Program : **Diploma in Computer Engineering / Information Technology / Computer Hardware Engineering / Cyber Forensics and Information Security**	
Course Code : **5139B**	Course Title: **Ethical Hacking Lab**
Semester : **5 / 5 / 6 / 6**	Credits: **1.5**
Course Category: **Program Elective**	
Periods per week: **3 (L:0 T:0 P:3)**	Periods per semester: **45**

Course Objective:

- Impart hands-on training on various ethical hacking techniques.
- Identify the security issues in a network environment and suggest the security measures to be practiced in an organization
- Understand the ethics to be followed in a network community.

Course Prerequisites:

Topic	Course code	Course name	Semester
Digital fundamentals		Digital Computer Fundamentals	3
Basic programming concepts		Programming in C	3

<course code> *Fundamentals of Artificial Intelligence and Machine Learning should be registered along with this.*

Course Outcomes :

On completion of the course, the student will be able to:

COn	Description	Duration (Hours)	Cognitive Level
CO1	Experiment with network commands and suggest counter measures for malwares.	9	Applying
CO2	Make use of different tools to conduct foot printing and port scanning.	10	Applying
CO3	Utilize tools for password hacking and software firewall.	11	Applying
CO4	Construct a wireless network system with MAC filtering.	12	Applying

	Lab Exam	3	

CO – PO Mapping

Course Outcomes	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7
CO1	3			3	3		
CO2	3			3	3		
CO3	3			3	3		
CO4	3			3	3		

3-Strongly mapped, 2-Moderately mapped, 1-Weakly mapped

Course Outline

Module Outcomes	Description	Duration (Hours)	Cognitive Level
CO1	**Experiment with network commands and suggest counter measures for malwares.**		
M1.01	Experiment with ipv4 configuration, gateway, DNS settings, ping command, netstat command, tracert command,	3	Applying
M1.02	Apply an antivirus software for protection against malware and also perform patching of OS	3	Applying
M1.03	Organize users in OS and set strong password for users	3	Applying
CO2	**Make use of different tools to conduct foot printing and port scanning.**		
M2.01	Make use of whois, nslookup commands for foot printing.	3	Applying
M2.02	Experiment with port scanning using NMAP and practice various options.	4	Applying
M2.03	Make use of ping and ping sweep using NMAP	3	Applying
	Lab Exam – I	1.5	
CO3	**Utilize tools for password hacking and software firewall.**		
M3.01	Experiment password hacking methods like brute force, dictionary attack using tools	3	Applying

M3.02	Utilize wire shark and perform traffic monitoring.	4	Applying
M3.03	Construct a software firewall using wireshark	4	Applying
CO4	**Construct a wireless network system with MAC filtering.**		
M4.01	Construct a wireless network with password protection and perform war driving	3	Applying
M4.02	Build a wireless network and protect it using MAC filtering	3	Applying
M4.03	Plan and configure a network system with full security measures like, antivirus software, firewall and wireless protection.	3	Applying
M4.04	Open Ended Experiments**	3	Applying
	Lab Exam – II	1.5	

**** - Suggested Open Ended Experiments**

(Not for End Semester Examination but compulsory to be included in Continuous Internal Evaluation. Students can do open ended experiments as a group of 2-3. There is no duplication in experiments between groups.)

1 Set up an Intrusion Detection System
2 Conduct IP Packet crafting
3 Perform Ping and Ping sweep using tools other than NMAP
4 Setup an IP logger

Text / Reference

T/R	Book Title/Author
T1	**Hands on Ethical Hacking and Network Defense**, 2nd Edition, Michael T Simpson, Kent Back man, James Coreley
R1	W. Stallings, **Data and Computer Communications**.
R2	W. Stallings, **Cryptography and Network Security: Principles and Practice**

Online Resources

SL.No	Website Link
1	http://uou.ac.in/foundation-course - Introduction to cyber security