Gyanmanjari Innovative University

Syllabus
Gyanmanjari Diploma Engineering College
Semester-3 (Diploma)

Subject: Ethical Hacking Methodologies - DET2CE13205

Type of course: Professional Core

Prerequisite: Basic computer literacy, logical thinking, and fundamental knowledge of computer networks, operating systems, internet usage, and web applications. Basic knowledge of Linux commands and security concepts will be helpful, but prior ethical hacking experience is not required.

Rationale:
This course introduces students to the fundamentals of Ethical Hacking and Cyber Security. It helps learners understand security concepts, attack methodologies, vulnerability identification, and countermeasures. Through practical exposure to tools such as Kali Linux, Nmap, Wireshark, Burp Suite, and Metasploit, students gain hands-on experience in authorized lab environments. The course prepares students to perform basic security testing, analyze cyber threats, and suggest suitable protection measures for systems, networks, and applications.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks		Total Marks
CI	T	P	C	SEE	CCE	
2	0	2	3	50	50	100

Legends: CI-Class Room Instructions; T – Tutorial; P - Practical, C – Credit; SEE - Semester End Evaluation; CCE-Continuous and Comprehensive Evaluation.

Course Content:

Sr. No	Course Content	Hrs.	% Weightage
1	**Operating Systems, Networking and Ethical Hacking Fundamentals** ***Theory Topics:*** Introduction to Operating Systems (OS) and their role in computing, Types of Operating Systems (Windows, Linux, macOS), Windows Desktop Environment (File Explorer, Task Manager, Control Panel, Settings), Windows File System (Drives, Folders, File Types, Hidden Files, File Extensions), Introduction to Windows Command Prompt (CMD), Importance of Command-Line Skills in IT and Cybersecurity, Introduction to Linux and its use in Cybersecurity, Linux Desktop Environment (Ubuntu/Kali Linux Overview), Linux File System Hierarchy (/, /home, /etc, /var, /tmp), GUI vs CLI, User Accounts and Permissions in Windows (Administrator, Standard User), User Accounts and Permissions in Linux (root, sudo, chmod Basics), Introduction to Virtualization and Virtual Machines (VMs), Introduction to Computer Networks, Types of Networks (LAN, WAN), IP Addresses (IPv4, Private and Public IP), MAC Addresses and IP vs MAC Difference, Network Devices (Router, Switch, Modem), Common Networking Protocols (HTTP, HTTPS, FTP, DNS, DHCP, SSH), Ports and Common Port Numbers (21, 22, 80, 443, 3389), Basic Network Troubleshooting Methodology, Introduction to Ethical Hacking, Types of Hackers (White Hat, Black Hat, Grey Hat), Penetration Testing Lifecycle (Reconnaissance, Scanning, Gaining Access, Maintaining Access, Reporting), Legal and Ethical Boundaries in Security Testing, Introduction to Kali Linux, Overview of Ethical Hacking Tools (Nmap, Wireshark, Burp Suite), Best Practices for Safe and Authorized Lab Environments. ***Practical:*** 1. Set up a complete ethical hacking lab environment using VirtualBox / VMware, including Kali Linux and a safe target virtual machine. 2. Configure basic lab network settings such as NAT, Host-Only Adapter, and isolated virtual network for controlled security practice. 3. Set up a Linux environment (Kali Linux on VirtualBox/VMware on personal laptop) - navigate the	12	20%

	desktop, open a terminal, and verify the installation by running basic commands (uname -a, whoami, pwd, ls, df -h). 4. Practice essential Linux commands required for cyber security tasks, including file handling, directory navigation, process viewing, network checking, and permission management. 5. Practice essential Linux terminal commands (ls, cd, pwd, mkdir, rm, cp, mv, cat, nano, chmod, ps, grep) - run each, capture the output, and write a one-line explanation of what it does. 6. Manage file permissions in Linux - create a new file, set read/write/execute permissions using chmod (e.g. chmod 755, chmod 644), and verify changes using ls -l. 7. Use the ping command to test connectivity to (a) the default gateway, (b) 8.8.8.8 (Google DNS), and (c) a website - document results and explain what success or failure at each step indicates. 8. Use nslookup to find the IP address of three different websites - document results and explain the role of DNS in everyday internet use. 9. Explore the Kali Linux application menu - open the terminal, browse the tool categories (Information Gathering, Vulnerability Analysis, Exploitation Tools), and document what five commonly used tools do without running them. 10. Prepare a basic security policy checklist for a computer lab, including password policy, device usage, internet access, data backup, and user responsibility. 11. Analyze a cyber security incident case study and identify the attacker's process, security weakness, impact, and preventive measures. 12. Create a one-page Ethical Hacking Authorization Template - include fields for target system, tester's name, scope of testing, permitted actions, time window, and reporting responsibility. 13. Prepare a security awareness poster or one-page document on safe password practices, phishing prevention, and responsible internet usage.		

Examination Style:

Sr. No.	Evolution Method	SEE	CCE
1	**Windows & Linux Live Command Demonstration** Perform essential Windows and Linux commands for file management, permissions, network configuration, and connectivity testing.	05	-
2	**Network Troubleshooting & Ethical Hacking Concepts – Viva** Analyze a networking or ethical hacking scenario and explain troubleshooting steps, penetration-testing phases, and legal boundaries.	05	-
3	**Active Learning Activity (ALA): Cyber Security Awareness and Ethical Practice** Prepare an OS and network lab diary with command outputs and develop an awareness document covering ethical hacking concepts and responsible security practices.	-	10
	Total	10	10

Examination Style:

1. **Windows & Linux Live Command Demonstration (05 Marks):**
   - Students will demonstrate a set of tasks live on their laptop - chosen by the faculty during assessment: navigate the Windows/Linux file system using commands, create a folder structure, set file permissions using chmod, find the network configuration using ipconfig or ip a, and test connectivity using ping. No prior preparation of the exact task is given. This task evaluates hands-on confidence with both operating system environments.

	2. **Network Troubleshooting & EH Concepts – Written / Viva (05 Marks):** • Students will be given a short scenario by faulty - either a network connectivity problem to diagnose step by step using networking commands, or an ethical hacking situation where they must identify the correct phase of the penetration testing lifecycle and explain the legal boundaries. A written or viva response of 3–5 sentences per point is required. This task evaluates methodical troubleshooting thinking and understanding of ethical hacking concepts. 3. **Active Learning Activity (ALA): OS & Network Lab Diary + EH Awareness Document (10 Marks):** • Students will maintain a structured Lab Diary documenting all Windows CMD and Linux/Kali terminal commands practiced during the module - each entry must include the command, a screenshot of the output, and a plain-English explanation of what it does and where it is used in real IT work. The diary must cover at All essential Windows and essential Linux commands. Students will also prepare a one-page Cyber Security Awareness Document explaining: what ethical hacking is, types of hackers, the five phases of penetration testing, and the legal and ethical responsibilities of a security tester. Deliverable is a combined PDF. This activity evaluates the student's ability to learn and apply foundational OS commands and communicate core ethical hacking concepts correctly.		
2	**Reconnaissance, Footprinting and Network Scanning** ***Theory Topics:*** Understanding the role of reconnaissance in ethical hacking, importance of information gathering before security testing, passive and active footprinting techniques, open-source intelligence concepts, domain and IP information gathering, DNS records and WHOIS lookup, website footprinting and email footprinting awareness, social media and public data exposure risks, network scanning fundamentals, identifying active hosts in a controlled lab network, port scanning concepts, service version detection, OS fingerprinting, banner grabbing, enumeration basics, user and service enumeration awareness, introduction to	12	20%

	vulnerability identification, CVE and CVSS basics, mapping discovered information to possible security weaknesses, risks of exposed services and misconfigured systems, countermeasures against footprinting and scanning, documentation of reconnaissance findings, and best practices for performing scanning activities only in authorized lab environments. ***Practical:*** 14. Use the previously configured ethical hacking lab environment to perform footprinting and scanning activities on authorized lab targets. 15. Perform passive information gathering for a given sample organization or lab scenario using publicly available and non-sensitive sources. 16. Collect and document domain-related information such as domain name, IP address, DNS records, and server details using safe lookup tools. 17. Perform WHOIS lookup and DNS analysis for teacher-approved domains and prepare a short footprinting observation report. 18. Identify active hosts in a controlled lab network using host discovery techniques. 19. Perform basic port scanning on a lab target machine to identify open, closed, and filtered ports. 20. Detect running services and service versions on a lab machine using Nmap in an authorized environment. 21. Perform OS fingerprinting on a target virtual machine and document the observed operating system details. 22. Practice banner grabbing in a controlled lab environment to understand how exposed service information may create security risks. 23. Prepare a network mapping diagram showing active hosts, IP addresses, open ports, and running services in the lab network. 24. Map identified services with possible security concerns using basic CVE and CVSS awareness. 25. Compare passive footprinting and active scanning techniques with examples, advantages, limitations, and ethical boundaries. 26. Prepare countermeasure recommendations against footprinting and scanning, including service hardening, firewall rules, and information exposure control.		

27. Create a structured reconnaissance and scanning report including objective, scope, tools used, observations, risks, and recommended security actions.

Examination Style:

Sr. No.	Evolution Method	SEE	CCE
1	**Footprinting and Information-Gathering Report** Investigate a teacher-approved domain or lab scenario using DNS, WHOIS, IP, website, and technology information while following ethical boundaries.	05	-
2	**Network Scanning and Vulnerability - Mapping Demonstration** Scan an authorized lab target using Nmap, analyze hosts, ports, services, and versions, and map findings to basic risks and countermeasures	05	-
3	**Active Learning Activity (ALA): Reconnaissance and Digital Exposure Analysis** Prepare a structured digital-footprint report covering passive and active reconnaissance, exposure risks, ethical considerations, and recommended security measures.	-	10
	Total	10	10

Examination Style:

1. **Footprinting & Information Gathering Report (05 Marks):**
   - Students will be given a teacher-approved domain, sample organization, or lab-based scenario. They must collect and document basic footprinting information such as domain name, IP address, DNS records, WHOIS details, website information, visible technologies, and publicly available contact or service details using safe and authorized tools. Students must clearly differentiate between passive and

	active information gathering and mention the ethical boundaries followed during the task. The report should include screenshots, observation table, tools used, risks identified, and basic countermeasure suggestions. This task evaluates students' ability to perform responsible information gathering and prepare a structured reconnaissance report. **2. Network Scanning & Vulnerability Mapping Demonstration (05 Marks):** • Students will use the previously configured ethical hacking lab environment to perform basic scanning on an authorized lab target. They must identify active hosts, open ports, running services, service versions, and possible operating system details using tools such as Nmap. Based on the scan results, students will map identified services with possible security risks using basic CVE and CVSS awareness. They must also suggest suitable countermeasures such as closing unused ports, service hardening, firewall configuration, and reducing information disclosure. Deliverables include scan screenshots, command summary, observation table, risk mapping, and a short conclusion. This task evaluates students' ability to perform controlled network scanning, analyze discovered services, and connect scanning results with basic vulnerability assessment practices. **3. Active Learning Activity (ALA): Reconnaissance and Digital Exposure Analysis (10 Marks)** • In this task, students will prepare a structured Digital Footprint Discovery Report for a selected teacher-approved organization, sample domain, or lab-based scenario. The report must include basic information gathering such as domain details, IP address information, DNS records, WHOIS information, publicly available website details, and visible technology indicators. Students must clearly differentiate between passive footprinting and active information gathering and explain the ethical boundaries of each technique. They will also identify possible information exposure risks such as open service details, outdated public information, exposed contact details, or unnecessary technical disclosure. Deliverables include a PDF/slide deck summarizing footprinting observations, tools used, screenshots, ethical considerations, risks identified, and recommended		

	countermeasures. This activity evaluates students' ability to collect, organize, interpret, and document reconnaissance information responsibly.		
3	**Vulnerability Assessment, System Security and Malware Defense** ***Theory Topics:*** Understanding vulnerability assessment and its role in ethical hacking, difference between vulnerability assessment and exploitation, vulnerability lifecycle, introduction to CVE, CVSS, severity levels, and risk prioritization, identifying common system vulnerabilities and security misconfigurations, understanding exposed services, outdated software, weak authentication, default credentials, insecure permissions, and patching issues, basics of system hacking concepts in an authorized lab context, password security fundamentals, password policy, hashing, salting, and authentication weaknesses, introduction to privilege escalation awareness and its prevention, vulnerability scanning methodology, interpreting vulnerability scan results, false positives and false negatives in assessment, introduction to Metasploit framework for controlled lab-based vulnerability demonstration, understanding malware and its categories including viruses, worms, Trojans, spyware, keyloggers, ransomware, backdoors, and rootkits, malware infection lifecycle, common malware delivery methods, impact of malware on systems and organizations, malware prevention and detection techniques, antivirus, EDR, sandboxing, backup, patch management, and user awareness, basics of incident response for infected systems, and best practices for preparing professional vulnerability assessment and malware analysis reports in a safe, ethical, and authorized environment. ***Practical:*** 28. Use the previously configured ethical hacking lab environment to perform vulnerability assessment activities on authorized lab targets. 29. Identify common system security weaknesses such as outdated software, weak passwords, unnecessary services, open ports, and insecure configurations. 30. Perform a basic vulnerability scan on a lab machine using teacher-approved tools and document the discovered issues. 31. Prepare a vulnerability classification sheet based on severity levels such as low, medium, high, and critical.	12	20%

	32. Study CVE and CVSS concepts and map selected vulnerabilities with their possible impact and risk score. 33. Analyze vulnerability scan results and differentiate between genuine findings, false positives, and false negatives. 34. Prepare a patch management checklist for securing a vulnerable system or lab machine. 35. Study password security by comparing weak passwords, strong passwords, password policies, hashing, and salting concepts. 36. Analyze common authentication weaknesses such as default credentials, weak password policy, and improper access control through lab-based examples. 37. Explore the Metasploit Framework interface and understand its role in controlled vulnerability demonstration without testing unauthorized systems. 38. Prepare a system hardening checklist covering user accounts, permissions, services, firewall settings, updates, and backup practices. 39. Analyze the malware infection lifecycle using a safe diagram-based or case-study-based approach without executing real malware. 40. Prepare a malware countermeasure report including antivirus, EDR, sandboxing, software updates, backup strategy, and user awareness.		

Examination Style:

Sr. No.	Evolution Method	SEE	CCE
1	**System Vulnerability Analysis and Risk Classification** Analyze an authorized lab system to identify vulnerabilities, classify their severity, assess their impact, and recommend suitable security hardening measures	05	-
2	**Malware Case Study and Incident Response Demonstration** Analyze a malware incident scenario and explain the malware type, infection method, impact, response process, recovery steps, and preventive measures.	05	-
3	**Active Learning Activity (ALA): Vulnerability Assessment and Malware Awareness** Prepare a structured report covering vulnerability assessment, risk classification, CVE and CVSS awareness, malware categories, system risks, and appropriate countermeasures.	-	10
	Total	10	10

Examination Style:

1. **System Vulnerability Analysis & Risk Classification (05 Marks):**
   - Students will use the previously configured ethical hacking lab environment to perform a basic system vulnerability analysis on a teacher-approved target machine. They must identify common weaknesses such as open ports, unnecessary services, weak passwords, default credentials, outdated software, insecure permissions, and missing security updates. Students must prepare a short risk classification table including vulnerability name, affected service/system, severity level, possible impact, and recommended solution. The deliverable must include

	screenshots, tool output summary, observation table, and a brief conclusion explaining how the identified weaknesses can affect system security. This task assesses the student's ability to analyze system vulnerabilities, prioritize risks, and recommend suitable hardening measure. **2. Malware Case Study & Incident Response Demonstration (05 Marks):** • Students will study a teacher-provided malware incident case scenario such as ransomware infection, phishing-based malware delivery, spyware/keylogger attack, or Trojan/backdoor compromise in a safe and authorized learning environment. They must identify the malware type, infection method, affected system components, possible impact, and warning signs observed in the scenario. Students will then demonstrate or explain the basic incident response steps including identification, isolation, containment, eradication, recovery, backup verification, patching, and user awareness measures. The deliverable must include a short case summary, incident response flow, preventive recommendations, and a 3–4 sentence conclusion explaining how proper response reduces security damage. This task evaluates students' understanding of malware behavior, incident handling process, system protection, and safe ethical response practices. **3. Active Learning Activity (ALA): Vulnerability Assessment and Malware Awareness (10 Marks):** • In this task, students will prepare a structured Vulnerability Assessment and Malware Awareness Report based on an authorized lab scenario. The report must include an explanation of vulnerability assessment, difference between vulnerability assessment and exploitation, common system vulnerabilities, security misconfigurations, weak authentication practices, outdated software risks, and exposed services. Students must classify selected vulnerabilities using severity levels such as Low, Medium, High, and Critical and relate them with basic CVE and CVSS awareness. The malware awareness section must cover types of malware such as viruses, worms, Trojans, ransomware, spyware, keyloggers, backdoors, and rootkits, along with their impact and prevention methods. Deliverables include a PDF/slide deck containing vulnerability observations, severity		

	classification, malware categories, preventive measures, and security recommendations. This activity evaluates students' ability to understand system-level weaknesses, classify security risks, and explain malware threats with suitable countermeasures.		
4	**Network Attack Analysis and Web Application Security** ***Theory Topics:*** Understanding common network attack concepts and their impact on confidentiality, integrity, and availability, packet sniffing concepts and risks of unencrypted communication, role of packet analysis in defensive security, session hijacking concepts and prevention techniques, Denial of Service and Distributed Denial of Service attack awareness, web server security fundamentals, common web server misconfigurations, introduction to web application security, OWASP Top 10 awareness, authentication and authorization weaknesses, insecure session management, input validation issues, SQL Injection concepts and prevention, Cross-Site Scripting concepts and prevention, Cross-Site Request Forgery awareness, insecure file upload risks, security issues in forms, cookies, and APIs, database security fundamentals, database attack concepts, risks of weak database credentials and exposed database ports, secure coding basics, prepared statements and parameterized queries, HTTPS and secure communication, web application testing methodology in authorized lab environments, use of Burp Suite and OWASP ZAP for safe request/response analysis, web security reporting format, and best practices for securing web applications, servers, and databases against common attacks. ***Practical:*** 41. Use the previously configured ethical hacking lab environment to perform network and web security analysis on authorized lab targets only. 42. Capture and analyze basic network traffic using Wireshark to understand protocols such as TCP, UDP, ICMP, DNS, HTTP, and HTTPS. 43. Analyze TCP three-way handshake and identify normal packet flow between client and server. 44. Capture HTTP request and response traffic in a controlled lab environment and identify headers, methods, status codes, cookies, and parameters.	12	20%

45. Study the risks of unencrypted communication by comparing HTTP and HTTPS traffic in a safe lab setup.
46. Analyze packet sniffing concepts and prepare a prevention checklist including encryption, HTTPS, VPN, and secure network configuration.
47. Study session management concepts by observing cookies, session IDs, and login/logout behavior in a vulnerable web application.
48. Prepare a case-based report on session hijacking concepts, possible risks, and prevention techniques.
49. Analyze Denial of Service and Distributed Denial of Service attacks through case-study-based learning without performing any real attack.
50. Use Burp Suite Community Edition to intercept and analyze request/response flow of a vulnerable lab web application.

Examination Style:

Sr. No.	Evolution Method	SEE	CCE
1	**Network Traffic Analysis and Packet Inspection Demonstration** Capture and analyze authorized network traffic to identify protocols, packet details, communication patterns, and potential security concerns.	05	-
2	**Web Application Vulnerability Testing and Security Report** Test a teacher - approved vulnerable web application, document identified weaknesses, assess their impact, and recommend suitable security measures.	05	-
3	**Active Learning Activity (ALA): Web and Network Security Analysis** Prepare a structured report covering network attacks, packet security, web vulnerabilities, database risks, secure coding practices, and appropriate countermeasures.	-	10
	Total	10	10

	Examination Style: **1. Network Traffic Analysis & Packet Inspection Demonstration (05 Marks):** • Students will use the previously configured ethical hacking lab environment to capture and analyze network traffic using **Wireshark** or any teacher-approved packet analysis tool. They must identify basic protocols such as TCP, UDP, ICMP, DNS, HTTP, and HTTPS and explain their role in communication. Students must observe packet details such as source IP, destination IP, protocol type, port number, request/response pattern, and basic header information. They should also compare normal traffic and suspicious traffic through a controlled lab or sample packet capture file. The deliverable must include packet screenshots, observation table, protocol explanation, and a short note on how packet analysis helps in defensive security. This task assesses the student's ability to inspect network communication, interpret packet-level information, and understand the importance of secure communication. **2. Web Application Vulnerability Testing & Security Report (05 Marks):** • Students will perform basic web application security testing on a teacher-approved vulnerable application such as DVWA, OWASP Juice Shop, or a lab-based web application. They must analyze authentication, session handling, input fields, forms, cookies, file upload functionality, and database-related security risks. Students may use tools such as Burp Suite Community Edition, OWASP ZAP, browser developer tools, and manual observation for request/response analysis in a controlled environment. They must document identified vulnerabilities with risk level, possible impact, evidence, and recommended countermeasures. The final deliverable must be a short web application security testing report including objective, scope, tools used, findings, screenshots, prevention methods, and conclusion. This task evaluates students' ability to identify web application weaknesses, connect them with secure coding practices, and prepare a professional security report.		

	3. **Active Learning Activity (ALA): Web and Network Security Analysis (10 Marks):** • In this task, students will prepare a structured Web and Network Security Analysis Report based on an authorized lab scenario. The report must include basic concepts of network attacks, packet sniffing, session hijacking awareness, DoS/DDoS attack concepts, web server security, web application vulnerabilities, and database security risks. Students must explain common web security issues such as weak authentication, insecure session handling, SQL Injection, Cross-Site Scripting, insecure file upload, poor input validation, and exposed database services. They must also include suitable preventive measures such as HTTPS usage, secure coding practices, input validation, parameterized queries, access control, secure cookies, and proper database configuration. Deliverables include a PDF/slide deck containing concepts, observations, risk explanation, screenshots from authorized lab work, and recommended countermeasures. This activity evaluates students' ability to understand network and web-based security risks and suggest practical protection mechanisms.		
5	**Wireless, Mobile, Cloud and Defensive Security** ***Theory Topics:*** Understanding wireless technologies and their role in modern network communication, fundamentals of wireless LAN security, common wireless security risks, overview of WPA, WPA2, and WPA3 security mechanisms, importance of strong wireless passwords and secure router configuration, wireless access control and network segmentation, mobile device security fundamentals, Android security basics, mobile application permission risks, secure mobile usage practices, mobile data protection and privacy awareness, introduction to cloud security, shared responsibility model in cloud computing, common cloud security risks and misconfigurations, identity and access management basics, secure storage and backup practices, intrusion detection systems and intrusion prevention systems, firewall concepts and types, honeypots and their role in security learning, social engineering concepts and human-based security risks, phishing awareness and prevention strategies, botnet concepts and their impact on digital infrastructure, physical security concepts, incident response basics, security audit checklist preparation, cyber security	12	20%

	documentation and reporting practices, and best practices for building a secure, aware, and defense-focused digital environment. ***Practical:*** 51. Analyze common wireless security settings such as SSID visibility, encryption type, password strength, guest network, and router admin access. 52. Compare WPA, WPA2, and WPA3 security mechanisms with their advantages, limitations, and recommended usage. 53. Study a wireless network security case scenario and identify possible risks such as weak passwords, open networks, default router credentials, and unauthorized access. 54. Analyze mobile device security settings such as screen lock, app permissions, device encryption, location access, backup settings, and unknown app installation. 55. Perform mobile application permission analysis for selected Android applications and classify permissions as low, medium, or high risk. 56. Prepare a mobile security awareness document covering safe app installation, permission control, data privacy, device lock, and secure browsing. 57. Prepare a complete security audit checklist for a small organization, computer lab, or academic department. 58. Analyze common social engineering and phishing scenarios and prepare prevention guidelines for identifying suspicious emails, messages, links, attachments, and human-based security threats. 59. Develop a final defensive security report combining wireless, mobile, cloud, firewall, IDS, social engineering, and physical security recommendations.		

Examination Style:

Sr. No.	Evolution Method	SEE	CCE
1	**Wireless, Mobile and Cloud Security Checklist Preparation** Prepare a structured checklist to identify risks, assess severity, and recommend protective measures for wireless, mobile, and cloud environments.	00	10
2	**Incident Response and Security Audit Demonstration** Analyze a security incident, prepare an appropriate response flow, conduct a basic security audit, and recommend suitable preventive controls.	05	00
3	**Active Learning Activity (ALA): Defensive Security Awareness and Audit Planning** Develop a comprehensive defensive security and audit plan covering wireless, mobile, cloud, network, physical, and human-related security risks.	05	00
	Total	10	10

Examination Style:

1. **Wireless, Mobile & Cloud Security Checklist Preparation (05 Marks):**
   - Students will prepare a detailed **security checklist** covering wireless networks, mobile devices, and cloud platforms. The wireless section must include SSID settings, WPA2/WPA3 usage, strong password policy, guest network configuration, router admin security, firmware update, and network segmentation. The mobile security section must include screen lock, app permissions, location access, unknown app installation, backup settings, and secure browsing practices. The cloud security section must include shared responsibility model, identity and access management, storage permissions, backup, monitoring, and prevention of public data exposure. The deliverable must include a checklist table with risk area, observation, severity, and recommended action. This task

	assesses the student's ability to apply security concepts for practical protection of wireless, mobile, and cloud environments. **2. Incident Response & Security Audit Demonstration (05 Marks):** • Students will be given a security incident or audit scenario related to phishing, unauthorized access, weak Wi-Fi security, mobile data leakage, cloud misconfiguration, or suspicious network activity. They must analyze the situation and prepare a basic incident response flow covering identification, containment, eradication, recovery, documentation, and reporting. Students must also suggest suitable preventive controls such as firewall rules, IDS/IPS monitoring, user awareness, strong authentication, secure backup, access control, and physical security measures. Deliverables include a short incident analysis document, audit checklist, response flow diagram, and final security recommendations. This task evaluates students' ability to analyze defensive security situations, prepare response strategies, and recommend practical controls for improving organizational security. **3. Active Learning Activity (ALA): Defensive Security Awareness and Audit Planning (10 Marks):** • In this task, students will prepare a structured Defensive Security Awareness and Audit Planning Report for a selected scenario such as a computer lab, small organization, academic department, or startup environment. The report must include wireless security practices, mobile device security, cloud security awareness, firewall and IDS/IPS concepts, phishing prevention, social engineering risks, physical security, and basic incident response planning. Students must identify possible security weaknesses such as weak Wi-Fi passwords, default router credentials, risky mobile app permissions, public cloud storage exposure, poor access control, and lack of user awareness. Deliverables include a PDF/slide deck summarizing identified risks, defensive controls, security awareness points, and an audit checklist. This activity evaluates students' ability to understand defensive cyber security practices and prepare a practical security improvement plan.		

Suggested Specification:

Distribution of Theory Marks (Revised Bloom's Taxonomy)						
Level	**Remembrance (R)**	**Understanding (U)**	**Application (A)**	**Analyze (N)**	**Evaluate (E)**	**Create (C)**
Weightage %	10%	15%	30%	15%	10%	20%

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcome:

After learning the course the students should be able to:	
CO1	Understand cyber security, ethical hacking concepts, threats, risks, and legal boundaries.
CO2	Perform basic footprinting, information gathering, and network scanning in an authorized lab.
CO3	Analyze system vulnerabilities, malware threats, and security misconfigurations.
CO4	Apply basic network and web security testing techniques using approved tools.
CO5	Prepare security checklists, incident response plans, and professional security reports.

Instructional Method:

The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

From the content 10% topics are suggested for flipped mode instruction.

Students will use supplementary resources such as online videos, NPTEL/SWAYAM videos/ e-courses, Virtual Laboratory.

The internal evaluation will be done on the basis of Active Learning Assignment.

Practical/Viva examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

Reference Books:

[1] Michael Gregg, *Certified Ethical Hacker Version 9*, Pearson IT Certification.
[2] Roger A. Grimes, *Hacking the Hacker*, Wiley Publications.
[3] *The Unofficial Guide to Ethical Hacking*, Premier Press.
[4] *Ethical Hacking and Countermeasures*, Cengage Learning.
[5] *Hands-on Ethical Hacking and Network Defense*, Cengage Learning.

Suggested Rubrics:

Suggested Assessment Guidelines

Module-1: Operating Systems, Networking and Ethical Hacking Fundamentals

Windows & Linux Live Command Demonstration (05 Marks)		
Criteria	**Description**	**Marks**
Command Execution and Practical Understanding	Correct execution of assigned Windows and Linux commands for file management, directory navigation, permissions, network configuration, and connectivity testing, along with a clear explanation of their purpose.	05
	Total	05

Network Troubleshooting & Ethical Hacking Concepts – Viva (05 Marks)		
Criteria	**Description**	**Marks**
Scenario Analysis and Conceptual Understanding	Logical analysis of the given networking or ethical hacking scenario, explanation of suitable troubleshooting steps or penetration-testing phases, and understanding of legal and ethical boundaries.	05
	Total	05

Module-2: Reconnaissance, Footprinting and Network Scanning

Footprinting and Information-Gathering Report (05 Marks)		
Criteria	**Description**	**Marks**
Information Gathering and Report Preparation	Accurate collection and documentation of domain, IP address, DNS, WHOIS, website, and technology information for a teacher-approved target, with suitable observations and adherence to ethical boundaries.	05
	Total	05

Network Scanning and Vulnerability-Mapping Demonstration (05 Marks)		
Criteria	**Description**	**Marks**
Scanning, Analysis and Risk Mapping	Correct use of Nmap in an authorized lab environment to identify active hosts, open ports, services, and versions, followed by appropriate mapping of findings to basic security risks and countermeasures.	05
	Total	05

Module-3: Vulnerability Assessment, System Security and Malware Defense

System Vulnerability Analysis and Risk Classification (05 Marks)		
Criteria	**Description**	**Marks**
Vulnerability Analysis and Risk Classification	Accurate identification of system vulnerabilities in an authorized lab environment, appropriate classification of their severity and impact, and recommendation of suitable security hardening measures.	05
	Total	05

Malware Case Study and Incident Response Demonstration (05 Marks)		
Criteria	**Description**	**Marks**
Malware Analysis and Incident Response	Correct analysis of the malware type, infection method, warning signs, and impact, along with a logical explanation of containment, eradication, recovery, and preventive measures.	05
	Total	05

Module-4: Network Attack Analysis and Web Application Security

Network Traffic Analysis and Packet Inspection Demonstration (05 Marks)		
Criteria	**Description**	**Marks**
Packet Capture and Traffic Analysis	Correct capture and analysis of authorized network traffic, identification of protocols, source and destination details, ports, packet headers, communication patterns, and potential security concerns.	05
	Total	05

Web Application Vulnerability Testing and Security Report (05 Marks)		
Criteria	**Description**	**Marks**
Vulnerability Testing and Security Reporting	Effective testing of a teacher-approved vulnerable web application, accurate documentation of identified weaknesses and their impact, and recommendation of suitable preventive and security measures.	05
	Total	05

Module-5: Wireless, Mobile, Cloud and Defensive Security

Wireless, Mobile and Cloud Security Checklist Preparation (05 Marks)		
Criteria	**Description**	**Marks**
Security Checklist and Risk Assessment	Preparation of a structured checklist that identifies wireless, mobile, and cloud security risks, classifies their severity, and recommends suitable protective measures.	05
	Total	05

Web Application Vulnerability Testing and Security Report (05 Marks)		
Criteria	**Description**	**Marks**
Incident Analysis and Security Audit	Logical analysis of the given security incident, preparation of an appropriate response flow, identification of audit findings, and recommendation of suitable preventive controls.	05
	Total	05