Master all Concepts of CYBER SECURITY!

Module 01

INTRODUCTION TO CYBERSECURITY

1.1 Overview of Cybersecurity

- **Overview:** Definition, scope, and impact in today's digital age.
- **Why it Matters:** Data breaches, identity theft, and infrastructure protection.
- **Security Triad (CIA):** Confidentiality, Integrity, Availability in real-world scenarios (e.g., data leaks, ransomware attacks, service disruptions).

1.2 Cyber Threats and Vulnerabilities

- **Types of Cyber Threats:** Insider Threats, Phishing, Supply Chain Attacks, Malware, APTs.
- **Real-World Case Studies:**
  - Equifax breach (2017)
  - WannaCry ransomware (2017)
- **Advanced Persistent Threats (APT):**
  - Nation-state examples (e.g., Stuxnet, SolarWinds).

1.3 Cybersecurity Frameworks and Standards

- **NIST and ISO 27001 in practice:** Real-world implementation examples for small and large organizations.
- **CIS Controls:** Implementing CIS controls in cloud environments.

Add-on Practical Lab:

- **Case Study Analysis:** Students research and dissect well-known security breaches, identifying vulnerabilities and threats, and map them to NIST and CIS controls.

Module 02

UNDERSTANDING VIRTUALIZATION & LAB SETUP

2.1 Introduction to Virtualization

- **Types of Virtualization:** Full Virtualization, Para-Virtualization, OS-Level Virtualization
- Benefits and Applications in Cybersecurity

2.2 Lab Environment Setup

- **Virtualization Tools:** VirtualBox, VMware
- Creating and Configuring Virtual Machines

2.3 Lab Environment Management

- Managing Virtual Labs for Penetration Testing and Learning

Course Curriculum

Module 03

LINUX FUNDAMENTALS

3.1 Linux Basics

- **Overview of key distributions used in cybersecurity:** Ubuntu (user-friendly), CentOS (server-focused), and Kali Linux (penetration testing).
- **Differences between various distributions and their use cases.**
- **Basic Linux Commands**
  - **Navigation:** ls, cd, pwd for navigating directories.
  - **File Operations:** cp, mv, rm, touch for file manipulation.
  - **Viewing Files:** cat, less, more, tail.

3.2 Linux File System and Permissions

- **Linux Directory Structure and File System Hierarchy**
  - **Exploring key directories:** /etc, /var, /home, /bin, /usr.
  - Understanding how the Linux file system is organized.
- **Managing File Permissions**
  - **Permission Types:** Read, write, and execute permissions for files and directories.
  - **Changing Permissions:** Using chmod to modify file and directory permissions.
  - **Changing Ownership:** Using chown to change file owners and groups.

3.3 Text Editors

- **CLI Based**
  - **Nano Editor:** A beginner-friendly terminal-based text editor with on-screen instructions.
  - **Vi Editor:** A powerful and lightweight command-line text editor with modes for editing.
- **GUI Based**
  - **Gedit:** A simple yet versatile GUI text editor for GNOME, ideal for general-purpose editing.
  - **Mousepad:** A lightweight GUI text editor for XFCE, designed for quick and efficient text editing tasks.

3.4 User and Group Management

- **Creating Users and Groups**
  - Adding users with useradd, assigning passwords with passwd.
  - Creating groups with groupadd and adding users to groups.
- **Managing Users Privileges**
  - Granting root privileges through sudo and modifying the /etc/sudoers file

Course Curriculum

Module 04

NETWORKING FUNDAMENTALS

4.1 Basic Networking Concepts

- **Types of Networks**
  - **LAN (Local Area Network):** Small, local networks like in homes or offices.
  - **WAN (Wide Area Network):** Large networks spanning cities, countries (e.g., the Internet).
  - **WLAN (Wireless LAN):** Wireless networks typically using Wi-Fi.
  - **MAN (Metropolitan Area Network):** Networks that span cities or large areas.
- **IP Addressing**
  - **IPv4: Structure** (e.g., 192.168.x.x), limited addresses.
  - **IPv6:** Next-gen addressing, structure (e.g., 2001:0db8:85a3::), increased scalability.
  - **IP Address Types:** Public vs. Private, Static vs. Dynamic, CIDR notation.

4.2 Networking Models

- **OSI Model**
  - **Seven Layers**: Physical, Data Link, Network, Transport, Session, Presentation, Application.
  - **Functions**: How data is transmitted and received across a network at each layer.
- **TCP/IP Model**
  - **Four Layers:** Link, Internet, Transport, Application.
  - **Functions**: Practical focus on data transmission and routing across the Internet.

4.3 Network Protocols and Ports

- **Common Protocols**
  - **HTTP/HTTPS:** Web traffic, with HTTPS providing encrypted communication.
  - **DNS:** Resolving domain names to IP addresses.
  - **SSH:** Secure remote command-line access.
  - **FTP:** File transfer over a network.
- **Common Port Numbers**
  - HTTP (80), HTTPS (443), DNS (53), SSH (22), FTP (21).
  - Role of Ports in Networking and Common Port Numbers.

4.4 DNS and Domain Names

- **DNS Records:** A, AAAA, CNAME, MX, TXT, PTR records and their uses.
- **Zone Files:** How DNS servers store domain information.
- **HTML Requests and Responses:** How web browsers request resources from servers.

Course Curriculum

Module 05

ETHICAL HACKING

5.1 Social Engineering

- **Techniques**
  - **Phishing:** Tricking users into providing sensitive information by impersonating legitimate entities, often via email or fake websites.
  - **Pretexting:** Crafting false scenarios or identities to manipulate victims into disclosing information.
  - **Baiting:** Offering enticing items (e.g., free downloads, USB drives) to gain unauthorized access to systems or personal information.
  - **Tailgating/Piggybacking:** Gaining physical access to restricted areas by following authorized personnel.
  - **Scareware:** Using fake warnings or threats (e.g., "Your system is infected!") to manipulate victims into downloading malicious software or providing sensitive information.

5.2 Denial of Service (DOS) & Distributed Denial of Service (DDOS)

- **Methods and Techniques**
  - **Flood Attacks:** Overwhelming network resources (e.g., bandwidth or server capacity) by sending massive amounts of traffic, rendering the system unusable.
  - **SYN Flood:** Exploiting the TCP handshake process to flood a target with incomplete connection requests.
  - **Amplification Attacks:** Using vulnerable systems to send a large volume of responses to a victim by exploiting network protocols (e.g., DNS Amplification, NTP Amplification).
  - **Botnets:** Using a network of infected computers (zombies) to coordinate large-scale DDoS attacks.

5.3 Wireless Network Hacking

- **Attacking Wireless Networks**
  - **WEP/WPA Cracking:** Exploiting weaknesses in older encryption protocols like WEP and WPA by capturing data packets and decrypting them using tools such as Aircrack-ng.
  - **Deauthentication Attacks:** Forcing devices off the network by sending fake deauth frames, often used in combination with password cracking.
  - **Rogue Access Points:** Setting up fake wireless access points to intercept user data.

Course Curriculum

- **Securing Wireless Networks**
  - **WPA2/WPA3 Encryption:** Implementing the latest encryption standards to protect wireless communications.
  - **Strong Passwords and PSKs:** Using complex, randomly generated passwords to protect wireless networks.
  - **MAC Address Filtering:** Limiting network access by only allowing specific MAC addresses to connect.
  - **Disabling SSID Broadcast:** Hiding the network's SSID (though not a foolproof solution).

5.4 System Hacking

- **Vulnerability Exploitation:** Identifying and exploiting flaws in the Windows OS or installed software (e.g., unpatched systems, zero-day exploits).
- **Remote Code Execution (RCE):** Gaining control over a system by exploiting vulnerabilities that allow arbitrary code execution.
- **Man-in-the-Middle (MitM) Attacks:** Intercepting network communications to capture sensitive data.

5.5 Android Hacking

- **Mobile Application Security**
  - **Android Architecture:** Understanding the structure of Android OS, including components like the Linux kernel, system libraries, and application framework.
  - **Security Risks:** Recognizing common vulnerabilities in Android applications, such as Insecure Data Storage, Improper Access Control, and Insecure Communication.
- **Tools for Testing Android Applications**
  - **APKTool:** A tool for reverse engineering Android apps by decompiling APKs and modifying them for further analysis.
  - **MobSF (Mobile Security Framework):** An automated security testing tool for Android apps that provides dynamic and static analysis.
  - **Drozer:** A comprehensive Android security assessment framework that helps identify vulnerabilities and misconfigurations in Android apps and devices.

5.6 Password Cracking Tools

- **John the Ripper:** A popular tool for password cracking through brute force or dictionary attacks.
- **Hashcat:** An advanced password recovery tool that supports GPU-accelerated attacks on various types of password hashes (MD5, SHA, etc.).
- **Rainbow Tables:** Precomputed hash tables used to crack encrypted passwords quickly by matching hashes.

Course Curriculum

Module 06

CRYPTOGRAPHY

6.1 Introduction to Cryptography

- **Basic Concepts**
  - **Encryption vs. Decryption:** Protecting and recovering information.
  - **Symmetric Encryption: O**ne key for encryption and decryption (e.g., AES).
  - **Asymmetric Encryption:** Public and private key pairs (e.g., RSA).
- **Common Cryptographic Algorithms**
  - **AES:** Advanced Encryption Standard for symmetric encryption.
  - **RSA:** Public-key cryptosystem for secure data transmission.
  - **SHA:** Secure Hash Algorithm used for integrity verification.

6.2 Cryptographic Protocols

- **TLS/SSL**
  - Ensuring secure communication over the Internet (e.g., HTTPS).
  - Understanding handshakes and certificates.
- **IPsec:**
  - Securing IP communications by authenticating and encrypting each IP packet.

Module 07

PENETRATION TESTING

7.1 Penetration Testing Phases

- **Information Gathering & Reconnaissance**
  - **Objective:** Identify the target's digital footprint and accessible resources.
  - **Techniques:**
    - Open Source Intelligence (OSINT) gathering.
    - DNS lookups, IP geolocation, and social media analysis.
  - **Tools:**
    - **TheHarvester:** Gathers email accounts and subdomains.
    - **Recon-ng:** A web reconnaissance framework.
    - **WHOIS:** For domain registration information.
    - **Shodan:** Search engine for Internet-connected devices.
    - **Dmitry:** Provides a detailed domain information report.
    - **Google Dorks:** Uses advanced search queries to find vulnerabilities.
- **Scanning & Enumeration**
  - **Objective:** Identify live hosts, open ports, and services.

Course Curriculum

- **Techniques:**
  - **Host Discovery:** Identify active hosts on the network.
  - **Port Scanning:** Identify open ports and associated services.
  - **Service Enumeration:** Gather detailed information about services running on open ports.
  - **Active Vulnerability Scanning:** Actively probe systems for known vulnerabilities.
  - **Passive Vulnerability Scanning:** Monitor network traffic to detect potential vulnerabilities without directly interacting with systems.
- **Tools:**
  - **Nmap:** Network scanning and port enumeration.
  - **Nikto:** Web server vulnerability scanner.
  - **Netcat:** Networking utility for reading and writing data across networks.

- **Exploitation**
  - **Objective:** Gain unauthorized access to systems.
  - **Techniques:**
    - Buffer overflows.
    - SQL injection.
    - Privilege escalation.
  - **Tools:**
    - **Metasploit:** Framework for developing and executing exploits.
    - **SQLmap:** Automated SQL injection tool.
    - **Hydra:** Password-cracking tool.
- **Post-Exploitation**
  - **Objective:** Maintain access and gather intelligence.
  - **Techniques:**
    - Pivoting.
    - Data exfiltration strategies.
  - **Tools:**
    - **Mimikatz:** Extracting passwords from memory.
    - **Empire:** PowerShell post-exploitation framework.
- **Reporting & Remediation**
  - **Objective:** Document findings and suggest security improvements.
  - **Techniques:**
    - Creating detailed penetration test reports.
    - Recommending security patches and mitigations.

Course Curriculum

7.2 Web Application Penetration Testing

- **Common Vulnerabilities**
  - SQL Injection, Cross-Site Scripting (XSS), CSRF, OS Command Injection, Directory
  - Traversal, Server-Side Request Forgery (SSRF), and more.
- **Advanced Testing for LFI/RFI**
  - Techniques for testing and exploiting Local File Inclusion (LFI) and Remote File
  - Inclusion (RFI) vulnerabilities.

7.3 Mobile Application Penetration Testing

- **Introduction to Android Application Testing**
  - Understanding APKs and mobile security models.
- **Techniques for Decompiling and Analyzing Mobile Applications**
  - **Decompiling APKs:**
    - Decompiling transforms APK files into readable formats, such as source code or XML, for analysis.
  - **Analyzing Security:**
    - Examine app components like Activities, Services, Broadcast Receivers, and Content Providers.
- **Tools:**
- **APKTool:** Tool for reverse engineering Android APK files.
- **MobSF:** Mobile Security Framework for security testing of mobile apps.

7.4 Network Penetration Testing

- **Vulnerability Scanning for Networks**
  - Techniques for identifying weak points in network configurations.
  - Network Forensics and Traffic Analysis
- **Tools**
  - **Wireshark:** For capturing and analyzing network traffic.
- **Wireless Network Penetration Testing**
  - Techniques for cracking WEP/WPA2 networks using tools like **Aircrack-ng**.

Module 08

SHELL SCRIPTING & AUTOMATION

8.1 Bash Scripting

- **Basics:** Writing simple scripts, understanding syntax, file permissions. Using tools like awk, grep, sed, and cut for text processing.
- **Automation:** Automating system tasks, network scans with scripts (e.g., using Nmap).

Course Curriculum

8.2 Python Scripting

- **Basics:** Python syntax, variables, loops, and functions.
- **Automation:** Writing security scripts for vulnerability scanning, interacting with APIs, and analyzing network traffic (e.g., with Scapy).

8.3 PowerShell

- **Basics:** PowerShell commands and scripting on Windows systems.
- **Automation:** Automating tasks like patch management, system audits, and information gathering.

Module 09

INCIDENT RESPONSE

9.1 Incident Response Basics

- **Steps and Procedures for Incident Handling**
  - **Preparation:**
    - Develop an incident response plan (IRP).
    - Establish roles, responsibilities, and communication protocols.
  - **Identification:**
    - Detect and confirm the presence of a security incident.
    - Utilize tools like IDS/IPS, SIEM systems, and monitoring logs.
  - **Containment:**
    - Isolate affected systems to prevent further damage.
    - Implement temporary fixes while preparing for eradication.
  - **Eradication:**
    - Eliminate the root cause of the incident (e.g., malware, unauthorized access).
    - Patch vulnerabilities and update security measures.
  - **Recovery:**
    - Restore systems to normal operation.
    - Test systems to ensure functionality and security.

Module 10

MALWARE ANALYSIS AND REVERSE ENGINEERING

10.1 Malware Analysis

- **Static Analysis :**
  - Examine the malware without executing it.
- **Techniques:**
  - Inspect file headers, strings, and embedded metadata.
  - Disassemble code to understand functionality.

- **Dynamic Analysis :**
  - Execute the malware in a controlled environment to observe behavior.
- **Techniques:**
  - Monitor file system, network, and registry activity.
  - Analyze API calls and system changes.

10.2 Reverse Engineering

- **Introduction to Reverse Engineering**
  - Reverse engineering involves deconstructing malware or software to understand its behavior, functionality, and weaknesses.
- **Use cases:**
  - Identify obfuscation techniques.
  - Extract encryption keys, hardcoded credentials, or hidden functionalities.

Module 11
DIGITAL FORENSICS

11.1 Digital Forensics

- Basics of digital forensics and its importance in cybersecurity.
- Types of digital evidence and best practices for evidence collection.

11.2 Forensic Investigation Techniques

- Disk and memory forensics for extracting critical data.
- Network and mobile forensics for analyzing cyber incidents.
- **Tools for Digital Forensics**
  - Autopsy – Open-source digital forensics platform for analyzing disk images.
  - Wireshark – Network packet analyzer for detecting suspicious activities.
  - Volatility – Memory forensics framework for extracting live system data.
  - FTK (Forensic Toolkit) – Professional forensic analysis tool for deep investigations.

Module 12
UNDERSTANDING LAYERS OF INTERNET

12.1 Overview of different layers of Internet

- **Surface Web:** The publicly accessible part of the internet, indexed by search engines like Google, Bing, or Yahoo.
- **Deep Web:** Contains content not indexed by standard search engines.
- **Dark Web:** A small portion of the deep web intentionally hidden and accessible only via specific tools like Tor (The Onion Router).

Course Curriculum

12.2 Accessing and Navigating the Dark Web

- **Tools Required:**
  - **Tor Browser:** Provides anonymity by routing internet traffic through multiple nodes.
  - **I2P (Invisible Internet Project):** Another network focused on anonymous communication

Module 13

CLOUD SECURITY

13.1 Introduction

- **Definition:**
  - Protection of cloud data, applications, and infrastructure.
- **Importance:**
  - Prevents data breaches, ensures compliance, and mitigates risks.

13.2 Shared Responsibility Model

- **Provider Responsibilities:**
  - Physical security and infrastructure protection.
- **Customer Responsibilities:**
  - Data security and access management.

13.3 Key Security Measures

- **Identity and Access Management (IAM):**
  - Implement role-based access control (RBAC).
  - Use multi-factor authentication (MFA).
- **Data Protection:**
  - Encrypt data at rest and in transit.
  - Implement Data Loss Prevention (DLP).

13.4 Monitoring and Response

- **Continuous Monitoring:** Use SIEM tools for threat detection.
- **Incident Response:** Develop a plan for handling breaches.

13.5 Best Practices

- Keep systems updated and patched.
- Conduct vulnerability assessments. ·
- Provide security awareness training for employees.