CYBERSECURITY COURSE OUTLINE.

Duration: 6months

***duration for specific modules may differ**

1. **Introduction**
2. **Information Security Threats and Vulnerabilities**
   a. Overview of threat Sources
   b. Overview of threat actors/agents
   c. Understanding malware and its types
   d. Overview of vulnerabilities
   e. Understanding different types of vulnerabilities
   f. LABS :
      i. Creating a trojan to gain access to a target system
      ii. Creating a virus to infect the target system
      iii. Creating a worm using the internet worm maker thing
      iv. User system monitoring and surveillance using spytech spyagent(and other tools)
      v. Finding vulnerabilities on exploit sites
   g. Quiz
3. **Information Security Attacks**
   a. Overview of Information security attacks
   b. Overview of hacking methodologies and frameworks
   c. Understanding network-level attacks
   d. Understanding Network-level attacks
   e. Understanding Application-level and OS-level Attacks

f. Understanding Social Engineering Attacks
g. Understanding Wireless Network-specific Attacks
h. Understanding IoT, OT and Cloud Attacks
i. Understanding Cryptographic Attacks
j. LABS:
    i. Perform a MITM Attack using Cain & Abel
    ii. Perform MAC Flooding using macof
    iii. Perform a DoS attack on a target host using hping3
    iv. Perform an SQL injection attack against MSSQL to extract databases using sqlmap
    v. Perform parameter tampering using John-the-ripper
    vi. Perform Social Engineering using Various techniques to sniff user's credentials
    vii. Crack a WPA2 Network using Aircrack-ng
    viii. Hack an Android Device by Creating Binary Payloads
    ix. Exploit Open s3 Buckets using AWS CLI

4. Network Security Fundamentals

a. Overview of Information Security Fundamentals
b. Overview of Network Security Fundamentals

5. Identification, Authentication, and Authorization

a. Overview of Access Control Principles, Terminologies and Models
b. Overview of Identity and Access Management(IAM)
c. LABS:

        i. Implementation of Access Controls on Windows Machine
        ii. Managing Access Controls in Linux Machine
        iii. Implementation of Role-Based Access Control in Windows Admin Center (WAC)
        iv. Implementation a Centralized Authentication Mechanism

6. Network Security Controls – Administrative Controls

    a. Understanding various regulatory frameworks, laws and acts
    b. Overview of Information Security Governance and Compliance Program
    c. Designing and development of Security policies
    d. Conducting different types of security and awareness training
    e. LABS:
        i. Implementation of Password Policies using Windows Group Policy
        ii. Implementation of Auditing Policies
        iii. Implementation of a secure network policy
        iv. Implementation of a Power shell security policy

7. Network Security Controls – Physical Controls

    a. Understanding the importance of physical security
    b. Understanding various physical security controls
    c. Overview of Workplace security
    d. Understanding Various environmental controls

8. Network Security Controls – Technical Controls

a. Overview of essential network security protocols
b. Understanding security benefits of network segmentation
c. Understanding different types of IDS/IPS and their role
d. Understanding different types of honeypots
e. Understanding different types of proxy servers and their benefits
f. Overview of VPN and its importance in network security
g. Overview of other network security controls
h. Understanding importance of load balancing in network security
i. Understanding various antivirus/anti-malware software
j. LABS:
    i. Implementation of Host-based firewall protection and Host-based firewall functionality
    ii. Blocking access to unwanted website and insecure ports using pfSense firewall
    iii. Implementation of Host-based IDS functionality and Network based IDS functionality
    iv. Detecting malicious traffic in the network using HoneyBOT
    v. Configuring VPN connection using tools such as SoftEther VPN

vi. Scanning the System for Viruses using Kaspersky Internet Security.

9. Network Security Assessment techniques and tools

a. Overview of threat hunting

b. Understanding various threat intelligence feeds and sources

c. Overview of vulnerability assessment

d. Overview of ethical hacking concepts

e. Penetration testing fundamentals and their benefits

f. Configuration management and asset management

g. LABS:

i. Collecting Data through Search Engines

ii. Gathering Threat Intelligence Feed using threatfeeds.io

iii. Performing vulnerability research in common weakness enumeration(CWE)

iv. Perform a vulnerability assessment to identify security vulnerabilities in the target system or network

10. Application Security

a. Understanding Secure Application Design and architecture

b. Understanding software security standards, models and frameworks

c. Understanding secure application, development, deployment and automation

d. Overview of application security testing techniques and tools

e. LABS:

   i. Implement Application Whitelisting using AppLocker

   ii. Blacklist Application using ManageEngine Desktop Centra

   iii. Perform Application Sandboxing using Sandboxie

   iv. Detecting Web application vulnerabilities using OWASP ZAP

   v. Detect injection vulnerability using burpsuite

   vi. Determine Application-Level Attacks

   vii. Perform Web Server Footprinting using Various footprinting tools.

11. Virtualization and Cloud Computing

a. Overview of virtualization essential concepts and OS Virtualization

b. Overview of Cloud Computing Fundamentals

c. Understanding the Insights of Cloud Security and Best Practices

d. LABS:

   i. Auditing Docker Host Security using Docker-bench-Security Tool

   ii. Create IAM Credentials on the Google Cloud Platform

   iii. Implement Key Management Services in AWS

   iv. Secure Amazon Web Services Storage

12. Wireless Network Security

a. Overview of wireless network fundamentals
b. Overview of wireless network encryption mechanisms
c. Understanding different types of wireless network authentication methods
d. Understanding and implementing wireless network security measures
e. LABS:

- **i.** Configure security on a wireless router

13. Mobile Device Security

a. Understanding Various Mobile Device Connection Methods
b. Understanding Various Mobile Device Management Concepts
c. Overview of Common Mobile Usage Policies in Enterprises
d. Overview of Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies.
e. Understanding and Implementing Various Enterprise-level Mobile Security Management Solutions
f. Understanding and Implementing General Security Guidelines and Best Practices on Mobile Platforms
g. LABS:

- i. Implement Enterprise Mobile Security using Miradore MDM Solution

14. **IoT and OT Security**

a. Understanding IoT Devices, Application Areas, and Communication Models
b. Overview of Security in IoT-enabled Environments
c. Understanding OT Concepts, Devices, and Protocols
d. Overview of Security in OT-enabled Environments
e. LABS:
    i. Secure IoT Device Communication using TLS/SSL

15. Cryptography

a. Overview of Cryptographic Security techniques
b. Understanding Various Cryptographic Algorithms
c. Understanding Various Hash Functions and Cryptography Tools
d. Overview of PKI and Certificate management concepts
e. Understanding Other applications of cryptography
f. LABS:
    i. Calculation of One-way Hashes using HashCalc
    ii. Calculation of MD5 Hashes using MD5 Calculator
    iii. Calculation of MD5 Hashes using HashMyFiles
    iv. Encryption and Decryption of data using BCTextEncoder
    v. Creating and using self-signed Certificates
    vi. Creating anD Managing Certificates using OpenSSL
    vii. Image Steganography using OpenStego

16. **Data Security**

   a. Understanding Data security and its importance
   b. Understanding Various Data security Controls
   c. Overview of Data Backup, retention, and destruction
   d. Overview of data loss prevention concepts
   e. LABS:
      i. Performing Disk Encryption using BitLocker Drive Encryption
      ii. Performing Disk Encryption using VeraCrypt
      iii. Implementation of Built-in File System-level Encryption on Windows
      iv. Performing Data Backup using Genie Backup Manager
      v. File Recovery using EaseUS Data Recovery Wizard
      vi. Back-Up and Restore Data in Windows
      vii. Perform Data Destruction using Windows DiskPart Utility

17. Network Troubleshooting

   a. Overview of Network Troubleshooting
   b. Learn Troubleshooting Basic Network issues using Utilities and Tools
   c. LABS:
      i. Network Troubleshooting using command line utilities and tools
      ii. Network Troubleshooting using Nmap
      iii. Network Troubleshooting using Hping3
      iv. Access the Remote Machine using PuTTY

18. **Network Traffic Monitoring**
    a. Understanding the Need and Advantages of Network Traffic Monitoring
    b. Understanding Baseline traffic Signatures for Normal and Suspicious Network Traffic
    c. Performing Network Monitoring for Suspicious Traffic
    d. LABS:
        - **i.** Interception of network traffic using wireshark and tcpdump
        - **ii.** Apply various filters in wireshark
        - **iii.** Analyze and examine various network packet Headers in Linux using tcpdump
        - **iv.** Scan Network to Identify Hosts in the Local Network

19. **Network Logs Monitoring and Analysis**
    a. Overview of Logging Concepts
    b. Understanding Log Monitoring and Analysis on Windows Systems
    c. Understanding log monitoring and analysis on Linux
    d. Understanding Various Log Management Tools
    e. LABS:
        - **i.** Configure, View and Analyze Windows Event Logs
        - **ii.** View and Analyze Windows logs
        - **iii.** View and Analyze Linux Logs

20. **Incident Response**
    a. Overview of Incident Response Concepts

b. Understanding the Role of First Responder in Incident Response

c. Overview of Incident Handling and Response Process

d. LABS:

   i. Conduct Security checks using buck-security on Linux

   ii. Analysis and validation of malware incident

   iii. Implementation Policies using group policy management console

21. Computer Forensics

a. Understanding the fundamentals of computer forensics

b. Understanding Digital Evidence

c. Identify the roles and responsibilities of a forensic investigator

d. Understanding the forensic investigation process and its importance

e. Understanding various forensic investigation phases

f. Understanding digital evidence sources to support forensic investigation

g. Collecting the evidence

h. Securing the evidence

i. Overview of Data acquisition

j. Performing evidence analysis

k. LABS:

   i. Create a Disk Image file of a hard disk partition

   ii. Acquire RAM from Windows Workstation

iii. Create a Disk Image File of a Hard Disk Partition
iv. Analyze the file system of a linux image using autopsy
v. Capture and analyze memory dump on Linux
vi. View Contents of forensic image file

22. Business Continuity and Disaster Recovery

a. Understanding Business Continuity(BC) and Disaster Recovery (DR) concepts
b. Overview of BC/DR Activities
c. Understanding Business Continuity Plan(BCP) and Disaster Recovery Plan (DRP)

23. Risk Management

a. Understanding Risk Management Concepts
b. Understanding Various risk management phases
c. Understanding Various risk management frameworks