Certificate Course in Cyber Security Essential - Practical approach- 100 Hours

Course Objective

The objective of this course is to provide the students a detailed knowledge in the field of Cyber security. The students will learn the fundamental ideas behind cyber security, the evolution of the paradigm, its applicability, benefits, as well as current and future challenges.

Target Audience

Technical Graduates / Working Professionals / Faculty / Government officials having knowledge in IT domain or willing to work in IT domain.

Eligibility Qualification

Any Engineering / Science graduate with mathematics up to 10+2 level; 2+ Year of experience in IT Domain

Course Outcome

The students will be provided an overview of networking and its maintenance, TCP/IP cyber security, network defence and web application and overview of cryptography and will help the students to make carrier in Network management and cyber security.

Reference Books

1. Networking Fundamentals: Wide, Local and Personal Area Communications: Kaveh Pahlavan, Prashant Krishnamurthy /Wiley India Pvt Ltd
2. TCP/IP Network Administration: Craig Hunt/Shroff Publishers and Distributors Pvt.ltd
3. Network Defense and Countermeasures: Easttom/Pearson Education
4. Cryptography & network Security: Principles and Practices, 4/e: William Stallings/Pearson

Teaching Schema

Sl. No.	Modules	Hours
1	Windows Environment	**05**
2	Linux Environment	**10**
3	TCP/IP Cyber Security Perspective	**10**
4	Security Threats and Vulnerabilities	**15**
5	Overview of Network Defence & Web Application Security	**20**
6	Web Application Security	**20**
7	Cryptography and Network Security	**10**
8	OS Hardening	**10**
	Total	**100**

Detailed Course Content

***

1. **Windows Environment**

- User account
- Basic commands
- File management etc

2. **Linux Environment**

- Introducing Linux,
- Installing Linux
- Distributions
- Devices and drives in Linux
- File system Hierarchy
- How user preferences are stored in your home directory
- Updating your system with up2date / yum.
- The command-line (shells, tab completion, cd, ls)
- file management: cd, df, find, locate
- Adding users, groups
- su - the obsoleted way to become the root user.
- All basic commands and etc

3. **TCP/IP Cyber Security Perspective**

- Describe OSI Layers and TCP/IP suite of layers
- Describe the need of layers
- Describe the difference between layers
- Describe the layers wise protocols

4. **Security Threats and Vulnerabilities**

- Understand the vulnerabilities and security threats
- Understand stages of attack
    - Information Gathering
    - Scanning
    - Vulnerability Analysis
    - Exploit systems
    - Covering Tracks
- Tools used at attack stages

5. **Overview of Network Defence & Web Application Security**

- Network Components (Firewall, IDS, Router)
- Defensible Network Architecture
- Introduction to Perimeter Security
- What is a Firewall?

- Why do you need firewall?
- Types of firewalls
- What can a firewall do?
- Is a firewall sufficient to secure network?
- What can a firewall not do
- Describe what is a Perimeter Security?
- Describe what are Perimeter Security devices?
- Describe why we use so many devices?
- Describe about the purpose and limitations of
- Perimeter Defenses
- Describe the challenges and Perimeter Design
- Describe defense in depth

6. **Web Application Security**
   - HTTP Basics
   - Introduction to Web Application Security & its importance
   - Information Gathering
   - SQL Injection
   - Cross Site Scripting
   - Session Mismanagement
   - Insecure Direct Object Reference

7. **Cryptography and Network Security**
   - Cryptography and its Applications
   - Network Security and Protocols for Secure Communication
   - Digital signature concept
   - Apache SSL concept

8. **OS Hardening**

- Process of securely configuring the system
- Correcting misconfiguration
- Disabling unnecessary & vulnerable services
- Make system more reliable
- Protect system from exploits and attacks

References

• https://www.pcisecuritystandards.org/pci_security/main

taining_payment_security

• https://www.sciencedirect.com/topics/computerscience/incident-response-process

• https://www.sans.org/readingroom/whitepapers/incident/incident-handlers-handbook33901