Title of Skill Course: Ethical Hacking

1. Department: Department of Forensic Science
2. Title: **Ethical Hacking**
3. Sector: Private Detective Agencies
4. Eligibility: M.Sc I Forensic Science
5. Year of implementation:

Course Structure

Skill Level	Theory Hours	Practical Hours	Total Hours	Credits	No. of students in batch
7	15	30	45	02	30

Syllabus

Learning Objectives:

1. To understand the basics of Networking.
2. To learn the different hacking methods.
3. To Study ethical hacking methods and their applications.
4. To understand the basics of Web Server attacks.
5. To gain the knowledge of social engineering.

Theory Syllabus (Contact Hrs: 15, Credits: 01)

Learning Objectives:

1. To understand the basics of Networking.
2. To learn the different ethical hacking methods.
3. To understand the basics of Web Server attacks and social engineering
4. To know the opportunities of ethical hacking in Cybercrime investigation.

Theory Syllabus (15 Hrs)

Unit I: Basics of Networking

What is networking, basic components, Client/Server model, TCP/IP model, OSI model, DHCP, MAC address, IP address, type of IP address (public/private, dynamic/static), Classes of IP, port numbers, ARP, Ping, Traceroute, Netstat, getmac, Firewall and types.

Unit II: Hacking the Web Applications- I

OWASP TOP 10, Vulnerability assessment and penetration testing lifecycle, OSINT, Information gathering, types of information gathering, enumeration, Nmap, maltego, whois, nikto, nessus, burpsuite and setting up the proxy

Unit III: Hacking the Web Applications- II

HTTP and HTTPS, GHDB, google dorking, SQL injection, Types of SQL injection, XSS, XSS types, CSRF attack, Directory Traversal, CORS attack, Privilege Escalation

Unit IV: Web Server attacks and social engineering

Dictionary attack, bruteforce attack, rainbow table attack, phishing, packet sniffing using wireshark, password cracking, ARP spoofing, DOS/DDOS and mitigation.

Practical Syllabus (30 Hrs)

List of Experiments: **24 hrs**

1. To install virtualbox and host kali linux machine.
2. To execute basic commands on kali linux using bandit CTF
3. Gathering information about the hosted web application using whois, wig, wfuzz, ping, traceroute
4. Setting up burpsuite and intercept the communication
5. Gathering information about the target system using enum4linux
6. To scan the target system and web application using different options of Nmap
7. Setting up the Nessus and Nikto tool and scan the web application for vulnerabilities
8. To perform dictionary attack on web application
9. To perform bruteforce attack on web application
10. To perform SQL attack to dump the database
11. To perform XSS attack to get sensitive information

Learning Outcomes:

1. Understand the Legal basics of Networking.
2. Distinguish Electronic & Mechanical failure.
3. Students will able be to write Forensic Data recovery Report.
4. Students will be able to acquire the multiple Professional opportunities.

Recommended Books:

1. Gerardus Blokdyk: *"Data Recovery Hardware A Complete Guide"*, 5STARCooks (16 April 2020) 2021 Edition.
2. B. R. Sharma: *"Forensic Science in Criminal Investigation & Trials",* Universal Law Publishing - An imprint of LexisNexis; Fifth edition (1 January 2014).
3. Indian Penal Code and Criminal Procedure code.

BOS Sub Committee:

1. Miss Manjushri Bagul
2. Mr. Vikram Hankare

Expert Committee:

1. Dr. C. N. Kayte
2. Mr. Aditya More

3.