack & Konboot Tool
- Creating a trojan, mac flooding, DHCP attack and more
- Sniffing credentials using Wireshark
- SQL Injection attack

- DoS attack using LOIC
- Session Hijacking

Which project is part of this Cybersecurity Training Course?

- **Problem Statement:** A web development company configured its network with many devices and started working on website development. As every organization requires a penetration tester to identify the loopholes in their network which an attacker/hacker can take advantage of, the organization hires you for this role. As a pen tester, you need to perform penetration testing on all their client's systems and websites. To test the systems' security, you must:
- Verify/analyze how the system is getting affected by creating a virus/trojans and injecting it into the system
- Ensure that the information transferred through email by the employees of the organization is safe
- Make a report of all the tests and share it with the administrator to take further actions