Cyber Security - Ethical Hacking

Course Structure

CODENERA

MAKE IMAGINATION POSSIBLE

Syllabus

- Linux & Networking Basics – OSI, TCP/IP, DNS, NAT, Firewall
- Footprinting & Reconnaissance – Whois, Shodan, Social Media
- Scanning Networks – Nmap, Banner Grabbing, IDS Evasion
- Enumeration – NetBIOS, SNMP, LDAP, DNS, SMTP
- System Hacking – Password Cracking, Privilege Escalation, Tracks
- Malware Threats – Trojans, Worms, Analysis Lab
- Sniffing & Spoofing – ARP, MAC, DNS, DHCP Attacks
- Social Engineering – Phishing, Insider Threats, Gophish
- Web App Hacking – SQLi, XSS, CSRF, File Upload

- **Session Hijacking – Network/Application Level, Tools**
- **DoS/DDoS Attacks – Botnets, LOIC, Protection Techniques**
- **Wireless & Bluetooth Hacking – WPA2, WEP, Kismet**
- **Web Server Attacks – Patch Mgmt, Nikto, Dirb, OpenVAS**
- **Mobile Hacking – Android, iOS, Spyware, MobSF**
- **IoT Hacking – Shodan, Firmware Analysis, IoTGOAT**
- **Cloud + Cryptography – S3 Misconfig, PKI, Hashing**

Core Tools

- **Linux & Networking Basics – OSI, TCP/IP, DNS, NAT, Firewall**

VirtualBox, Kali Linux, Netstat, ifconfig
(Linux Fundamentals 1,2,3)

- **Footprinting & Reconnaissance – Whois, Shodan, Social Media**

Nmap, theHarvester, Whois, Dig
(Intro to Networking)

- **Scanning Networks – Nmap, Banner Grabbing, IDS Evasion**

Nmap (deep), Shodan (free search)
(Nmap in Depth)

- **Enumeration – NetBIOS, SNMP, LDAP, DNS, SMTP**

enum4linux, DNSenum, Netcat
(Enumeration)

- **System Hacking – Password Cracking, Privilege Escalation, Tracks**

Metasploit Framework, John the Ripper
(Metasploit)

- **Malware Threats – Trojans, Worms, Analysis Lab**

Hydra, Wireshark
(Brute It, Crack the Hash)

- **Sniffing & Spoofing – ARP, MAC, DNS, DHCP Attacks**

tcpdump, Ettercap
(Packet Analysis, Wireshark Room)

- **Social Engineering – Phishing, Insider Threats, Gophish**

SET Toolkit, Gophish
(Phishing Emails, Pre Security)

- **Web App Hacking – SQLi, XSS, CSRF, File Upload**

Burp Suite Community, SQLmap, Nikto
(OWASP Top 10, Burp Suite)

- **Session Hijacking – Network/Application Level, Tools**

OWASP ZAP, Gobuster
(Web Fundamentals)

- **DoS/DDoS Attacks – Botnets, LOIC, Protection Techniques**

LOIC (for lab), ICMP tools
(AttackBox DDoS Room)

- **Wireless & Bluetooth Hacking – WPA2, WEP, Kismet**

Aircrack-ng, Kismet
(Wireless Security Intro)

- **Web Server Attacks – Patch Mgmt, Nikto, Dirb, OpenVAS**

Nikto, Dirbuster
(Web Scanning)

- **Mobile Hacking – Android, iOS, Spyware, MobSF**

MobSF (local setup), APKTool
(Android Exploitation Basics)

- **IoT Hacking – Shodan, Firmware Analysis, IoTGOAT**

Shodan, Firmware emulators
(IoT Security Basics)

- **WCloud + Cryptography – S3 Misconfig, PKI, Hashing**

GPG, OpenSSL, Hashcat
(Intro to Crypto)

Project Title :

1. **Setup Cybersecurity Lab**

Install Kali Linux, Metasploitable2 on VirtualBox; Configure internal network

2. **Recon & Scanning Project**

Use Nmap and theHarvester to create a target profile report

3. Enumeration Challenge

Enumerate SMB, SNMP, and NetBIOS services using enum4linux

4. System Hacking Simulation

Exploit a vulnerable machine using Metasploit and escalate privileges

5. Malware Behavior Analysis
Analyze and document behavior of a sample Trojan using PEStudio and Wireshark

6. Sniffing & Spoofing Demo
Perform ARP spoofing in a controlled lab and capture login credentials

7. Phishing Simulation
Use SET Toolkit to create a phishing email and capture credentials in a demo environment

8. Web App Pen Test Report
Perform SQLi/XSS on DVWA and document findings in professional format

5. Session Hijack Lab
Demonstrate session hijacking using Burp Suite or manual cookie manipulation

6. DoS Simulation
Simulate a DoS attack using LOIC in an isolated lab and capture impact on services

7. Wireless Audit
Crack WPA2 password in test lab using Aircrack-ng and create a mitigation guide

8. Web Server Vulnerability Assessment
Run Nikto and OpenVAS on a vulnerable server and generate a risk report

9. Mobile App Analysis
Perform static analysis on APK using MobSF and identify weaknesses

10. IoT Device Footprinting
Use Shodan to gather data on exposed IoT devices and suggest countermeasures

11. Cloud Bucket Misconfig Demo
Explore misconfigured S3 buckets and demonstrate data exposure scenarios

12. Crypto Implementation Project
Use GPG and OpenSSL to encrypt/decrypt files and explain key handling