Cyber Security-Curriculum

1.CyberSecurity Fundamentals

1.1 Security Principles

- Introduction to CS theory, CIA Triad, Control Types
- Security Frameworks, Cyber Crime, Cyber Crime Laws
- Intellectual Property, Privacy, Data Breach
- Policies, Standards and Guidelines
- Risk Management Frameworks, Personnel Security
- Security Governance, Ethics
- Security Principles

1.2 Incident Response

- Breach, Event, Exploit, Incident
- Intrusion, Threat, Vulnerability, Zero Day
- Preparation
- Detection & Analysis
- Contamination, Eradication & Recovery
- Post Incident Activity
- IR Models - Leveraged, Dedicated, Hybrid

1.3 Business Continuity

- Notification Systems
- Call Tress
- RabbitMQ

1.4 Disaster Recovery

- Providing Executive Summary
- Technical GuideLines for IT Personnel
- Checklists

1.5 IAM and Access Control

- Based On - Subject (Who), Object (What) & Rules (How & When)
- Defence In Depth
- PAM (Privileged Access Management)
- Logical Access Control

1.6 Security Principles

- CIA Triad
- Risk Management
- Security Control
- Security Governance

Cyber Security-Curriculum

1.7 Network Security

Types of Computer Network

- LAN, WAN, WLAN, VPN, EPN,
- POLAN, PAN, CAN, MAN, SAN

Different Networking Devices

- Hubs, Switchers, Routers, Firewall
- Servers, Printers, Gateways, Repeaters
- Bridges, Modem, Access Points, End Point
- Packet, Port, Protocol, Ethernet, WiFi
- IP Address, Mac Address

Protocol

- IPV4 - 32 Bit
- IPV6 - 128 Bit

Network Attacks

- DOS, DDOS, Fragment, Oversized Packet, Spoofing
- Man-In-The-Middle, XSS, SQL Injection, Privilege Escalation, Insider Threat

Threats

- Spoofing, DDOS, Virus, Worm, Trojan
- MITM, Side-Channel, Phishing, Rootkits, Malware, Spyware

Network Security Infrastructure

- Power, HVAC
- Fire Suppression, Redundancy, MOU & MOA

1.8 Security Operations

- Data Handling
- Sensitivity Levels - High, Moderate, Low, Unrestricted
- Logging & Monitoring - Ingress & Egress
- Encryption - Symmetric & Asymmetric
- Cryptographic Hash
- System Hardening
- Social Engineering

2.Setting Up Kali Linux

- Setup Introduction
- Downloading All the Tools
- Install and Setup Tools Burn with Balena Etcher
- Burn with Rufus
- Live Boo2.7 Live Boot Changes and Booting
- Installing Kali on Virtualbox using ISO
- Booting into Kali Linux using Virtualbox post installation
- Troubleshooting

Cyber Security-Curriculum

3.Working with Kali Linux

3.1 Setting Up Kali Linux

- Introduction to Linux Basics - Preface
- Terminal
- Working with Directories
- Working with Files in Linux
- Directories Structure in Linux
- Additional Directories and Functionalities
- Standard In out and Error
- File Permissions in Linux

3.2 Linux Basics

- File Permissions in Linux
- Linux Environments
- Linux Utilities
- Linux Filter Helpers
- Linux Processes
- Communication Utilities
- User Management Basics

4.Setup Coding Environment and Scripting Languages

4.1 GitHub

- Git and Github Basics
- Repositories and Maintenance
- RSA Key and Other commands in Github

4.2 SQL

- Introduction to SQL and its uses in Cybersecurity
- SQL PhpMyAdmin Setup and misc
- SQL Queries and Stored Procedure

Web Technologies - HTML

- IDE Setup
- HTML Basics
- HTML Forms and its Use Cases

4.3 Web Technologies - Javascript

- Introduction to Javascript
- Javascript Use cases in CS
- Javascript Comments and Javascript Output Statements
- Javascript Variables and Constants, Data Types
- Operators, Condition Control and Looping Statements
- Functions
- Browser APIs
- Jquery

Cyber Security-Curriculum

4.4 Web Technologies - PHP

- PHP Introduction
- PHP Output Statements
- PHP Conditional, Control and Looping Statements
- PHP Functions
- Methods and Super Globals
- PHP Form Handling

4.5 Powershell

- Powershell Introduction
- Powershell Variables, Datatypes and IO Statements
- Powershell Cmdlets and Files IO
- Powershell Conditional Control and Looping Statements
- Powershell Hashtables, Regex and Backticks
- Powershell Scripting

4.6 Bash

- Bash Introduction
- Bash Datatypes and Variables
- Bash Input Variables
- Bash Operators and Conditional and Selective control statement
- Bash Looping Statements
- Bash Functions
- Bash UI Customizativon
- IP Scanner Script in Bash

4.7 Python

- Python Introduction
- Python IDE Setup and Introduction
- Python Virtualenv and Output Statements and Comments
- Python Variables and Datatypes
- Python Control and Looping Statements
- Python Functions and Misc

4.8 Lua

- Lua Setup and Introduction
- Lua Basics, Data Types and Expressions
- Lua Decision and Looping Statements
- Lua Functions

Cyber Security-Curriculum

4.9 Java

- Java Introduction and Setup
- Java IO Statements and Basics
- Java Conditional and Control and Looping Statements
- Functions and Exception Handling
- Java Networking

4.10 C

- C Introduction and Setup
- C Syntaxes and Output
- C Data Types, variables constants and output
- C Conditional and Control Statements and Looping statements
- C Functions

4.11 C++

- Introduction to C++, Comparison with C and Similarities
- C++ OOPs, Functions and Error Handling
- C++ File Handling
- C++ Network Programming

4.12 Ruby

- Ruby Introduction and Setup
- Ruby Basics and Variables
- Ruby Condition Control and Looping Statements
- Ruby Functions.mp4
- Ruby Socket Programming

4.13 Visual Basic Script

- Introduction to Visual Basic for Application
- VBA Basics
- VBA Scripting

Cyber Security-Curriculum

5.Basics of Kali Tools

5.1 Testing Machine Setup with VirtualBox and Error management for VMWare

5.2 NMAP

- Nmap Introduction and Setup
- NMAP Full with Example on Kioptrix

5.3 Metasploit

- Metasploit Introduction
- Metasploit Scanning
- Metasploit Usage

5.4 Burp Suite

- Burp Basics
- Burp Bruteforce
- Burp Scanner
- Burp Crawler
- ZAP Introduction setup and basic usage
- ZAP Brute Force
- ZAP Additional Conflicts

5.5 Nessus

- Nessus Introduction
- Nessus Scanning

5.6 Netcat

5.7 Fluxion

5.8 Lynis

- Lynis Introduction
- Lynis Scanning

5.9 Tiger

5.10 John the Ripper

- John the Ripper Introduction and Basic Scan
- John the Ripper ZIP Crack and Linux Crack

Cyber Security-Curriculum

5.11 **Hydra**

5.12 **WpScan**

5.13 **Nikto**

- Nitko Introduction
- Nitko Scanning

5.14 **Aircrack-Ng**

5.15 **Wireshark**

5.16 **Autopsy**

- Autopsy Introduction
- Autopsy Scanning

5.17 **King Phisher**

5.18 **Beef**

- Beef Introduction Setup and Setup Error Handling
- Beef Scanning and Hooking Browsers

5.19 **Skipfish**

- Skipfish Introduction and Setup
- DVWP setup for Skipfish and other Applications
- Skipfish Scanning Wordpress

5.20 **Maltego**

- Maltego Introduction
- Maltego Scanning

5.21 **SQLMap**

5.22 **Dirb**

5.23 **Reaver**

5.24 **DVWA**

- Setup Ubuntu and DVWA
- Configure DVWA

Cyber Security-Curriculum

6.Pentesting CTF Local and Remote Instances

6.1 Hack the Box Lab

- Introduction and Setup
- Hack the Box VPN Setup and Connection
- HTB Meow
- HTB Fawn
- HTB Dancing
- HTB Redeemer

6.2 VulnWeb

- Vulnweb with Kioptrix 1.

7.Web VAPT

- Web Technologies
- Pentesting Methodology
- Setting up Pentesting Lab
- Testing for OWASP Top 10 using Kali Tools
- Report Writing

8.Cybersecurity Beyond the Basics

- Deep Web in Cybersecurity
- Encryption
- Cyber Forensics
- Cyber Forensics - Practical Example
- Virus and Malware
- Session Hijacking Theory
- Session Hijacking Practical with Burp Suite and DVWA

Cyber Security-Curriculum

CAPSTONE PROJECTS

1 Web & Network Security VAPT Audit

- The Web & Network Security VAPT Audit project focuses on identifying and mitigating vulnerabilities across web applications and network infrastructures.
- Through comprehensive Vulnerability Assessment and Penetration Testing (VAPT), this project aims to discover security loopholes and provide actionable insights for fortifying system defences.
- The process involves scanning for weaknesses, exploiting potential vulnerabilities, and generating detailed reports that highlight areas of concern.
- This approach ensures that both web applications and network components are resilient against a variety of cyber threats.
- The project will also include recommendations for best practices to enhance overall security posture.

2 Android Application Penetration Testing

- This project explores the techniques and methodologies used in ethical hacking of Android mobile applications to identify security vulnerabilities.
- By simulating real-world attack scenarios, the project aims to uncover flaws in mobile app security, such as insecure data storage, improper authentication, and code vulnerabilities.
- The process involves static and dynamic analysis, code decompilation, and testing against common exploits.
- The findings will help developers understand critical security risks and implement robust measures to safeguard mobile applications.
- Ultimately, this project serves as a guide for building more secure Android applications by understanding the perspective of a potential attacker.

3 Phishing Awareness Simulation

- The "Phishing Awareness Simulation" project aims to educate users about phishing tactics by simulating real-world phishing scenarios.
- By creating realistic phishing emails and landing pages, users can observe how easily deceptive messages can lure victims into revealing sensitive information.
- The project uses a controlled environment to test the effectiveness of these simulations, providing feedback and educational material on recognizing phishing attempts.
- Through this interactive approach, users learn to identify warning signs, such as suspicious links, sender authenticity, and manipulative language, ultimately reducing their vulnerability to phishing attacks.
- This hands-on experience fosters cybersecurity awareness, emphasizing vigilance and safe online practices.

Cyber Security-Curriculum

LIVE PROJECT

1 **Forensic Analysis with Autopsy**

- The Forensic Analysis with Autopsy project provides an in-depth look into digital forensic investigations using the Autopsy software.
- It covers techniques for collecting, analysing, and preserving digital evidence from various devices, including computers, mobile phones, and external storage.
- The project aims to demonstrate how Autopsy can be utilised to trace digital footprints, recover deleted files, and analyse data structures to build a case.
- With real-world case studies, the project offers insights into the forensic workflow, from data acquisition to evidence reporting.
- It highlights the importance of maintaining the integrity of evidence and following legal protocols during an investigation.