UNIT I

INTRODUCTION

PART–A				
Q. No	**Questions**	**CO Mapping**	**BT Level**	**Complexity**
1	What is ethical hacking?	CO1	Understand	Low
2	What are the different types of hackers?	CO1	Understand	Low
3	How would a penetration tester help an organization improve security?	CO1	Understand	Medium
4	Why is it important to regularly perform vulnerability assessments?	CO1	Understand	Medium
5	Should companies allow ethical hackers to conduct penetration tests regularly? Why or why not?	CO1	Analyze	Medium
6	How does reconnaissance contribute to a successful penetration test?	CO1	Understand	Medium
7	What is the Computer Fraud and Abuse Act (CFAA)?	CO1	Understand	Low
8	What is the GDPR’s role in cyber security?	CO1	Understand	Low
9	Name the four layers of the TCP/IP model?	CO1	Remember	Low
10	What is the role of the application layer?	CO1	Understand	Low
11	What is the difference between TCP and UDP?	CO1	Understand	Low
12	What is the role of the internet layer?	CO1	Understand	Low
13	What is the difference between IPv4 and IPv6?	CO1	Understand	Low
14	What is a DDoS attack?	CO1	Understand	Low
15	Define malware.	CO1	Remember	Low

16	Why is endpoint security important in an enterprise environment?	CO1	Understand	Medium
17	Define brute-force attack.	CO1	Remember	Low
18	What is physical security in cyber security?	CO1	Understand	Low
19	What are the different phases of ethical hacking?	CO1	Understand	Low
20	What is the Electronic Communications Privacy Act (ECPA)?	CO1	Understand	Low
21	What is tailgating in cyber security?	CO1	Understand	Low
22	What is a sandbox in malware analysis?	CO1	Understand	Low
23	What is an ARP spoofing attack?	CO1	Understand	Low

PART–B

Q. No	Questions	CO Mapping	BT Level	Complexity
1	Explain the importance of ethical hacking in cyber security.	CO1	Understand	Medium
2	Given a scenario where a hacker identifies a system flaw without authorization and demands a reward, classify the hacker as Black Hat, White Hat, or Gray Hat.	CO1	Analyze	Medium
3	Explain the responsibilities of a penetration tester.	CO1	Understand	Medium
4	Design a cyber security strategy that incorporates both penetration testing and vulnerability assessments.	CO1	Create	High
5	If you were conducting a penetration test, which testing approach (black-box, white-box, or gray-box) would you choose for a financial institution, and why?	CO1	Understand	Medium

6	Explain the purpose of each step in a penetration testing process.	CO1	Understand	Medium
7	How would you ensure compliance with legal and ethical standards during a penetration test for a multinational company?	CO1	Understand	Medium
8	Compare cyber security laws in different countries.	CO1	Evaluate	Medium
9	How do the OSI and TCP/IP models differ in terms of their layer functions and overall design?	CO1	Understand	High
10	Explain common protocols in the application layer (HTTP, DNS, SMTP).	CO1	Understand	Medium
11	Explain three-way handshake in TCP.	CO1	Understand	Medium
12	Describe about IP fragmentation and reassembly.	CO1	Understand	Medium
13	Explain CIDR notation and sub netting in IP addressing.	CO1	Understand	High
14	Which network attack (MITM, SYN flood, ARP spoofing) poses the greatest risk in modern networks, and why?	CO1	Analyze	High
15	Explain in detail about different types of malware and their attack mechanisms.	CO1	Understand	Medium
16	How do antivirus software and other security measures protect against malware infections?	CO1	Understand	High
17	How intruder attacks are detected and mitigated – Explain.	CO1	Understand	High
18	Create a comprehensive physical security policy for a company handling sensitive data.	CO1	Create	High

UNIT II

FOOT PRINTING, RECONNAISSANCE AND SCANNING NETWORKS

PART–A				
Q. No	**Questions**	**CO Mapping**	**BT Level**	**Complexity**
1	What is OSINT (Open Source Intelligence)?	CO2	Understand	Low
2	What is the difference between information and foot printing?	CO2	Understand	Low
3	What is Google Hacking Database (GHDB)?	CO2	Understand	Low
4	How does Trace route help in foot printing?	CO2	Understand	Low
5	What is Geo-tagging and how is it misused?	CO2	Understand	Low
6	What is the role of robots.txt in security?	CO2	Understand	Low
7	What is the difference between legal and illegal competitive intelligence gathering?	CO2	Understand	Medium
8	What is the psychological basis of social engineering attacks?	CO2	Understand	Low
9	What is the role of ICMP in network scanning?	CO2	Understand	Low
10	How does Netcat function in port scanning?	CO2	Understand	Low
11	What is a FIN scan and when is it used?	CO2	Understand	Medium
12	What is fragmentation scanning?	CO2	Understand	Medium
13	Define passive foot printing.	CO2	Remember	Low
14	What are the risks of foot printing in cyber security?	CO2	Understand	Low

15	What is Google Dorking?	CO2	Understand	Low
16	How can cache and archived web pages help in foot printing?	CO2	Understand	Medium
17	What is the purpose of WHOIS lookup?	CO2	Understand	Low
18	What is Zone Transfer in DNS foot printing?	CO2	Understand	Low
19	What is social engineering reconnaissance?	CO2	Understand	Low
20	What is the role of OSINT (OpenSource Intelligence) in competitive intelligence?	CO2	Understand	Low
21	Define spear phishing.	CO2	Remember	Low
22	How does pretexting operate as a social engineering tactic?	CO2	Understand	Low
23	How would you use Shodan to perform a foot printing exercise on a target network?	CO2	Understand	Medium
24	Differentiate between active and passive scanning.	CO2	Understand	Low
25	Assess how well Zen map meets the needs of network administrators in diverse environments, and suggest improvements.	CO2	Analyze	Medium
26	What is the difference between SYN scan and FIN scan?	CO2	Understand	Low
27	What is banner grabbing in scanning?	CO2	Understand	Low
28	What is decoy scanning and how does it work?	CO2	Understand	Low
PART–B				
Q. No	**Questions**	**CO Mapping**	**BT Level**	**Complexity**
1	What is OSINT, and how is it applied in ethical hacking and penetration testing?	CO2	Understand	Medium
2	How do cybercriminals use foot printing techniques, such as social media foot printing and email header analysis, to plan their attacks?	CO2	Understand	Medium

3	How can Google Dorking be used to identify security weaknesses in a target system?	CO2	Understand	Medium
4	What types of information can an attacker obtain from WHOIS records and how can it be exploited?	CO2	Understand	Medium
5	How can social media foot printing be exploited to facilitate identity theft?	CO2	Understand	High
6	How can email header analysis be used for foot printing in cybersecurity?	CO2	Understand	High
7	Explain real-world case studies where competitive intelligence was used unethically.	CO2	Understand	Medium
8	Discuss phishing, vishing, and baiting are used for foot printing – How?	CO2	Understand	Medium
9	How do security professionals and attackers use Shodan for reconnaissance and foot printing?	CO2	Understand	High
10	Explain in detail about the passive and active scanning techniques.	CO2	Understand	Medium
11	Describe Stealth scanning and aggressive scanning techniques.	CO2	Understand	Medium
12	How do network scanners detect live hosts in a network.	CO2	Understand	High
13	How do foot printing help ethical hackers and cybercriminals.	CO2	Understand	High
14	Discuss the Google Hacking techniques can be used for reconnaissance.	CO2	Understand	Medium
15	Explain the following terms are used in the foot printing -WHOIS, DNS lookup, and Reverse IP lookup.	CO2	Understand	Medium
16	Explain the impact of social media intelligence (SOCMINT) in cyber security.	CO2	Understand	Medium
17	Explain the role of email tracking and email header analysis help in information gathering.	CO2	Understand	Medium
18	How can businesses use foot printing to gather competitive insights, and where should ethical boundaries be drawn?	CO2	Understand	Medium

19	Create a scenario-based training module that illustrates how phishing, vishing, and baiting can be used for foot printing, along with counter measures.	CO2	Create	High
20	Analyze the strengths and limitations of using tools like Maltego, the Harvester, and Recon-ng for comprehensive foot printing.	CO2	Analyze	High
21	How does network scanning help in detecting system vulnerabilities?	CO2	Understand	High
22	Compare Nmap, Netcat and Advanced IP Scanner in network scanning.	CO2	Evaluate	Medium
23	What are the differences between TCP, UDP, and stealth scanning techniques, and how do they influence the outcomes of a penetration test?	CO2	Understand	High
24	What advanced scanning techniques do attackers use to evade IDS and firewalls?	CO2	Understand	Medium

UNIT III

ENUMERATION AND VULNERABILITY ANALYSIS

PART–A				
Q. No	**Questions**	**CO Mapping**	**BT Level**	**Complexity**
1	What is active enumeration vs passive enumeration?	CO3	Understand	Low
2	What command is used for NetBIOS name lookup?	CO3	Understand	Low
3	What is the purpose of an SNMP MIB (Management Information Base)?	CO3	Understand	Low
4	What is an LDAP distinguished name (DN)?	CO3	Understand	Low
5	What is Reverse DNS lookup, and how is it used in hacking?	CO3	Understand	Low
6	What is the difference between penetration testing and vulnerability assessment?	CO3	Understand	Medium
7	What is the Eternal Blue exploit, and why is it dangerous?	CO3	Understand	Medium
8	What is Dirty COW vulnerability in Linux?	CO3	Understand	Low
9	What is a zero-day vulnerability in embedded systems?	CO3	Understand	Low
10	What tool is commonly used for NetBIOS enumeration?	CO3	Understand	Low
11	What is the default port for SNMP?	CO3	Understand	Low
12	What is the purpose of SNMPv3 compared to SNMPv1 and SNMPv2?	CO3	Understand	Low
13	What is an LDAP query, and how is it used?	CO3	Understand	Medium
14	What is an LDAP injection attack?	CO3	Understand	Low

15	How does an attacker use NTP enumeration to gather information?	CO3	Understand	Medium
16	What are the VRFY and EXPN commands in SMTP enumeration?	CO3	Understand	Low
17	How does SMTP enumeration help attackers identify valid email addresses?	CO3	Understand	Medium
PART–B				
Q. No	**Questions**	**CO Mapping**	**BT Level**	**Complexity**
1	Compare different enumeration techniques used in cyber security.	CO3	Evaluate	High
2	Explain in detail about the NetBIOS enumeration.	CO3	Understand	High
3	How SNMP vulnerabilities can lead to serious network attacks – Explain.	CO3	Understand	Medium
4	Compare LDAP enumeration and Active Directory enumeration.	CO3	Evaluate	High
5	Explain in detailed about NTP enumeration.	CO3	Understand	Medium
6	Evaluate the root causes of real-world DNS security failures and discuss the contributing factors.	CO3	Evaluate	High
7	Compare different vulnerability assessment methodologies.	CO3	Evaluate	High
8	How do attackers exploit Windows SMB vulnerabilities and how to mitigate them.	CO3	Understand	High
9	Compare Linux privilege escalation techniques and how they can be mitigated.	CO3	Evaluate	High
10	Compare different enumeration techniques used in cyber security.	CO3	Evaluate	High
11	How do NetBIOS enumeration help attackers in privilege escalation – Explain.	CO3	Understand	High
12	How can SNMP vulnerabilities be exploited to launch network attacks?	CO3	Understand	Medium

13	Compare LDAP enumeration and Active Directory enumeration.	CO3	Evaluate	High
14	Given a network with time synchronization issues, describe how you would conduct NTP enumeration to uncover potential vulnerabilities.	CO3	Understand	Medium
15	Discuss real-world attacks caused due to improper DNS security.	CO3	Understand	High
16	Design a new vulnerability assessment methodology that incorporates dynamic threat intelligence and continuous monitoring.	CO3	Create	High
17	How can Windows SMB vulnerabilities be identified and mitigated in a controlled lab environment?	CO3	Understand	Medium
18	How do Linux privilege escalation techniques differ from one another, and what common mitigations exist?	CO3	Understand	Medium
19	Design a training module using case studies of embedded OS vulnerabilities to educate security professionals on emerging threats and countermeasures.	CO3	Create	High

UNIT IV

SYSTEM HACKING

PART–A				
Q. No	**Questions**	**CO Mapping**	**BT Level**	**Complexity**
1	List two primary components of a web application and briefly state their functions.	CO4	Remember	Low
2	Define “vulnerability” in the context of web servers.	CO4	Remember	Low
3	Name two common web server vulnerabilities that attackers often exploit.	CO4	Remember	Low
4	List two essential components of a wireless network.	CO4	Remember	Low
5	Define wardriving.	CO4	Remember	Low
6	List two encryption protocols commonly used to secure wireless networks.	CO4	Remember	Low
7	What is the primary function of a wireless sniffer tool?	CO4	Understand	Low
8	What is the basic function of the HTTP protocol in web communication?	CO4	Understand	Low
9	Mention the one vulnerability related to session management in web applications.	CO6	Remember	Low
10	State the primary function of a Web Application Firewall.	CO4	Remember	Low
11	What is the purpose of MAC address spoofing in wireless attacks.	CO4	Understand	High
12	What is the XSS and its potential impact on web security?	CO4	Understand	Low
13	What is the Cross-Site Request Forgery (CSRF)?	CO4	Understand	Low

PART–B				
Q.No	**Questions**	**CO Mapping**	**BT Level**	**Complexity**
1	Explain the purpose of a web vulnerability scanner in testing web applications.	CO4	Understand	Medium
2	How a database server functions as part of a web application – Explain.	CO4	Understand	Medium
3	Analyze a hypothetical web server attack by detailing how specific vulnerabilities in web application components can be exploited by attackers.	CO4	Analyze	Medium
4	Evaluate and compare the tools used by web attackers with those used by security testers, and propose enhancements to improve their effectiveness in real-world scenarios.	CO6	Evaluate	Medium
5	Design a comprehensive security strategy to protect a web server against common vulnerabilities, including aspects like patch management and intrusion detection.	CO4	Create	High
6	Discuss the typical attack sequence in a web server hacking incident, detailing phases such as reconnaissance, exploitation, and post-exploitation activities.	CO4	Understand	Medium
7	Critically evaluate current web server security policies and propose a set of enhancements to minimize the risk of web attacks.	CO4	Evaluate	Medium
8	Analyze various wireless hacking techniques including wardriving and discuss how attackers use these methods to discover and exploit wireless network vulnerabilities.	CO4	Analyze	Medium
9	Evaluate different tools used for wireless hacking and design a mitigation strategy to defend against these tools effectively.	CO6	Evaluate	Medium
10	Develop a comprehensive wireless network security plan that addresses identified vulnerabilities, incorporating both physical and logical security measures.	CO4	Create	High

11	Discuss a real-world case study of a wireless network attack, identifying the vulnerabilities exploited and evaluating the steps taken for remediation.	CO6	Understand	Medium
12	Design an advanced wireless intrusion detection system (WIDS) framework, detailing its components and explaining how it differentiates between benign and malicious activities.	CO4	Create	High
13	Develop a comprehensive defense strategy for a corporate wireless network that addresses both physical and logical vulnerabilities.	CO6	Create	High

UNIT V

NETWORK PROTECTION SYSTEMS

PART–A				
Q. No	**Questions**	**CO Mapping**	**BT Level**	**Complexity**
1	What is an Access Control List (ACL)?	CO5	Understand	Low
2	What is the difference between Standard ACL and Extended ACL?	CO5	Understand	Low
3	What is a Cisco ASA Firewall, and how does it work?	CO5	Understand	Low
4	What are the main features of a Cisco ASA firewall?	CO5	Understand	Low
5	Name two firewall configuration analysis tools.	CO5	Remember	Low
6	What is the role of risk analysis in firewall security?	CO5	Understand	Low
7	Differentiate between IDS and IPS.	CO5	Understand	Low
8	What is the primary function of an Intrusion Prevention System (IPS)?	CO5	Understand	Low
9	What is the difference between NIDS and HIDS?	CO5	Understand	Low
10	How does Host-Based IDS (HIDS) detect threats?	CO5	Understand	Low
11	What is web filtering, and why is it used?	CO5	Understand	Low
12	Name two web filtering techniques.	CO5	Remember	Low
13	What is the role of a Security Incident Response Team (SIRT)?	CO5	Understand	Low
14	What are the primary responsibilities of a CSIRT (Computer Security Incident Response Team)?	CO5	Understand	Low
15	What is a honeypot in cyber security?	CO5	Understand	Low

16	What is the difference between a low-interaction and high-interaction honeypot?	CO5	Understand	Low
PART–B				
Q. No	**Questions**	**CO Mapping**	**BT Level**	**Complexity**
1	Explain the types of ACLs and their role in network security.	CO5	Understand	Medium
2	How do ACLs enhance network security, and what are their limitations?	CO5	Understand	High
3	Describe the architecture of Cisco ASA Firewall and its working.	CO5	Understand	Medium
4	How to configure a Cisco ASA firewall for maximum security – Explain?	CO5	Understand	High
5	Compare various firewall risk analysis tools and their effectiveness.	CO5	Evaluate	High
6	Discuss the advantages and disadvantages of IDS vs. IPS.	CO5	Understand	Medium
7	Explain the working of a Network-Based IDS (NIDS) and Host-Based IDS (HIDS) with examples.	CO5	Understand	Medium
8	Discuss the role of web filtering in cyber security and different filtering techniques.	CO5	Understand	High
9	Explain the incident response process followed by security teams.	CO5	Understand	Medium
10	How do organizations set up an effective Computer Security Incident Response Team (CSIRT)?	CO5	Understand	High
11	How do honeypots assist in detecting intrusions and analyzing cyberattacks?	CO5	Understand	High
12	Compare honey nets and honeypots in terms of cyber security defense.	CO5	Evaluate	High