Cyber Security Course Curriculum

Module 1

Introduction to Cyber Security

1. What is cyber security?
2. Need for cyber security (case studies)
3. statistics
4. Layered approach to cyber security

Objective

- The objective of this chapter is to understand the concept of cyber security along with its need in day to day life.
- Layered-security approach is about maintaining appropriate security measures and procedures at five different levels within your IT environment.

Theory / Practical

Theory

Duration

2 Hours

Latest Technological Trends

1. Introduction to IoT
2. How the Internet of Things (IoT) Is Changing the Cybersecurity Landscape?
3. Threats and Countermeasures of IoT and BYOD
4. Cyber security concerns and solution in Smart City & Home Automation

Objective

- By including IoT and BYOD student will get into insight of latest technological advancement in Cyber security as well as in technology. Also student will understand cyber security is playing vital roll in these technology by pointing threats.

Theory / Practical

Theory

Duration

1 Hour

Basics of Networking

1. GET MAC,NCPA.CPL, cmd line
2. Obtaining IP address from DHCP Server
3. IP address: types of IP's, Classes of IP's.
4. IPV4 and IPV6 address
5. Sharing Files and Folders

Objective

- To get familiarize with an OS and its Basic Settings, File management in OS
- To learn the comparison between Linux and Windows

Theory / Practical

Theory and Practical

Duration

4 Hours

Introduction to virtualization and installation of OS on virtual Box.

1. Introduction to virtualization.
2. Installation of virtual box
3. Installation of OS.

Objective

- To get introduced to virtual application system and the sequence of booting file.
- To learn basic concepts of networking

Theory / Practical

Duration

Module 2

Introduction to Cyber Security

1. What is password?
2. Types of passwords :
   - BIOS password.
   - System password :
     - Administrator password.
     - User password.
3. Passwords storage – windows and Linux.
4. Types of passwords attacks.

Objective

- This chapter will give complete idea of Passwords and are extremely important aspect of security policy. They are the front line of protection for user accounts.
- How one can safeguard his system by setting strong password

Theory / Practical

Theory and Practical

Duration

3 Hours

Web browser Security

1. Understanding web browsers.
2. Security features of different web browsers.

- Internet Explorer.
- Google Chrome.
- Firefox Mozilla.
- Opera.

Objective

- This chapter will give complete understanding of web browsers.
- This will explain security settings and features of different web browsers which will be very useful for users to secure his web browsing activities.

Theory / Practical

Theory and Practical

Duration

2 Hours

Firewall And UTM

1. Understanding the Firewall.
2. What exactly Unified Threat Management Is?
3. Use of Firewall and UTM.
4. Advantages and Disadvantages of UTM.

Objective

- This chapter covers the firewall as a security measure and its types.
- Different firewall techniques which are useful for data protection. One can select the technique as per own requirement.
- UTM is single hardware platform blended with layers of threat protection.
- Protect your network using multi-layered proven protection technologies including Advanced Threat Protection (ATP), IPS, VPN, email and web filtering combined with the industry's simplest admin interface.

Theory / Practical

Theory

Duration

1 Hour

Module 3

Physical Security

1. Understanding physical security
2. Need for physical security.
3. Physical security equipments :
   - Close circuit television cameras (CCTV) :
     - Analogue cameras.
     - Digital cameras.
   - Biometrics :
     - Fingerprint.
     - Iris.
     - Retina.
     - Face.
     - Security tokens.
     - Smart card.

Objective

- The objective of this chapter is to understand physical security and its need.
- For application of physical security we are going to study some security equipments like CCTV cameras and biometrics system.
- This will help to implement physical security in any organization.

Theory / Practical

Theory

Duration

1 Hour

Mobile Security

1. Different Mobile platforms.
2. Mobile security features.
3. Applications of mobile security.
4. Different security options in mobile like encryption etc.

Case studies.

Objective

- This chapter covers different mobile platforms. Different applications used for mobile security.
- How to create mobile hotspots.

Theory / Practical

Theory and Practical

Duration

2 Hours

Module 4

Email Security

1. What is E-mail?
2. Understanding how Email works.
3. Types of Email.
4. Email Security :
   - How to set up spam filters?
   - Prevent yourself from phishing.
   - Use encryption.

Keep your computer updated.

Objective

- This chapter covers details of electronic mail.
- How E-mail works and its types.
- E-mail Tracing includes how to identify fake mail through Email header analysis.
- Email security includes how to secure emails by setting spam filters, by using encryption etc.

Theory / Practical

Theory and Practical

Duration

4 Hours

Module 4

Malware

1. What are Malwares?
2. Different types of Malwares like viruses, Worms, Trojans, Adwares, Spywares.
3. Ransomware Rootkits, and Keyloggers etc.
4. How to secure system from malware?

Objective

- In this topic students will be able to understand different types of malwares.
- This chapter includes very important area that how to secure yourself from Malwares?

Theory / Practical

Theory and Practical

Duration

2 Hours

Module 5

Cryptography

1. Understanding cryptography
2. Goals of cryptography
3. Cryptographic methods :
   - Rotation
   - Substitution :
     - Mono-alphabetic substitution.
     - Poly-alphabetic substitution.
   - Transposition.
4. Types of cryptography :
   - Symmetric key cryptography.
   - Asymmetric key cryptography.
5. Use of Hash function in cryptography.

Digital Signature in cryptography.

Objective

- The objective of this chapter is to understand the science of cryptography.
- In cryptography we will cover security along with cryptographic methods and types of
  cryptography.

Theory / Practical

Theory and Practical

Duration

3 Hours

Module 6

Wireless Security

1. Concept of Wireless Networks
2. Security Features of WiFi
3. Wireless Encryption Protocols :
   - WEP
   - WPA
   - WPA2
4. Wireless Attacks and Countermeasures

Objective

- Wireless Security will be given an insight view of wireless networks and their security parameters to the students.

Theory / Practical

Theory and Practical

Duration

2 Hours

Module 7

Ethical Hacking

1. Concept of Ethical Hacking.
2. Ethical hacking steps.
   - Reconnaissance :
   - Active reconnaissance.
   - Passive reconnaissance.
   - Scanning :
   - Port scanning.
   - Network scanning.
   - Vulnerability scanning.
   - Gaining Access.
   - Maintaining Access.
   - Covering Tracks.

Objective

- The objective of this topic is to understand the difference between hacking and ethical hacking.
- How ethical hacking is used for security purpose.
- In this chapter we are going to cover steps of ethical hacking in detail.

Theory / Practical

Theory and Practical

Duration

4 Hours

Module 8

Virtualization and Cloud Computing

1. Basic Concept of Virtualization
   - Types of Virtualization
   - Benefits
2. Data Center Virtualization
3. Desktop Virtualization
4. Virtualizing Enterprise Application
5. Network Virtualization
6. Server Virtualization
7. Load Balancing with Virtualization

Cloud computing :

1. Definition of cloud
2. Cloud Architecture
3. Advantages of cloud
4. Risks involved in cloud computing.
5. Cloud Storage
6. Cloud Services :
   - Software As Service (SAS)
   - Platform As Service (PAS)
   - Infrastructure As A Service
7. Public Cloud Environment

Objective

- Virtualization is latest technology. With knowledge of Virtualization, one physical server can be made to act as many virtual servers. It offers a range of benefits, which is reducing the number of physical servers an organization needs.
- Cloud computing is a general term for anything that involves delivering hosted services over the Internet, Distributed Computing.
- With this chapter, student will clear with concept, Requirement, Application of cloud.

Theory / Practical

Theory and Practical

Duration

2 Hours

Module 9

Cyber Crime and Cyber Laws

1. What are cyber-crimes?
2. Types of cyber-crimes.
    - Password related crimes
    - Email related crimes
    - Desktop related crimes
    - Social networking sites related crimes
    - Website related crimes
    - Network related crimes.

Social engineering related crimes

1. Categories of Cyber Crime
    - Individual
    - Property
    - Government
2. Online Banking
    - Online banking frauds

Safety tips for online banking

Objective

- This chapter will educate the students regarding
- Cyber-crimes related to day to day activity of students on internet.
- Different categories of cyber-crimes and how one should be careful while handling the internet.
- How One should be careful while doing online banking.

Theory / Practical

Theory

Duration

1 Hours

Cyber laws (Information Technology Act 2000)

1. What is cyber law?
2. Evolution of cyber law in India.
3. Jurisdiction of IT Act
4. Penalties under IT Act.
5. Difference between civil law and criminal law
6. Offences under IT Act- some sections :
   Section 43, Section 65, Section 66, Section 67, Section 72, Section 69, Section 79.
7. Intellectual Property Rights (IPR).

Objective

- Through this chapter students will understand what cyber laws are and how different sections are applicable for different cyber-crimes.
- By teaching cyber laws we try to create awareness among students regarding penalties under different sections.

Theory / Practical

Theory

Duration

1 Hours

Module 10

ISO 27001

1. Introduction to ISO 27001
2. General requirements for ISO standardization.
   - Methodological requirements
   - Security control requirements.
3. Different corporate policies.

Implementation and establishment of ISMS

Objective

- This chapter will cover ISO standardization for information security.
- For any size of company which are the general requirements to take ISO standard.
- How to establish and implement information security management system

Theory / Practical

Theory

Duration

1 Hour

Module 11

IP based communication: (VOIP)

1. Introduction
2. How VoIP worked?
3. Requirements, Availability and
4. Service Limitation
5. Threat or Risk
6. Countermeasures
7. Media gateway control
8. Protocol
9. SIP (Session Initiation Protocol)

Objective

- It is new technology that improves
- Internet communication.
- This topic will brief on its function & some of its Application like Skype etc.

Theory / Practical

Theory

Duration

1 Hour

Module 12

Protection of information Assets BC/DR Planning & Development

1. Explain Disaster.
2. Types of Disaster.
3. Risks Involved.
4. Disaster recovery.
5. BCDR Plan Steps
6. Basic of Business Continuity Plan
7. Benefits of BCP and DRP Planning
8. BCP Process Steps
9. Development of Business Continuity Plan

Objective

- The objectives of a business continuity plan (BCP) are to minimize financial loss to the institution; continue to serve customers and financial market participants.
- Also on development model this chapter focused on how to get the business up and running in the event that a specific facility or function is disrupted, rather than on the precise nature of the disruption.

Theory / Practical

Theory

Duration

2 HourS

Total - 40 Hours