edureka!
Discover Learning

CYBER SECURITY
CERTIFICATION COURSE

Course Curriculum : Your 9 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

Edureka's Cybersecurity Certification Course will help you in establishing a strong foundation towards your journey in the Cybersecurity domain. As part of this Cybersecurity course, you will be learning about the various fundamental concepts about Security essentials, Cryptography, Network Security, Application Security, Data & Endpoint Security, Cloud Security, Cyber Attacks and Identity & Access Management.

Curriculum

Security Essentials

Learning Objective: In this module, you will learn about the essential building blocks and basic concepts around cyber security such as Confidentiality, Integrity, Availability, Authentication, Authorization, Vulnerability, Threat & Risk 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 Cyber Security
- CIA Triad
- Vulnerability, Threat and Risk
- Risk Governance & Risk Management
- Security Architecture
- Security Governance
- Security Auditing
- Compliance
- Computer Security Architecture & Design

Hands On/Demo::

- Data Breaches
- Internet Threat Scenario

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:

- Background of Cryptography
- Symmetric Cryptography
- Data Encryption Standard (DES)
- Triple-DES
- The Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)
- Blowfish
- RC4
- RC5
- RC6
- Asymmetric Cryptography
- The Diffie-Hellman Algorithm
- RSA
- Elliptic Curve Cryptosystems (ECC)
- Cryptographic Hash Functions
- Attacks against Encrypted Data
- Digital Certificates and its Format (X.509, X.500)
- Certificate Authority, Certificate Repository, Certificate Revocation lists
- Digital Certificate life cycle (Initialize, Issue, Cancel)

Hands On/Demo::

- Image Steganography
- Hashing

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:

- Network architecture, protocols, and technologies: Layered architecture, Open Systems Interconnect (OSI) Model
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Hybrid TCP/IP Model
- Application Layer Protocols: HTTP, SNMP, DNS, POP, SMTP
- Transport layer protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
- Network/Internet layer protocols: Internet Protocol (IP) v4, IPv6, IPsec protocols
- Link layer protocols: Address Resolution Protocol (ARP) / Reverse ARP / Proxy ARP, Ethernet, VLAN

Hands On/Demo::

- Sniffer
- IP Address

Application Security

Learning Objective: In this module, you learn the importance of Application level security. You will glance over various known application weaknesses, techniques to attack them and various controls/ solutions to these vulnerabilities. You will also get an overview of Secure SDLC methodology.

Topics:

- Importance of Application Security
- OWASP Top 10 web application vulnerabilities
- SSDLC (Secure Software Development Life Cycle)

Hands On/Demo::

- SQL Injection
- Buffer Overflow

Data & Endpoint Security

Learning Objective: In this module, you will glance over, various aspects related to data and endpoint (host) security. This being a primary need, is a very crucial topic.

Topics:

- Data Security
- Data Security Controls
- Endpoint Security
- Host/ Endpoint Security Controls

Hands On/Demo::

- Computer Monitoring
- System Recovery

IdAM (Identity & Access Management)

Learning Objective: Identity and access management (IdAM) is the security discipline that enables the appropriate individuals to access the right resources at the right times for the right reasons. IdAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet the increasingly rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise. Enterprises that develop mature IAM capabilities can reduce their identity management costs and more importantly, become significantly more responsive in supporting new business initiatives.

In this module you will glance over, various aspects related to the principle of Identity & Access Management. This covers various intricacies around concepts of Authorization, Authentication,

Identity & access management and its benefits to an enterprise.

Topics:

- Authorization
- Authentication
- Access Control
- Privilege levels
- IAM life cycle
- Identity & Access Management Process and activities (Role Based, Single Sign on)

Hands On/Demo::

- Password Management
- Phishing

Cloud Security

Learning Objective: In this module you will glance over a vast topic of securing the cloud! You will first have an overview of types of cloud infrastructure and then delve into security concerns & potential solutions.

Topics:

- Cloud Computing Architectural Framework
- Concerns & Best Practices
- Governance and Enterprise Risk Management
- Legal Issues: Contracts and Electronic Discovery
- Compliance and Audit Management
- Information Management and Data Security
- Interoperability and Portability
- Traditional Security, Business Continuity, and Disaster Recovery

- Data Centre Operations
- Incident Response
- Application Security
- Encryption and Key Management
- Identity, Entitlement, and Access Management
- Virtualization
- Security as a Service

Hands On/Demo::

- Virtual Machine
- Cloud based Application Vulnerabilities

Phases of a Cyber Attack

Learning Objective: In this module, you will gain an overview of the techniques & controls involved during various phases of a cyber-attack.

Topics:

- Phase 1 —Reconnaissance: Adversary identifies and selects a target
- Phase 2 —Weaponize: Adversary packages an exploit into a payload designed to execute on the targeted computer/network
- Phase 3 —Deliver: Adversary delivers the payload to the target system
- Phase 4 —Exploit: Adversary code is executed on the target system
- Phase 5 —Install: Adversary installs remote access software that provides a persistent presence within the targeted environment or system
- Phase 6 —Command and Control: Adversary employs remote access mechanisms to establish a command and control channel with the compromised device
- Phase 7 —Act on Objectives: Adversary pursues intended objectives e.g., data exfiltration, lateral movement to other targets

Hands On/Demo::

- Footprinting
- Scanning and Enumerating

Security Processes in practice for Businesses

Note: This is a self-pacedmodule

Learning Objective: A business primarily is about making profits via achieving set targets and by catering best to customers and keeping shareholders and investors happy. This involves huge number of complex and interdependent discrete processes to run smoothly, efficiently and in a well monitored way. Today IT being one of the core enablers & also an increasingly major business platforms – threats are more than likely to cause enough disruption that may cause the business to derail completely.

In this module we will glance over a variety of such business processes - to appreciate the relation, applicability and practicability of various information/ cyber security and risk management concepts that may be put in place to help the business stay predictable, safer and within a controlled cyber risk profile thereby enabling it to continue chasing its set targets.

Topics:

- Key Security Business Processes
- Corp. & Security Governance
- IT Strategy management
- Portfolio/Program/Project management
- Change management
- Supplier (third party) management
- Problem management
- Knowledge management
- Info-sec management
- BCP
- IT Operations management

- Overview of top 20 security controls

Hands On/Demo::

- Honeypot
- Website Mirroring

Project

What are the system requirements for this Cybersecurity Online Course?

The requirement for doing practicals on the Cybersecurity course is a system with Intel i3 processor or above, minimum 8GB RAM and 20 GB HDD Storage

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

For Practicals, we will provide you a virtual machine with Linux OS as the client which you can setup using the detailed installation guides provided in the LMS. In case you come across any doubt, the 24*7 support team will promptly assist you.

Which Case Studies will be part of this course?

The following Case studies will be a part of this course:

Case Study 1:

Statement: Data Encryption: - Encrypt and decrypt a file using Advanced Encryption Package.

Case Study 2:

Statement: Intrusion Detection System (IDS): - Install and configure network intrusion detection

system using SAX2 IDS

Case Study 3:

Statement: Personal Firewall: - Protect the system by installing and configuring the Zone Alarm Firewall

Case Study 4:

Statement: Password Changing: - Changing Windows password when it is lost using Active Password Changer

Case Study 5:

Statement: Network Scanning: - Monitoring and study network traffic using Wireshark

Which Projects are a part of this Cybersecurity Training?

The following is the problem statementof the certification project as part of this Cybersecurity Certification training:

John is a security administrator with ABC Inc. He was trying to log in on the system used by one of the employees who was terminated recently. The employee had changed the system admin password before leaving the organization. John has a task to get the admin access back by resetting the password. John has to change the password without using any third-party tool due to organization's security policy. Once the password is changed, he has to make sure that the same issue doesn't occur again. He also enhances the system security as follows:

Anti-Malware: He finds out that the earlier user has installed some malicious tools on the system. Using a good antivirus, he finds out malware and clean the system

System Hardening: To enhance the security he hardens the system by enabling/disabling some of the services on the computer

Firewall: John modifies some rules of the firewall to block some type of traffic

Cryptography: He also creates a hidden encrypted volume to store confidential data on the computer. He uses the existing features of the system to create the encrypted volume

Virtual Private Network: John wants the user of the system to access websites using VPN