CYBERSECURITY CURRICULUM

STARTER & FULL

A. Beginners Curriculum.

WEEK 1

Saturday: Concept of Cybersecurity

- What is Cybersecurity (Definition, terminologies, importance, and setbacks)
- The CIA Triad.
- Domains in Cybersecurity (Security Engineers, Governance and Compliance, Security operations, Risk management and Threat intelligence)
- A quiz on Cybersecurity.

Sunday: History and Standards

- Revision and discussion on lessons learnt in previous class.
- Cybersecurity History and Standards (Standards, regulations, and framework)
- MITRE ATT&CK and CYBERKILL CHAIN
- Techniques, Tactics and Procedures
- People, Process and Technologies

Week 2

Saturday: Common threats plaguing the Cybersecurity space.

- Revision and discussion on lessons learnt in previous class.
- Introduction to Cyber Threat
- Discussion on Malware (Adware, Virus, Worms, Spyware, Trojan horse, Rootkits, Ransomware and fileless malware).
- A short quiz on Malware
- Malware analysis on Any run and other platforms (Practical)

Sunday: Sophisticated attacks on devices and networks

- Phishing
- SQL injection
- Cross-site scripting
- Zero days and DDOS
- Take home assignment on topic of discussion.

Week 3

Saturday: Cryptography

- Revision and discussion on lessons learnt in previous class.
- Introduction to Cryptography (Encryption, Hashing, Decryption)
- A short quiz on how to encrypt and decrypt using different online encryptor.
- The use of Cyberchef for encoding and decoding information (Practical)

Sunday: Authorization and Authentication

- Authentication and Authorization
- User Access and Privilege Access Manager
- Rules around access control

Week 4

Saturday: Endpoint and personal security

- Introduction to personal security (Account safety and password management, MFA, Use of VPN, Message and browser security, Software update and the impact of social engineering)
- Short quiz
- Endpoint/personal hardening (Windows Hardening, Linux hardening)
- Take home assignment.

Sunday: OSINT and Mini-project assessment

- Introduction to Open Source Intelligence (OSINT)
- Review and understanding of the Eternal Blue Exploit.
- Group presentations
- Live simulations of mini project using packet tracer (Practical)
- Discussion on challenges encountered and how to do it better.

B. **Advanced Curriculum**

Week 5

Saturday: Setting up the Lab environment.

- Importation of Windows 10/11 into Virtual box
- Installation of packet tracer
- Installation of Wireshark for packet analysis
- Installation of hex editor

Sunday: Continuation

- Importation and installation of Kali Linux
- Brief introduction of the Kali Linux
- Resolving installation issues.

Week 6

Saturday: Network Basics

- Revision and discussion on lessons learnt in previous class
- Network basics (types, OSI model, TCP/IP model, Network protocols)
- Short quiz
- Setting up a device-internet connection using packet tracer (Practical)
- Configuration of switches, routers, and endpoints in a network (Practical)
- Creating a LAN, WAN and MAN network (Practical)

Sunday: Network Security

- Introduction to Network security (Firewalls, Wireless network security, packet analysis)
- Use of Wireshark for packet analysis (Practical)
- Hands on experience with Hex Editor (Practical)
- Mini-Project (Creation of packet filtering firewall rules)

Week 7

Saturday: Dark web

- What is Darkweb
- Similarities and differences between the Darkweb, Deepweb and surface web
- How to access the Darkweb (Practical)
- Forums on the dark web
- REvil team and the Lazarus team activities on the Darkweb
- Take home assignment on the different Forums on the Darkweb

Sunday: Unsecure use of application and devices

- Security effect arising from the use of unpaid/cracked software
- Disadvantages of free VPN
- Man-in-the-middle (MITM) attack
- Free/Public Wi-Fi connection and its bad sides
- Cross connection between LAN-WAN, WAN-WAN, etc. (Practical)

Week 8

Saturday: Technologies used in Cybersecurity

- Network Intrusion and Detection Systems
- Data Loss Prevention System
- File Integrity System
- Cookies and their uses
- Data Privacy and why it should be enforced on data collection websites
- Take home assignment

Sunday: Documentations in Cybersecurity

- Risk Management and documentation
    - Communication with stakeholders (users, IT Team, Security team, top management)
- Security Incidents, events, log management and monitoring (Practical)
- Incident response Playbook and reports (Practical)
- Follow up and Escalation of security incidents and its remediation

Week 9

Saturday: OWASP TOP 10

- Definition, types and listing of the OWASP Top 10 Vulnerabilities
- The use of OWASP ZAP for Vulnerability testing (Practical)
- Analysis of the vulnerabilities detected.
- How to remediate these vulnerabilities
- A short quiz on OWASP top 10

Sunday: Familiarities with Metasploit and Exploit DB

- What is Metasploit, uses and how it can be used to exploit vulnerabilities
- Exploit DB: A platform to exploit any vulnerability except zero days
- Download and Installation of Metasploit (Practical)

- The use of ExploitDB for payload injection (Practical)
- Mini-project: Infection or delivery of malicious payloads to an endpoint.

Week 10

Saturday: Business Continuity and Disaster Recovery Plan (BCDR)

- Definition, Importance and Differences
- How to develop an BCDR
- BCDR testing and implementation
- Stakeholders that determine what should be in the BCDR plan.
- Importance of availability zones.

Sunday: Case studies and looking ahead

- Cyber Breach and lessons learnt (Uber, Target and SolarWinds)
- Cybersecurity and the 2023 general election
- Digital Forensic and Incident response
- Trending topics in Cybersecurity (IoT, Cloud, AI, 5G)

Week 11

Saturday: Rubbing minds and Capstone project

- Question and Answers
- Guides and roadmap to being a Cybersecurity Professional
- Capstone project.

Class requirement:

- Windows Laptop (minimum core i3, 100GB storage space, stable internet, Mics and audio working well)
- Necessary software: Virtualbox, Kali Linux and Windows 10/11 for virtualbox, OWASP ZAP, Tor browser, hex editor, Metasploit, Packet tracer and Microsoft suite.