Foundation Course in Digital Ethical Hacking

`

Savitribai Phule Pune University
(Formerly University of Pune)
DEPARTMENT OF TECHNOLOGY

aAbout the course:

Brief Job Description: This job role is responsible to find vulnerabilities and weaknesses in various systems. The main duties consist of testing and identifying vulnerabilities in applications, networks and computer systems, then integrating the test results into a report, recommending improvements in existing security services and upgrading testing tools.

Personal Attributes:
This job mayrequire the individual to work independently and make decisions for his / her own area of work as well as work ina team focusing on specific areas to find vulnerabilities. The individual should have a high level of analytical thinking ability, passion for information security and attention for detail, should be ethical, compliance- and result- oriented. The individual would need to work with different departments and hence should also be able to demonstrate interpersonal skills, along with willingness to undertake extensive desk research and be willing for long working hours.

1. **Aim & Objectives of the Course:**

- Demonstrate a systematic understanding of the concepts of security in a computer system or network at the policy level and the strategic policy needs that are required to be adopted
- Identify remedial techniques for every offensive attack technique.
- Analyze the unique information security posture for every level of an organization.
- Adopt a proactive approach to security for a more comprehensive protection of data as well as reputation.
- Employ industry accepted tools on different platforms to identify and analyze an organization's risks and weaknesses.
- Research on tools under development or under beta testing on their possible utility in identifying and analyzing an organization's risks and weaknesses.

2. **Title of the course:**

Foundation in Digital Ethical Hacking

3. **Abbreviation of the Course:**

CDEH

4. **Academic year in which course is to be initiated**

Academic year	Open to	Examination
2024-25	All students	End of the course

`

5. **Eligibility criteria for admission to the course:**

1st year completed of any Bachelor's degree or any Certificate OR Equivalent.

6. **Structure of the course (course duration):**

(45 Hours)

Sr. No.	Module Name	Mandatory / Optional	Estimated Size (learning Hrs)
1	Introduction to Hacking	Mandatory	1
2	Information Gathering / Vulnerability Scanning	Mandatory	3
3	Malwares	Mandatory	4
4	System Hacking	Mandatory	5
5	Sniffing	Mandatory	3
6	Web Site and Web server Hacking	Mandatory	4
7	SQL Injection and Cross-site Scripting	Mandatory	5
8	Buffer Overflow	Mandatory	3
9	Multi-Platform (cross-platform) System Hacking and Wireless Hacking	Mandatory	4
10	Mobile Pen testing	Mandatory	3
11	Network DoS and DDoS	Mandatory	3
12	Cryptography	Mandatory	4
13	Penetration Testing IDS/IPS and Firewall	Mandatory	3
			45

7. **Fee Structure:** The tuition fees or laboratory fees and other fees must be paid at the time of admission to the course. Students can opt for any one of the three learning modes The course fees is as follows.

    1. **Blended Online Learning**: Rs. 12,500=00 + GST

8. **Teaching scheme of the course (mode of teaching and learning):**

Blended Online Learning - Self-Paced

9. **Examination system:**

On successful completion of examination, students will be awarded Certificate in Digital Ethical Hacking by

the University and Skills Factory Learning Private Limited jointly. The examination pattern for this Course is as follows:

Code	Title	Type	Distribution of marks			Credits
			Internal	Univ.	Total	
CDEH	Certificate in Digital Ethical Hacking	Theory, Practical cum Assignments	30	70	100	2

Mandatory Internal and External Evaluation: The course evaluation has two components: Internal assessment for 30 marks that may contain assignment/oral/viva/internal test, etc. and the External examination which will be online mode for 70 marks.

10. Procedure for conducting External and Internal assessment:

Online assignment submission and online examination as per University Rules and schedule.

11. Grade System:

- The examination outcome will not affect the regular academic examinations.
- Students will be awarded grades on the basis of marks achieved.
- The examination will be conducted for all modules at the end of the course.
- Criteria for assessment will be created by Skills Factory Learning Pvt Ltd (SFLPL). Each performance criterion@ (PC) will be assigned Theory and Skill Based Practical marks proportional to its importance in the module.
- The assessment will be conducted online through Skills Factory Learning Pvt Ltd (SFLPL)
- Format of questions will include a variety of styles suitable to the Performance Criteria (PC) being tested such as multiple choice questions, fill in the blanks, situational judgment, etc.

@Performance Criteria are statements that together specify the standard of performance required when carrying out an exam task.

12. Rules for Performance Improvement examination

- A Performance Improvement examination will be held by SFLPL after one month from the date of declaration of result.
- This Re-examination fees will be charged at Rs. 1000+ GST

13. Award of grades:

Marks	Grade
80 and above	A+
70 to 79	A
60 to 69	B
41 to 59	C
40 and less	D

External (Online) evaluation comprises of the aforesaid modules on the basis of following components:

Module	Examination Pattern	Type of questions (pl changefont)	Marks
Module 1, 2, 3	Online Examination	Objective questions, MCQs	20
Module 4, 5, 6	Online Examination	Objective questions, MCQs	20
Module 7, 8	Online Examination	Objective questions, MCQs	20
Module 9, 10	Online Examination	Objective questions, MCQs	20
Module 11,12, 13	Online Examination	Objective questions, MCQs	20
Total			100

14. Basis for allocation of marks:

Course-related practical work will be entirely based on the skills to be developed in the students.It would include the topics as has been prescribed in the syllabi of every module.

Internal Assessment: 30 marks

Practical components may be based on laboratory work, project, presentation etc. unless otherwise clearly specified in the syllabi of the modules.

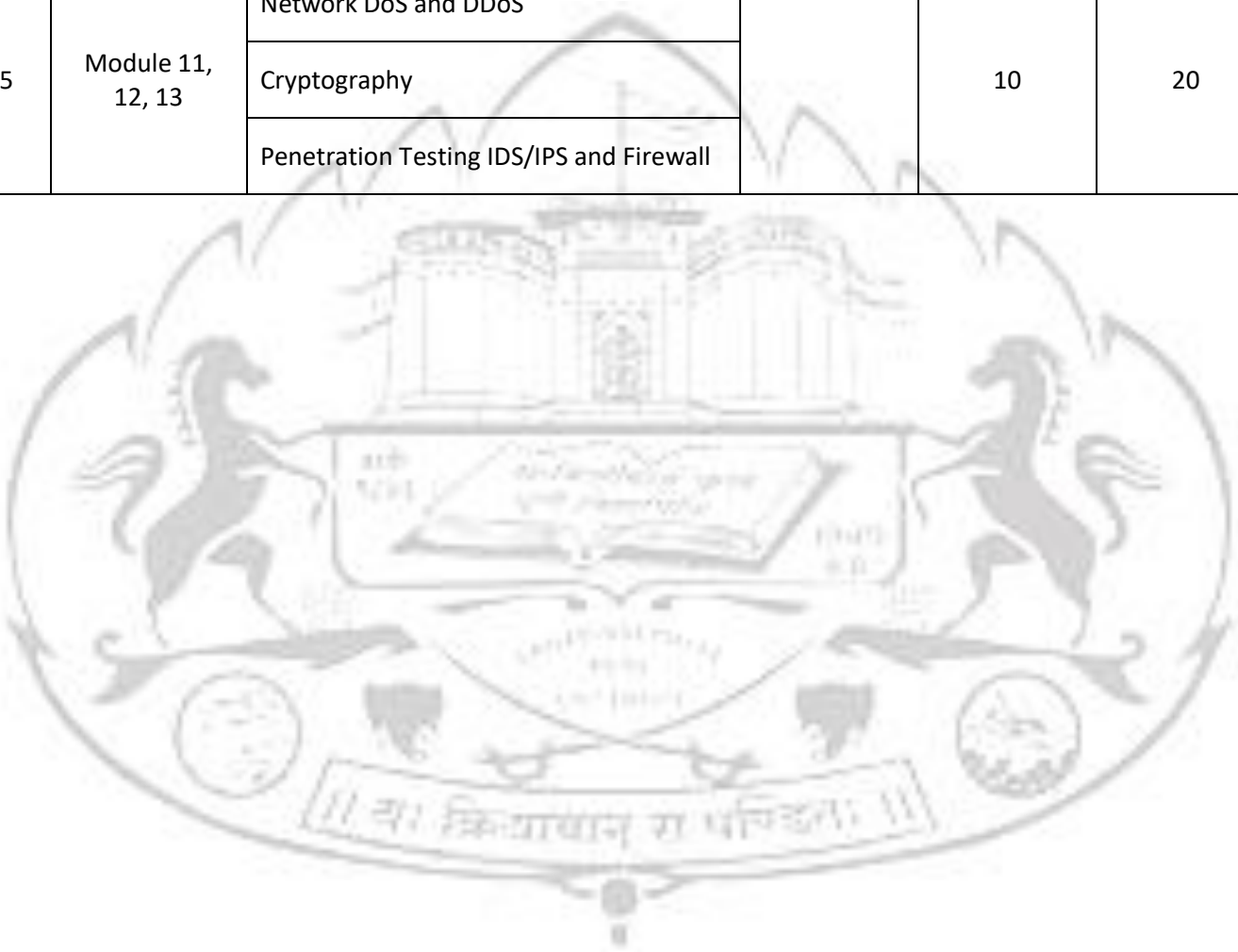
University Examination (External Evaluation): 70 marks

The marks would be clubbed with the internal assessment for the award of grades.

The Certificate in Digital Ethical Hacking course is divided into 2 credits:

Sr. No.	Module No.	Topics	No of Credits	No. of Hrs	Marks
1	Module 1, 2, 3	Introduction to Hacking	One credit for theory part and one credit for practical part totalling two credits as per syllabus	08	20
		Information Gathering / Vulnerability Scanning			
		Malwares			
2	Module 4, 5, 6	System Hacking		12	20
		Sniffing			

		Web Site and Web server Hacking			
3	Module 7, 8	SQL Injection and Cross-site Scripting		8	20
		Buffer Overflow			
4	Module 9, 10	Multi-Platform (cross-platform) System Hacking and Wireless Hacking		7	20
		Mobile Pentesting			
5	Module 11, 12, 13	Network DoS and DDoS		10	20
		Cryptography			
		Penetration Testing IDS/IPS and Firewall			



Syllabus

15. Model Syllabus for Certificate in Digital Ethical Hacking

Sr. No.	Module Name	Topics	Objective	Theory Duration 15 Hrs.	Practical cum Assignment Duration 30 Hrs
1	Introduction to Hacking	1. Introduction o Hacking 2. Essential Terminology 3. Confidentiality Integrity Availability (C.I.A.) 4. Types of Hackers 5. Types of System Attacks 6. Impact of Hacking	To familiarize the student with basic information and terminology to understand subsequent modules.	1	NA
2	Information Gathering/ Vulnerability Scanning	1. Footprinting Concepts 2. Footprinting Methodology 3. Footprinting through Social Networking Sites 4. Email Footprinting 5. WHOIS Footprinting 6. Scanning Techniques 7. Network Scanning 8. Scan for Vulnerability 9. Vulnerability Assessment 10. Network Vulnerability Scanning 11. Vulnerability Scanning for Mobile	Learn techniques of information gathering, assessing the information for weaknesses and how these weaknesses can be exploited. Classifying the vulnerabilities found with respect to its probable impact.	1	2
3	Malwares	1. Introduction to Malware 2. Concepts of Virus, Worm, Trojan 3. Types of Trojans 4. Types of Virus and Worms 5. Malware Reverse Engineering	Learning malware detection techniques. Reverse engineering of malware.	1	3
		6. Penetration Testing			
4	System Hacking	1. System Hacking Goals 2. Methodology 3. Password Cracking 4. Key loggers 5. Spyware 6. Covering Tracks	Understanding the process of exploiting vulnerabilities, password cracking, post exploitation and clearing tracks	2	3
5	Sniffing	1. Defining Sniffing 2. Types of Sniffing	Understanding of Network sniffing	1	2

		3. IP Spoofing	and packet spoofing techniques.		
		4. MAC Spoofing			
		5. DHCP Hijacking			
		6. ARP Spoofing			
		7. DNS Spoofing			
		8. Network Sniffing			
		9. Online credential sniffing and Countermeasures			
		10. Sniffing Detection Techniques			
		11. Web Sniffing			
6	Web Site and Web server Hacking	1. Webserver Attacks	To understand the misconfiguration of web servers and the consequent vulnerabilities arising thereof. Quantifying these vulnerabilities through the use of web application pentesting tools.	1	3
		2. Attack Methodology			
		3. Webserver Footprinting Tools			
		4. Enumerating Webserver Information			
		5. Webserver Attack			
		6. Metasploit			
		7. Webserver Security			
		8. Web Server Security Scanner			
		9. SQL Injection Attacks			
		10. Cross-Site Scripting (XSS) Attacks			
		11. Cross-Site Request Forgery (CSRF) Attack			
		12. Session Fixation Attack			
		13. Cookie/Session Poisoning			
		14. Buffer Overflow Attacks			
		15. CAPTCHA Attacks			
		16. Improper Error Handling			
		17. Web Services XML Poisoning			
		18. Web App Hacking Methodology			
		19. Attacking Web Servers			
		20. Analyze Web Applications			
		21. Attack Authentication Mechanism			
		22. Authorization Attack Schemes			
		23. Attack Session Management Mechanism			
		24. Perform Injection Attacks			
		25. Web Application Hacking Tools			
7	SQL Injection and Cross-site Scripting	1. SQL Injection	To understand how web servers in a sophisticated security	2	3
		2. Types of SQL Injections			
		3. SQL Injection Attacks			

		4. Advanced SQL Injection 5. SQL Injection Counter- measures 6. Cross-site Scripting (XSS) Attacks 7. Cross-site Scripting Attack Scenario 8. Advanced XSS Attack 9. Cross-site Request Forgery (CSRF) Attack	environment can be attacked using SQLI and XSS.		
8	Buffer Overflow	1. Buffer Overflow Attacks 2. Basic Integer Overflows 3. Exploiting Format String Vulnerabilities 4. Stack based Buffer overflow 5. Heap Based Buffer Overflow	Understand how BoF attacks occur and identify the vulnerability that is exploited	1	2
9	Multi-Platform (cross-platform) System Hacking and Wireless Hacking	1. Hacking Methodology 2. Exploiting Bugs in Linux / Windows 3. Stress testing of Operating System 4. Fuzzing 5. Network Hacking 6. Bypassing Authentication 7. Exploiting Operating System level vulnerabilities 8. Exploit identification and Payload Management	Learn about Cross Platform hacking by exploiting possible vulnerabilities in popular operating systems. Understanding 802.11 weaknesses, WEP cracking, de-authentication and its countermeasures.	1	3
10	Mobile Pentesting	1. Hacking Android OS 2. Android Trojan 3. Securing Android Devices 4. Hacking iOS 5. Jailbreaking iOS 6. Securing iOS Devices	Understanding different architectures of mobile platforms. Finding vulnerabilities	1	2

		7. Mobile Device Management (MDM) 8. Bring Your Own Device (BYOD) 9. Mobile Penetration Testing	using automated techniques and exploiting them to stated objective.		
11	Network DoS and DDoS	1. DoS/DDoS Attack 2. Botnets, Zombies 3. DoS/DDoS Attack Tools 4. Attack Forensics 5. Enabling TCP Intercept 6. DoS/DDoS Protection Tools 7. DoS/DDoS Attack Penetration Testing 8. Mitigate Attacks 9. Deflect Attacks 10. Application-Level Flood Attacks	To understand the use of DoS/DDoS attack for stress testing.	1	2
12	Cryptography	1. Cryptography 2. Encryption Algorithms 3. Advantages of cryptography 4. Ciphers 5. Data Encryption Standard (DES) 6. Advanced Encryption Standard (AES) 7. RC4, RC5, RC6 Algorithms 8. RSA 9. Public Key Infrastructure (PKI) 10. Disk Encryption	To understand how the latest algorithms and tools can be used for data and communication protection using encryption.	1	3
13	Penetration Testing IDS/IPS and Firewall	1. Penetration Testing Methodology 2. Understanding of IDS/IPS 3. Understanding of Firewall 4. Report Generation	To understand the methodology of penetration testing and applicable areas of its deployment and subsequent report creation.	1	2

16. Course Outcomes:

- A practical understanding of the current cyber security issues and how errors by administrators, programmers and users can lead to exploitable insecurities.
- Review and practice computer and network etiquette and ethics found in working environments.
- Identification and analysis of the stages an ethical hacker requires taking in order to compromise a target system.
- Critically evaluate security techniques used to protect system and user data.
- Creation of test plans and deliverables including reports and data that detail the types of vulnerabilities discovered.
- Evaluation of best practices in security concepts to maintain confidentiality, integrity and availability of

computer systems or network.

- Work effectively with colleagues.
- Maintain a healthy, safe and secure working environment.
- Provide data/information in standard formats.
- Develop knowledge, skills and competence

17. <u>Book Recommendation:</u>

Certificate in Digital Ethical Hacking textbook by Skills Factory Learning Pvt Ltd.