Mukesh Patel School of Technology Management and Engineering
Information Technology Department

Course Policy

Program/Branch/Semester	**:**	B.Tech and MBA(Tech)/Information Technology/ Sem VII (Elective Course)
Academic Year	**:**	2023-24
Course Code & Name	**:**	_____Ethical Hacking
Credit Details	**:**	L T P C 2 0 2 3
Course Coordinator Faculty	**:**	Dr Pintu Shah
Contact No. & Email	**:**	022-45024747 pintu.shah@nmims.edu
Office	**:**	
Office hours	**:**	Will be update after time table
Other Course Faculty members teaching this course	**:**	NA
Course Faculty for Laboratory: Pintu Shah **Contact No. & Email:** 022-45024747 pintu.shah@nmims.edu **Office:** **Office Hours:**		**Course Faculty for Tutorial: NA** **Contact No. & Email:** **Office:** **Office Hours:**
Queries by Emails are encouraged.		
Course link	**:**	https://portal.svkm.ac.in/usermgmt/login

1 Introduction to the Course

1.1 Importance of the course

Cyber threat has emerged as one of the major threat faced by businesses. Number of cyber-attacks are increasing along with its cost of mitigation. The goal of the ethical hacking or penetration testing is to improve the security posture of an organization by identifying the vulnerabilities and patching them before the attacker can exploit. This requires adversarial mindset i.e. to think like an attacker and use the tools and techniques used by them. Penetration testing has emerged as the mandatory requirement for compliance with some of the standards

like ISO 27001 and PCI DSS. This course equips students with the necessary mindset and skillset to jump start the exciting career in this expanding field.

1.2 Objective of the Course

- To understand various testing methodologies.
- To introduce students to various tools and techniques used in the real world to perform penetration testing.
- To understand legal, professional and ethical issues related to ethical hacking.

1.3 Pre-requisite

- Basic Knowledge of Computer Network, Operating Systems and programming

2 Course Outcomes (CO) and mapping with Program Outcomes (PO)

2.1 Course Outcomes

After successful completion of the course, a student will be able to-

1. Demonstrate hacking in a lab environment.
2. Describe various countermeasures.
3. Describe various professional, ethical and legal issues related to ethical hacking.

2.2 CO-PO Mapping

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1			H				M		M		M	
CO2					H		M		M		M	
CO3						H		M				

Green- medium mapping Blue- high mapping

3 Syllabus, Pre-class activity and References

3.1 Teaching and evaluation scheme

Teaching Scheme				Evaluation Scheme	
Lecture Hours per week	**Practical Hours per week**	**Tutorial Hours per week**	**Credit**	**Internal Continuous Assessment (ICA) As per Institute Norms (50 Marks)**	**Theory (3 Hrs, 100 Marks)**
2	2	0	3	Marks Scaled to 50	Marks Scaled to 50

3.2 Syllabus

Unit	Description	Duration
1	**Introduction:** Need for adversarial thinking and penetration testing, ethics of hacking, hacking process, types of hackers, types of penetration testing, testing methodologies (OSSTMM, PTES, and OWASP Testing Guide), and Rules of engagement.	**6**
2	**Reconnaissance and scanning:** Introduction, types of reconnaissance, various techniques of recon (social engineering, web based recon, DNS based recon, network based recon, Google hacking etc.), countermeasures, scanning, types of scanning (port scanning, network scanning, and vulnerability scanning), Sniffers	**8**
3	**Exploitation:** Password cracking, spoofing, session hijacking, DoS / DDoS, Buffer Overflow, malware, evading firewall and IDS, SQL Injection, OWASP top 10 web application vulnerabilities, hacking wireless networks, metasploit, meterpreter, AV evasion, metasploit databases and tool integration, privilege escalation.	**10**
4	**Hacking Mobile platforms:** Overview of android and iOS, OWASP mobile to 10 risks and mitigation.	**2**
5	**Legal, Professional and Ethical issues:** Cyber laws in India, various ethical dilemma, professional conduct, and penetration testing report writing	**2**
6	Case Study	**2**
	Total	**30**

3.2 Pre-class activity

Faculty will provide pre-class activity details on the student portal. Students are expected to go through the material before attending the upcoming session.

3.3 References

Text Books

1. R. Pillay, "Learn Penetration Testing", Packt Publication, 2019.
2. M. Walker, "CEH Certified Ethical Hacker All-in-One Exam Guide", McGraw-Hill Education, 4th Edition, 2019.

Reference Books:

1. N. Jaswal, "Mastering Metasploit", Packt Publication, 4th Edition, 2020.
2. S. Oriyano and M. Solomon, "Hacker Techniques, Tools, and Incident Handling" , J B Learning, 3rd Edition, 2020.
3. Gilberto Najera-Gutierrez, Juned Ansari , Daniel Teixeira, and Abhinav Singh, "Improving your Penetration Testing Skills", Packt Publication, 2019.
4. http://www.pentest-standard.org/

Note: The latest edition of books should be referred.

4 Laboratory details

Students can use any programming language for lab work. Faculty will upload lab document on the portal before the commencement of the lab. The document will contain lab details like aim, learning outcomes, theory, procedure, and review questions.

Tentative list of the lab experiment is given below. Faculty may revise this list during the semester.

Sr. No.	Week No.#	List of Lab Exercises	Mapped CO
1	1.	Experiment 1: Reconnaissance and foot printing	1
2	2	Experiment 2: Nmap tool	1
3	3	Experiment 3: DoS and MITM attack	1,2
4	4	Experiment 4: Social Engineering attack (SEA)	1,2
5	5	Experiment 5: SQL Injection and XSS attack	1,2
6	6	Experiment 6: ATT&CK Framework	1,2,3
7	7	Experiment 7: Password Cracking	1,2
8	8	Experiment 8: CTF (Scanning and Enumeration)	1

9	9	Experiment 9: CTF (Exploitation and Privilege Escalation)	1
10	10	Experiment 10: CTF (Report Writing)	1,2,3
11	11	Experiment 10: CTF (Report Writing) (Contd.)	1,2,3
12	12	Revision	
13	13	Revision	
14	14	Lab Exam and Viva	
15	15	Lab Exam and Viva	

5 Tutorial Plan

No Tutorial for this course

Sr. No.	Week No.#	Tutorial exercises / activity	Mapped CO

6 Assessment Policy

6.1 Component wise Continuous Evaluation Internal Continuous Assessment (ICA) and Term End Examination (TEE)

Assessment Component	ICA (100 Marks) (Marks scaled to 50)						TEE (100 marks) (Marks scaled to 50)
	Lab Performance	Lab Exam and Viva	Assignment (Group activity)	Scribe Notes	Class Test1 and Class Test 2	Class Participation	
Weightage	7.5%	5%	7.5%	5%	20%	5%	50%
Marks	15	10	15	10	40(20+20)	10	100

6.2 Assessment Policy for Internal Continuous Assessment (ICA)

Assessment of ICA comprises of the following components.

1. **Class test 1 and 2**

a. Two class tests will be conducted as per the academic calendar.
b. It may be conducted online/ offline for 20 marks each

2. **Lab performance evaluation (15 marks)**

   Each lab will be assessed for 10 marks. Following points will be considered while assessment
   a. Lab implementation and troubleshooting (6 marks)
   b. Documentation and timely submission (4 marks)

   Note: 50% penalty for late submission. Absent students will be graded out of 5 marks for that specific lab.

3. **Lab test and viva (10 marks) -** Lab exam will be conducted at the end of the semester based on the labs performed during the semester. Viva Voce will be based on the lab work and theory class.
   a. Lab test – 5 marks
   b. Viva – 5 marks

4. **Assignment (15 marks)**
   a. CR/SR will form a group of 2-3 students. This activity should be completed in the first week.
   b. Each group will select one recent security hack. This activity should be completed in the 2nd week.
   c. Students will research on the selected hack.
   d. Each group will create detailed report and presentation. Report format will be provided by the faculty.
   e. Report and presentation submission deadline is **October 3, 2023.**
   f. **Marks Distribution**
      i. **Detailed report – 8 marks**
      ii. **Presentation – 7 marks**

5. **Class Participation (10 marks)-** The faculty will ask questions during the class or may give some in-class assignment/quiz. Successful response to the question or completion of the in-class activity will fetch marks for the students. The idea is to encourage students to participate actively in the class. Your class attendance will be considered as a part of class participation.

6. **Scribe Notes (10 marks):** Students will be required to submit one page **hand written** lecture note for each lecture using Cornell notes method (https://www.youtube.com/watch?v=nX-xshA_0m8). Faculty will not grade **LATE submissions**.

6.3 Assessment Policy for Term End Examination (TEE)

A final term end exam will be conducted as per the academic calendar. Details of the same will communicated by the course coordinators.

7. Lesson Plan

Session No.	Topics	Mapped CO	Reference
1	Introduction, Need for adversarial thinking and penetration testing	3	TB1/2
2	Ethics of hacking, hacking process, types of hackers	3	TB2
3	Types of penetration testing, OSSTMM	3	TB1
4	PTES	3	RB4
5	OWASP Testing Guide, and Rules of engagement.	3	TB2
6	Introduction, types of reconnaissance	1	TB1
7	Various techniques of recon and countermeasures	1,2	TB1
8	Various techniques of recon and countermeasures (Contd.)	1,2	TB1
9	Various techniques of recon and countermeasures (Contd.)	1,2	TB1
10	Scanning, types of scanning.	1	TB2
11	Types of scanning (Contd.)	1	TB2
12	**Test 1**		
13	Types of scanning (Contd.) and countermeasures	1,2	TB2
14	Sniffers and countermeasures	1,2	TB2
15	Password cracking	1,2	TB1
16	Spoofing and session hijacking	1,2	TB1
17	DoS / DDoS	1,2	TB2
18	Buffer Overflow, malware	1,2	TB2
19	Evading firewall and IDS, AV evasion	1,2	TB2
20	SQL Injection	1,2	TB2
21	OWASP top 10 web application vulnerabilities	1,2	TB1
22	Hacking wireless networks	1,2	TB1
23	Metasploit and meterpreter, Metasploit databases and tool integration, privilege escalation		RB1
24	**Test 2**		
25	Overview of android and iOS	1,2	TB2
26	OWASP mobile to 10 risks and mitigation.	1,2	TB2
27	Cyber laws in India, various ethical dilemma	3	Faculty Presentation

28	Professional conduct, and penetration testing report writing	3	RB4
29	Case Study	1,2,3	
30	Case Study	1,2,3	

A session topic may map to more than one CO depending on the CO statements for a particular course

7 Teaching-learning methodology

Faculty expects active participation from the students to create positive learning environment. Students will be assigned group assignment. Lecture and laboratory session will be conducted as follows-

1. **Lectures:**
   - Faculty will primarily use power point presentation for lecture delivery.

2. **Laboratory:**
   - Lab document containing details of experiment will be uploaded on the student portal before the lab every week.
   - Faculty will grade lab regularly. Late submission will invite 20% penalty. Faculty expects student to display academic honesty in the submission. Students will be marked based on parameters like completion of lab assignment, originality, logic developed, interaction during the lab, submission, punctuality and discipline.

10. Active learning techniques

Active learning is a method of learning in which students are actively or experientially involved in the learning process. Following active learning techniques will be adopted for the course.

1. Blended Learning: some of the topics will be delivered in blended mode. Pre reading material/video links will be provided before the commencement of the topic. This material will be posted on the student portal.
2. Games: students will play games to understand concepts of ethical hacking.

11. Course Material

Following course material will be uploaded on the student portal:

- Course Policy
- Lecture Presentations
- Books / Reference Books / NPTEL video lectures link (if any)
- Assignments
- Lab Manual

12. Course Outcome Attainment

Following means will be used to assess attainment of course learning outcomes.

- Use of formal evaluation components of continuous evaluation, assignments, laboratory work, and course end survey

- Informal feedback during course conduction

13. Academic Integrity Statement

Faculty expects academic integrity from all students. Student should refer to student resource book (SRB) for academic guidelines.