

CIRRICULUM FOR CYBERSECURITY

In this course learners will be taught ethical hacking from scratch . No prior knowledge is required to pursue the curriculum . At the end of the course learners would be able to identify flaws , break things down to build better solutions.

1. Introduction:

- * Course Overview
- * What , Why , when , where and hows of cybersecurity

2. Setting up a hacking lab:

- * Initial Prepration
- * Installing Kali , Tails and Ubuntu as VM on windows

3. Linux Basics:

- * Basic Overview
- * The Linux Filesystem
- * Understanding sudo and sudo su
- * The Terminal and linux commands
- * Finding Files in kali
- * Managing Kali Linux Services - SSH , HTTP , FTP
- * Installing and removing tools - apt , pip , apt-get , dpkg etc

4. Command Line Fun :

- * The bash Environment
- * Bash Scripting
- * Text Searching and Manipulation : grep , sed , cut , awk , nano , vi , comm , diff , vimdiff , etc

5. Network Hacking:

- * Introduction to penetration Testing
- * Networking Basics
- * Connecting a wireless adapter to kali

- * What is mac how to change it ?
- *Wireless Modes (Managed and Monitored)
- *Wireshark
- *tcpdump

6. Hardware for hacking:

- *Raspberry pi
- *Arduino
- *Rubber Ducky , Scripting
- * Wifi Pineapple
- *HackRF
- *OMG Cable
- *IOT for Hacking

7. Social Engineering :

- * hacking an Organisation
- * Tackticks For Hacking
- * Power of listenig
- * Demonstrations

8. Information Gathering :

- * Taking Notes
- * Website reach
- * Google hacking
- *Netcraft
- * Shodan
- *Pastebin
- *Email Harvesting
- *Password Dumping
- *OSINT Framework
- *Maltego
- *DNS Enumeration
- *Port Scanning
- *SMB Enumeration
- *SMTP Enumeration

9. Network Hacking :

- *Packet Sniffing Basics
- *Wifi Bands - 2.4Ghz and 5Ghz
- *Targetted Packet Sniffing
- *Deauthentication Attack (Disconnecting Any Device from the network)

10. Network Hacking :

- *Gaining Access introduction
- *Theory Behind Cracking WEP Encryption
- *WEP-Cracking Basics
- *Fake Authentication Attack
- *ARP Request Replay Attack

11. Network Hacking - Gaining Access - WPA/WPA2 Cracking :

- * Intro to WPA and WPA2 Cracking
- *Capturing the Handshake
- *Creating the wordlist
- *Cracking WPA and WPA2 Using a wordlist Attack

12. Network Hacking - Post Connection Attacks - Information Gathering :

- *Installing Windows as a VM
- *Discovering Devices Connected to the same network
- *Gathering sensitive info about connected devices
- *Gathering More Sensitive info

13. Network Hacking - Detection and security :

- *Detecting ARP Poisoning Attacks
- * Detecting Suspicious Activities in the Network
- * Preventing MITM Attacks - Methods

14. Website Hacking :

- * Burpsuite
- *SQL injection Attacks
- * Client Side attacks

- * Server side attacks
- *Information Gathering
- *Discovering and reporting Vulnerabilities

15. Vulnerability Scanning :

- *Overview
- *Scanning With Nessus
- *Scanning With Nmap

16. Reporting :

- * Documentation
- *Vulnerability Assessment
- *Pentesting Reports
- *Reporting and legal terminology

17. Cybersecurity Certifications:

- *eJPT
- *CEH
- * CCNA
- *OSCP
- *OSCE