U23CBT63

ETHICAL HACKING

Comprehensive Learning Material

All Five Units — 45 Periods

Course Code	Credits	L	T	P
U23CBT63	3	3	0	0

Units Covered

Unit	Title	Periods
Unit I	Introduction to Ethical Hacking	9
Unit II	Footprinting, Reconnaissance and Scanning Networks	9
Unit III	Enumeration and Vulnerability Analysis	9
Unit IV	System Hacking	9
Unit V	Network Protection Systems	9

⚠ Legal Notice: All content in this material is strictly for educational purposes. Ethical hacking must only be performed with explicit written permission from the system owner. Unauthorized access is illegal under the IT Act and other applicable laws.

Course Objectives

The main learning objective of this course is to prepare the students to understand, analyze, and respond to cybersecurity threats through ethical hacking techniques. Upon completing this course, students will be able to:

1. Understand the basics of computer-based vulnerabilities — including attack types, malware, and TCP/IP architecture.
2. Explore different footprinting, reconnaissance, and scanning methods — to identify live hosts, open ports, and network topology.
3. Expose the enumeration and vulnerability analysis methods — for both Windows and Linux operating systems.
4. Understand hacking options available in Web and wireless applications — including web server attacks and wireless network exploitation.
5. Explore the options for network protection — including firewalls, IDS/IPS, and access control systems.
6. Practice tools to perform ethical hacking to expose the vulnerabilities — using industry-standard tools and methodologies.

What is Ethical Hacking?

Ethical hacking (also called penetration testing or white-hat hacking) is the practice of intentionally probing computer systems, networks, or web applications to find security vulnerabilities that a malicious hacker could potentially exploit. Unlike malicious hackers, ethical hackers have explicit permission from the system owner.

How to Use This Material

- Read each unit before attending the corresponding lecture.
- Pay special attention to key terms (highlighted in red) and definitions.
- Attempt the review questions at the end of each unit to test your understanding.
- Practice with tools ONLY in isolated lab environments with proper authorization.
- Cross-reference with CEH (Certified Ethical Hacker) study materials for exam preparation.

UNIT I
INTRODUCTION TO ETHICAL HACKING

1.1 Ethical Hacking Overview

Ethical hacking is a systematic, authorized process of bypassing system security to identify potential data breaches and threats in a network or system. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing.

Ethical Hacker: A security professional who uses hacking skills and techniques with the owner's permission to test and improve the security of computer systems and networks.

Penetration Testing: A simulated cyberattack against a computer system to check for exploitable vulnerabilities. Also called pen testing or pentesting.

1.1.1 Types of Hackers

Type	Description	Authorization
White Hat (Ethical)	Security professionals who test systems with full permission	Authorized
Black Hat (Malicious)	Hackers who break into systems for personal gain, crime, or damage	Unauthorized
Grey Hat	Hackers who may violate laws but without malicious intent — often report flaws	Without permission
Script Kiddies	Inexperienced individuals using existing tools/scripts without understanding	Unauthorized
Hacktivists	Hackers motivated by political or social goals (e.g., Anonymous)	Unauthorized
State-Sponsored	Government-backed hackers conducting cyber espionage or sabotage	State-authorized
Insider Threats	Employees or trusted individuals misusing their access	Misused authorization

1.1.2 Phases of Ethical Hacking

Phase	Name	Description
Phase 1	Reconnaissance	Passive and active information gathering about the target.

Phase 2	Scanning	Identify open ports, services, and live hosts on the network.
Phase 3	Gaining Access	Exploit vulnerabilities to gain unauthorized access.
Phase 4	Maintaining Access	Establish persistence — backdoors, rootkits, Trojans.
Phase 5	Clearing Tracks	Remove evidence of the intrusion from logs and files.

1.1.3 Types of Penetration Testing

- Black Box Testing: The tester has no prior knowledge of the system — simulates an external attacker.
- White Box Testing: The tester has full knowledge of the system — simulates an insider threat.
- Grey Box Testing: The tester has partial knowledge — simulates a semi-trusted user.
- External Testing: Attacks from outside the organization's network perimeter.
- Internal Testing: Attacks from within the network — simulating a malicious insider.
- Blind Testing: Organization knows a test is occurring but the tester has no information.

1.2 Role of Security and Penetration Testers

Security professionals play multiple roles in protecting organizational assets. The key roles and their responsibilities include:

Role	Responsibilities
Penetration Tester	Conduct authorized attacks, document findings, recommend remediation.
Security Analyst	Monitor systems for threats, analyze security events, maintain SIEM tools.
Vulnerability Assessor	Scan systems for known vulnerabilities, prioritize risks.
Security Engineer	Design and implement security controls and infrastructure.
Incident Responder	Investigate and respond to security breaches and incidents.
Red Team	Offensive team that simulates real-world attacks on an organization.
Blue Team	Defensive team that monitors, detects, and responds to attacks.
Purple Team	Collaboration between red and blue teams to improve defenses.

1.3 Penetration Testing Methodologies

Several well-established methodologies guide penetration testing engagements:

- OWASP Testing Guide: Focus on web application security testing.
- PTES (Penetration Testing Execution Standard): Covers all phases from pre-engagement to reporting.
- OSSTMM (Open Source Security Testing Methodology Manual): Scientific methodology for security testing.
- NIST SP 800-115: Technical guide to information security testing and assessment.
- CEH Methodology: EC-Council's certified ethical hacker framework used globally.

 Note: Always obtain written authorization (Rules of Engagement) before beginning any penetration test. Document everything.

1.4 Laws of the Land

Ethical hacking must be performed within the boundaries of applicable laws. Key legislation includes:

Law / Act	Country	Key Provision
IT Act 2000 (Amended 2008)	India	Section 43/66: Unauthorized access, hacking, data theft — imprisonment up to 3 years.
Computer Fraud & Abuse Act (CFAA)	USA	Prohibits unauthorized access to computer systems.
Computer Misuse Act 1990	UK	Makes unauthorized access and modification of computer material illegal.
GDPR	EU	Data protection regulation — breaches must be reported within 72 hours.
Cybercrime Convention	International	Council of Europe treaty on combating cybercrime.

 Legal Notice: Even with permission, ethical hackers must avoid accessing data they are not authorized to view, must not damage systems, and must protect confidential findings.

1.5 Overview of TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) is the fundamental communication protocol suite of the Internet. Understanding TCP/IP is essential for ethical hackers as most attacks target these protocols.

1.5.1 The TCP/IP Model Layers

Layer	Name	Protocol Examples	Function
Layer 4	Application Layer	HTTP, FTP, SMTP, DNS, SNMP	End-user applications and services
Layer 3	Transport Layer	TCP, UDP	End-to-end communication, segmentation, error recovery
Layer 2	Internet Layer	IP, ICMP, ARP, IGMP	Logical addressing and routing
Layer 1	Network Access	Ethernet, Wi-Fi, MAC	Physical transmission and framing

1.5.2 The Application Layer

The Application Layer is the topmost layer that interfaces directly with the end user's applications. Key protocols include:

- HTTP/HTTPS (Port 80/443): Web communication — a primary target for web application attacks.
- FTP (Port 20/21): File transfer — vulnerable to sniffing as credentials are sent in plaintext.
- SMTP (Port 25): Email sending — vulnerable to open relay attacks and email spoofing.
- DNS (Port 53): Domain name resolution — vulnerable to DNS poisoning and amplification attacks.
- SNMP (Port 161/162): Network device management — older versions (v1/v2) use weak community strings.
- SSH (Port 22): Secure remote login — brute force attacks are common against SSH.
- Telnet (Port 23): Insecure remote login — transmits data in plaintext, deprecated.

1.5.3 The Transport Layer

The Transport Layer provides end-to-end communication. The two main protocols are TCP and UDP:

Feature	TCP	UDP
Connection	Connection-oriented (3-way handshake)	Connectionless
Reliability	Reliable — guarantees delivery and order	Unreliable — no guarantee
Speed	Slower due to overhead	Faster — minimal overhead
Use Cases	HTTP, FTP, Email, SSH	DNS, VoIP, Video streaming, SNMP
Attack Relevance	SYN flood, TCP hijacking	UDP flood, DNS amplification

1.5.4 TCP Three-Way Handshake

TCP establishes connections using a three-way handshake — a process exploited in SYN flood attacks:

7. SYN: Client sends a SYN (synchronize) packet to the server.
8. SYN-ACK: Server responds with SYN-ACK (synchronize-acknowledge).
9. ACK: Client sends ACK — connection is established.

 Note: SYN Flood Attack: Attacker sends many SYN packets without completing the handshake, exhausting server resources.

1.5.5 The Internet Layer — IP Addressing

IP addressing provides unique identification for every device on a network. Key concepts:

- IPv4: 32-bit addresses (e.g., 192.168.1.1), divided into 4 octets. Approximately 4.3 billion addresses.
- IPv6: 128-bit addresses (e.g., 2001:0db8:85a3::8a2e:0370:7334). Virtually unlimited addresses.
- Subnet Mask: Defines the network and host portions of an IP address (e.g., 255.255.255.0 or /24).
- Private IP Ranges: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 — not routable on the public Internet.
- CIDR Notation: Classless Inter-Domain Routing — /24 means 24 bits for the network, 8 for hosts (256 addresses).

IP Class	Range	Default Subnet Mask	Usage
Class A	1.0.0.0 – 126.255.255.255	255.0.0.0 (/8)	Large organizations
Class B	128.0.0.0 – 191.255.255.255	255.255.0.0 (/16)	Medium organizations
Class C	192.0.0.0 – 223.255.255.255	255.255.255.0 (/24)	Small organizations
Loopback	127.0.0.0 – 127.255.255.255	—	Local host testing

1.6 Network and Computer Attacks

Understanding attack types is fundamental to ethical hacking. Attacks can be broadly categorized:

Attack Category	Examples	Description
Passive Attacks	Sniffing, Eavesdropping	Monitor and collect data without altering it — hard to detect
Active Attacks	DoS, MITM, Session Hijacking	Alter, disrupt, or destroy data or systems

Close-in Attacks	Social Engineering, Shoulder Surfing	Physical proximity to the target
Insider Attacks	Data Theft, Privilege Abuse	Misuse of authorized access by employees
Distribution Attacks	Supply Chain Attacks	Tampering with hardware/software before delivery

Common Attack Types

- Denial of Service (DoS/DDoS): Overwhelming a system to make it unavailable to legitimate users.
- Man-in-the-Middle (MITM): Intercepting communications between two parties without their knowledge.
- SQL Injection: Inserting malicious SQL code into input fields to manipulate databases.
- Cross-Site Scripting (XSS): Injecting malicious scripts into web pages viewed by other users.
- Phishing: Fraudulent emails/messages that trick users into revealing credentials or downloading malware.
- Brute Force: Systematically trying all possible passwords until the correct one is found.
- Buffer Overflow: Sending more data to a buffer than it can hold, overwriting adjacent memory.
- ARP Spoofing: Sending fake ARP messages to link the attacker's MAC address with a legitimate IP.

1.7 Malware

Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.

Malware Type	Description	Key Characteristic
Virus	Attaches to legitimate programs, spreads when executed	Requires host file, user activation
Worm	Self-replicating, spreads over networks without user action	No host needed, uses network vulnerabilities
Trojan Horse	Disguised as legitimate software to gain access	No self-replication, deceives users
Ransomware	Encrypts files, demands payment for decryption key	Monetarily motivated — e.g., WannaCry
Spyware	Secretly collects and transmits user data	Keyloggers, credential harvesters
Adware	Displays unwanted advertisements	Often bundled with free software

Rootkit	Hides malware and attacker's presence deep in OS	Very difficult to detect and remove
Botnet	Network of infected computers controlled remotely	Used for DDoS, spam, cryptocurrency mining
Keylogger	Records every keystroke made by the user	Captures passwords, messages, sensitive data

1.7.1 Protecting Against Malware Attacks

Effective defense against malware requires a layered security approach:

- Install and regularly update antivirus and anti-malware software.
- Keep all operating systems, browsers, and applications patched and up to date.
- Use a firewall to filter inbound and outbound network traffic.
- Enable email filtering and block malicious attachments and phishing links.
- Apply the principle of least privilege — users should only have the minimum access needed.
- Regularly back up critical data using the 3-2-1 rule (3 copies, 2 media types, 1 offsite).
- Conduct regular security awareness training for all staff.
- Use application whitelisting to prevent unauthorized software from running.
- Deploy Endpoint Detection and Response (EDR) solutions for advanced threat detection.

Unit I — Review Questions

10. Define ethical hacking. How does it differ from malicious hacking?
11. What are the five phases of ethical hacking? Describe each briefly.
12. Explain the TCP three-way handshake. How is it exploited in a SYN flood attack?
13. Distinguish between TCP and UDP. Give two attack examples for each.
14. Define and differentiate: Virus, Worm, Trojan Horse, and Ransomware.
15. What is a Rootkit? Why is it particularly dangerous?
16. List six measures to protect against malware attacks.
17. What are the different types of hackers? Explain the ethical/legal context of each.

UNIT II

FOOTPRINTING, RECONNAISSANCE AND SCANNING NETWORKS

2.1 Footprinting Concepts

Footprinting: The process of collecting as much information as possible about a target system, network, or organization before launching an attack. It is the first step in ethical hacking.

Footprinting helps an attacker understand the target's security posture, network architecture, operating systems, and potential entry points. The information gathered during footprinting guides all subsequent phases.

Types of Footprinting

Type	Description	Detectability
Passive Footprinting	Gathering information without directly interacting with the target — using public sources	Very Low — target is unaware
Active Footprinting	Directly interacting with the target system (e.g., port scanning, social engineering)	Higher — may trigger alerts
Anonymous Footprinting	Using proxies, VPNs, or anonymized tools to hide identity while gathering info	Low
Pseudonymous Footprinting	Using a fake identity or credentials to gather information	Moderate

2.1.1 Information Gathered During Footprinting

- Organization Information: Employee names, phone numbers, email addresses, office locations.
- Network Information: Domain names, IP address ranges, DNS records, network topology.
- System Information: Operating systems, web server software versions, open ports and services.
- Web Information: Website content, technologies used, login portals, hidden directories.
- Social Engineering Data: Organizational hierarchy, key personnel, relationships between employees.

2.2 Footprinting through Search Engines

Search engines index vast amounts of publicly available information, making them powerful footprinting tools.

Google Hacking (Google Dorking)

Google advanced search operators can reveal sensitive information accidentally exposed online:

Google Dork Operator	Purpose	Example
site:	Restrict results to a specific domain	site:example.com
filetype:	Find files of a specific type	filetype:pdf confidential site:example.com
intitle:	Find pages with keywords in the title	intitle:"admin login"
inurl:	Find pages with keywords in the URL	inurl:admin inurl:login
cache:	View Google's cached version of a page	cache:example.com
link:	Find pages linking to a URL	link:example.com
intext:	Find pages containing specific text	intext:"password" filetype:txt

 Note: The GHDB (Google Hacking Database) at exploit-db.com/google-hacking-database contains thousands of documented Google dorks used in security research.

2.3 Footprinting through Web Services

Several online services provide valuable reconnaissance data:

- WHOIS Lookup: Retrieves domain registration information — registrant name, email, phone, registrar, creation/expiry dates.
- DNS Lookup (nslookup / dig): Resolves domain names to IP addresses and retrieves DNS records (A, MX, NS, TXT, CNAME, SOA).
- ARIN / RIPE / APNIC: Regional Internet Registries — provide IP address and ASN allocation information.
- Netcraft: Shows hosting information, server technologies, uptime history, and SSL certificate details.
- Shodan: A search engine for Internet-connected devices — reveals open ports, banners, and vulnerabilities.
- Censys: Similar to Shodan — scans the entire Internet for open services and certificates.
- Archive.org (Wayback Machine): View historical versions of websites — may reveal removed sensitive content.

DNS Record Types

Record Type	Purpose	Example
A Record	Maps domain name to IPv4 address	example.com → 93.184.216.34
AAAA Record	Maps domain name to IPv6 address	example.com → 2606:2800::1

MX Record	Identifies mail servers for the domain	mail.example.com, priority 10
NS Record	Identifies authoritative name servers	ns1.example.com, ns2.example.com
CNAME Record	Alias for another domain name	www.example.com → example.com
TXT Record	Arbitrary text — used for SPF, DKIM	v=spf1 include:example.com ~all
SOA Record	Start of Authority — administrative info	Primary NS, admin email, serial number

2.4 Footprinting through Social Networking Sites

Social networking sites are rich sources of personal and organizational information:

- LinkedIn: Employee names, job titles, technologies used, organizational hierarchy, recent projects.
- Facebook/Instagram: Personal details, location check-ins, friend networks, event attendance.
- Twitter/X: Real-time posts, location data in metadata, professional relationships.
- GitHub/GitLab: Source code repositories may accidentally expose API keys, passwords, and internal infrastructure details.
- Job Postings: Reveal the technologies an organization uses, open positions suggest weak areas.

2.5 Competitive Intelligence

Competitive intelligence involves gathering information about a target organization from business and commercial sources:

- Annual Reports and SEC Filings: Financial information, key risks, technology investments.
- Press Releases: New products, partnerships, acquisitions, personnel changes.
- Patent Databases: Reveal proprietary technologies and R&D directions.
- Business Registries: Company structure, directors, registered addresses.
- Intelligence Platforms: Maltego, SpiderFoot for automated OSINT (Open Source Intelligence) gathering.

2.6 Footprinting through Social Engineering

Social Engineering: Psychological manipulation of people to reveal confidential information or perform actions that compromise security. It exploits human trust rather than technical vulnerabilities.

Technique	Description	Example
Phishing	Sending fraudulent emails to	Fake bank login page email

	steal credentials	
Spear Phishing	Targeted phishing aimed at a specific individual	Fake email from CEO to CFO
Vishing	Voice phishing — phone calls impersonating authority	Fake IT support call asking for password
Smishing	SMS-based phishing	Fake bank SMS with malicious link
Pretexting	Creating a fabricated scenario to extract info	Fake vendor calling HR for employee list
Baiting	Leaving infected USB drives for victims to find	USB labelled 'Salary 2024' left in lobby
Tailgating	Physically following authorized person into secure area	Carrying boxes to 'help' entering a server room

2.7 Footprinting Tools

Tool	Purpose	Category
Maltego	Visualize relationships between people, domains, networks, organizations	OSINT / Visualization
Recon-ng	Web reconnaissance framework with modular approach	OSINT Framework
theHarvester	Collect emails, names, hosts, subdomains from public sources	Email / Domain OSINT
SpiderFoot	Automated OSINT data collection and correlation	OSINT Automation
FOCA	Extract metadata from documents (PDFs, Word files)	Metadata Analysis
Metagoofil	Extract metadata from publicly available documents	Metadata Analysis
Whois	Domain registration information lookup	DNS/WHOIS

2.8 Network Scanning Concepts

Network Scanning: The process of identifying active hosts, open ports, and running services on a network. It provides a map of the attack surface.

Types of Scanning

- Port Scanning: Identify which ports are open on a target host and what services are running.
- Network Scanning: Discover all active hosts (IP addresses) on a network — using ping sweeps or ARP.
- Vulnerability Scanning: Automated scanning for known vulnerabilities on identified systems.
- OS Fingerprinting: Determine the operating system and version running on a host.
- Service Version Detection: Identify the exact version of services (e.g., Apache 2.4.51).

2.9 Port Scanning Tools

2.9.1 Nmap (Network Mapper)

Nmap is the most widely used network scanning and discovery tool. It can identify live hosts, open ports, services, OS versions, and even specific vulnerabilities.

Nmap Command	Purpose
nmap 192.168.1.1	Basic TCP scan of a single host
nmap -sn 192.168.1.0/24	Ping sweep — discover all live hosts in a subnet
nmap -sS target	Stealth SYN scan — half-open scan, less detectable
nmap -sU target	UDP scan — identifies UDP services
nmap -sV target	Service version detection
nmap -O target	Operating system detection
nmap -A target	Aggressive scan — OS, version, scripts, traceroute
nmap -p 1-1000 target	Scan specific port range
nmap -p- target	Scan all 65535 ports
nmap --script vuln target	Run vulnerability scripts

2.9.2 Other Scanning Tools

- Angry IP Scanner: Fast, lightweight GUI-based IP and port scanner.
- Masscan: Extremely fast port scanner — can scan the entire Internet in minutes.
- Hping3: Command-line TCP/IP packet assembler — useful for crafting custom packets.
- Zenmap: Graphical frontend for Nmap with scan profiles and topology mapping.
- NetScanTools: Commercial scanning suite for professional network auditing.

2.10 Scanning Techniques

Scan Type	Method	Use Case

TCP Connect Scan (-sT)	Completes full 3-way handshake — easily logged	When stealth is not required
SYN Stealth Scan (-sS)	Sends SYN, receives SYN-ACK, sends RST — never completes handshake	Default stealth scan
FIN Scan (-sF)	Sends FIN packet — closed ports reply RST, open ports ignore	Bypass older firewalls
NULL Scan (-sN)	Sends packet with no flags set	Bypass stateless firewalls
XMAS Scan (-sX)	Sends FIN+PSH+URG flags — like a Christmas tree	Firewall bypass testing
ACK Scan (-sA)	Determine if ports are filtered or unfiltered by a firewall	Firewall rule mapping
Idle Scan (-sI)	Uses a 'zombie' host to send packets — attacker's IP hidden	Ultra-stealth scanning
UDP Scan (-sU)	Sends UDP packets — slower, less reliable	Find UDP services like DNS, SNMP

2.11 Scanning Beyond IDS and Firewall

Intrusion Detection Systems (IDS) and firewalls can detect and block scanning activity. Ethical hackers use various techniques to evade these defenses:

- Fragmentation: Split packets into smaller fragments that the IDS cannot reassemble for analysis.
- Decoy Scanning (nmap -D): Use multiple decoy IP addresses to hide the real source.
- Idle Scanning: Use a zombie host so the attacker's IP never appears in target logs.
- Slow Scanning: Spread scans over long time periods to avoid triggering rate-based IDS alerts.
- Source Port Manipulation: Use trusted source ports (e.g., 80, 443) that firewalls may allow through.
- IPv6 Evasion: Some security tools have weaker IPv6 monitoring — use IPv6 to bypass IPv4 defenses.
- Proxy Chains: Route scanning traffic through multiple proxies to obscure origin.

Unit II — Review Questions

18. Define footprinting. What is the difference between passive and active footprinting?
19. What is Google Dorking? Give three examples of useful Google dork operators.
20. List and explain five types of DNS records that are useful during reconnaissance.
21. What is Shodan and how is it used in ethical hacking?

22. Define social engineering. Describe phishing, spear phishing, and vishing.
23. Explain the difference between a SYN scan and a TCP Connect scan.
24. What is an XMAS scan? What flags does it set and what is its purpose?
25. Describe four techniques used to evade IDS detection during scanning.

UNIT III

ENUMERATION AND VULNERABILITY ANALYSIS

3.1 Enumeration Concepts

Enumeration: The process of extracting detailed information from a target system — such as usernames, group names, machine names, shared resources, and services — by establishing active connections to the system.

Enumeration goes beyond scanning — it establishes active connections and queries systems for specific information. It provides the detailed data needed to prepare an attack.

Information Extracted During Enumeration

- User account names and group memberships.
- Computer names, hostnames, and domain information.
- Shared folders, printers, and network resources.
- Running services and their versions.
- Routing tables and ARP tables.
- Active Directory structure (if applicable).
- SNMP information: MIB data, device configurations.
- Application banners: web server, FTP, SSH version info.

3.2 NetBIOS Enumeration

NetBIOS: Network Basic Input/Output System — an API that allows applications on different computers to communicate across a local network. Uses ports 137 (UDP), 138 (UDP), and 139 (TCP).

NetBIOS enumeration can reveal computer names, logged-in users, MAC addresses, and shared resources on a Windows network.

- nbtstat -A <IP>: Query a remote host's NetBIOS name table.
- nbtstat -n: Display local NetBIOS name table.
- net view \\<hostname>: List shared resources on a Windows host.
- NetBIOS codes reveal the machine name, domain, and services (e.g., <00> = workstation, <20> = file server).
- Countermeasure: Disable NetBIOS over TCP/IP if not required. Block ports 137-139 at the firewall.

3.3 SNMP Enumeration

SNMP: Simple Network Management Protocol — used to monitor and manage network devices (routers, switches, printers, servers). Runs on UDP port 161 (agent) and 162 (manager).

SNMP Version	Security Level	Risk
SNMPv1	Community string only	Highly vulnerable —

	(plaintext)	community string sniffable
SNMPv2c	Community string (still plaintext)	Still vulnerable — widely deployed
SNMPv3	Username/password with encryption (AES/DES)	Secure if properly configured

Default community strings — 'public' (read) and 'private' (write) — are frequently left unchanged and easily guessed.

- snmpwalk -v2c -c public <IP>: Walk the entire MIB tree of a target device.
- snmpget -v1 -c public <IP> OID: Retrieve a specific OID value.
- Tools: SNMPScanner, SolarWinds IP Network Browser, OpUtils.
- Countermeasure: Use SNMPv3, change default community strings, restrict SNMP access by ACL.

3.4 LDAP Enumeration

LDAP: Lightweight Directory Access Protocol — used to access and maintain distributed directory information services (e.g., Microsoft Active Directory). Default port: 389 (LDAP), 636 (LDAPS).

LDAP enumeration can reveal Active Directory objects including users, computers, groups, organizational units (OUs), and policies.

- ldapsearch command on Linux: Query AD for all user objects.
- Tools: JXplorer, SoftTerra LDAP Browser, AD Explorer (Sysinternals).
- Anonymous LDAP binding (if enabled) allows enumeration without credentials.
- Countermeasure: Disable anonymous LDAP binding, restrict LDAP access, use LDAPS (encrypted).

3.5 NTP Enumeration

NTP: Network Time Protocol — synchronizes clocks of networked computers. Runs on UDP port 123.

NTP servers can be queried to reveal information about connected hosts:

- ntpq -p <IP>: Query an NTP server for its peer list — may reveal internal hostnames and IP addresses.
- ntptrace: Trace the time synchronization chain.
- monlist command (deprecated): Used to enumerate all clients that have synchronized with the NTP server — also used in NTP amplification DDoS attacks.
- Countermeasure: Disable monlist, use NTP authentication, restrict NTP access.

3.6 SMTP Enumeration

SMTP: Simple Mail Transfer Protocol — used for sending email. Default port: 25 (unencrypted), 587 (submission), 465 (SMTPS).

SMTP servers can be used to enumerate valid user accounts:

- VRFY command: Verify if a user exists on the mail server (e.g., VRFY admin).
- EXPN command: Expand a mailing list to reveal all member addresses.
- RCPT TO: Send test email to enumerate valid addresses — different error messages reveal existence.
- smtp-user-enum tool: Automates SMTP user enumeration.
- Countermeasure: Disable VRFY and EXPN commands, configure consistent error messages.

3.7 DNS Enumeration

DNS enumeration extracts information about the DNS infrastructure:

- DNS Zone Transfer (AXFR): If misconfigured, reveals all DNS records for a domain — attacker gets full map of network.
- dig axfr @nameserver domain.com: Attempt a zone transfer.
- DNS Brute Forcing: Try common subdomain names to discover hidden hosts.
- Tools: DNSRecon, Fierce, Sublist3r.
- Countermeasure: Restrict zone transfers to authorized secondary name servers only.

3.8 Vulnerability Assessment Concepts

Vulnerability: A weakness in a system, application, or network that can be exploited by a threat actor to gain unauthorized access or cause harm.

Vulnerability Assessment: The systematic process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system — without exploiting them.

Distinction between vulnerability assessment and penetration testing:

Aspect	Vulnerability Assessment	Penetration Testing
Goal	Identify and list vulnerabilities	Exploit vulnerabilities to assess real risk
Depth	Wide but shallow — finds many issues	Narrow but deep — verifies exploitability
Risk	Low risk to the target system	Higher risk — may impact availability
Output	List of vulnerabilities with severity ratings	Proof of exploitation, business impact
Frequency	Regular, automated scans	Periodic, scheduled engagements

Vulnerability Scoring — CVSS

The Common Vulnerability Scoring System (CVSS) provides a standardized way to rate the severity of vulnerabilities:

CVSS Score	Severity	Action Required

9.0 – 10.0	Critical	Patch immediately — active exploitation likely
7.0 – 8.9	High	Patch within 24-72 hours
4.0 – 6.9	Medium	Patch within 30 days
0.1 – 3.9	Low	Patch at next maintenance window
0.0	None	No vulnerability

3.9 Desktop and Server OS Vulnerabilities

3.9.1 Windows OS Vulnerabilities

Windows systems are the most targeted due to their widespread use in enterprise environments.

- SMB Vulnerabilities: EternalBlue (MS17-010) — exploited by WannaCry ransomware and NotPetya.
- RDP Vulnerabilities: BlueKeep (CVE-2019-0708) — remote code execution via RDP (port 3389).
- Unpatched Systems: Many organizations run outdated Windows versions without critical patches.
- Weak Password Policies: Default or weak passwords on administrator accounts.
- NTLM Hash Exposure: Pass-the-Hash attacks — steal NTLM hashes and replay them without needing the plaintext password.
- Privilege Escalation: Token Impersonation (Meterpreter getsystem), DLL Hijacking, Registry exploits.
- Tools for Windows Vulnerability Identification: Nessus, OpenVAS, Microsoft Baseline Security Analyzer (MBSA).

3.9.2 Linux OS Vulnerabilities

Linux systems, while generally more secure, are not immune to vulnerabilities:

- Shellshock (CVE-2014-6271): Bash vulnerability allowing remote code execution via CGI scripts.
- Dirty COW (CVE-2016-5195): Privilege escalation via race condition in the kernel.
- Misconfigured SUID Binaries: Exploitable to gain root privileges.
- Weak SSH Configuration: Root login enabled, weak ciphers, no fail2ban protection.
- Insecure Cron Jobs: World-writable scripts running as root.
- Outdated Kernel: Privilege escalation exploits targeting unpatched kernels.
- Tools: Lynis (Linux security auditing), LinEnum (Linux privilege escalation enumeration).

3.9.3 Vulnerabilities of Embedded OSes

Embedded operating systems power IoT devices, routers, printers, and industrial systems (ICS/SCADA). They present unique security challenges:

- Default Credentials: Most IoT devices ship with default username/password (admin/admin) — rarely changed.
- No Update Mechanism: Many embedded devices cannot be patched or receive updates infrequently.
- Insecure Protocols: Telnet, HTTP without TLS, old SNMP versions.
- Firmware Vulnerabilities: Extractable firmware may contain hardcoded credentials or cryptographic keys.
- Physical Access: Many embedded devices lack physical security.

Unit III — Review Questions

26. Define enumeration. How does it differ from scanning?
27. What information can be gathered through NetBIOS enumeration?
28. Explain why SNMPv1 and v2c are considered insecure. What is the recommended version?
29. What is a DNS Zone Transfer? Why is it a security risk if misconfigured?
30. Distinguish between vulnerability assessment and penetration testing.
31. What is CVSS? How are vulnerabilities scored?
32. Describe the EternalBlue vulnerability. What attack was it used in?
33. What are the unique security challenges of embedded operating systems?

UNIT IV
SYSTEM HACKING

4.1 Hacking Web Servers

Web servers are high-value targets because they are publicly accessible and often connected to backend databases and internal networks. A compromised web server can be a gateway into the entire organization.

Web Server: A computer system that processes requests via HTTP/HTTPS and delivers web content. Common web servers include Apache, Nginx, Microsoft IIS, and Tomcat.

4.1.1 Common Web Server Attacks

Attack	Description	Target
Directory Traversal	Accessing files outside the web root by manipulating paths (../../../etc/passwd)	File system
HTTP Response Splitting	Inject CRLF sequences to split HTTP responses	Browser/Proxy
Web Cache Poisoning	Poison the cache to serve malicious content to users	CDN/Proxy cache
Server-Side Request Forgery (SSRF)	Force server to make requests to internal resources	Internal network
File Inclusion (LFI/RFI)	Include local or remote files via vulnerable PHP parameters	Application files
Banner Grabbing	Read server banner to identify software version for targeted exploits	Server identification
Misconfiguration Exploits	Default pages, open directory listing, debug mode enabled	Server configuration

4.1.2 Web Server Attack Methodology

34. Information Gathering: Identify web server software (Apache, IIS, Nginx) and version via banner grabbing, HTTP headers, error pages.
35. Footprinting: Enumerate website structure, hidden directories (using Gobuster, Dirb), and files.
36. Mirroring: Download a complete copy of the website for offline analysis.
37. Vulnerability Scanning: Use Nikto, Nessus to identify known web server vulnerabilities.
38. Session Hijacking: Intercept or steal session cookies after user authentication.
39. Password Attacks: Brute force admin login pages using Hydra or Burp Suite Intruder.

4.2 Web Application Components and Vulnerabilities

4.2.1 OWASP Top 10 Vulnerabilities

The OWASP (Open Web Application Security Project) Top 10 is the industry-standard list of the most critical web application security risks:

Rank	Vulnerability	Description
A01	Broken Access Control	Users can act outside their intended permissions — access other users' data
A02	Cryptographic Failures	Sensitive data exposed due to weak/absent encryption
A03	Injection	SQL, OS, LDAP injection — untrusted data sent as part of a command
A04	Insecure Design	Missing security controls in the design and architecture phase
A05	Security Misconfiguration	Default credentials, unnecessary features, verbose errors
A06	Vulnerable Components	Using libraries/frameworks with known vulnerabilities
A07	Authentication Failures	Weak passwords, missing MFA, session management issues
A08	Software/Data Integrity Failures	Unverified updates, insecure deserialization
A09	Logging/Monitoring Failures	Insufficient logging — attacks go undetected
A10	SSRF	Server-side request forgery to internal services

4.2.2 SQL Injection (SQLi)

SQL Injection is one of the most dangerous and prevalent web application vulnerabilities. It occurs when user input is incorporated into SQL queries without proper sanitization.

- Classic SQLi: ' OR '1'='1' -- injected in a login form bypasses authentication.
- Blind SQLi: No visible output — attacker infers data through boolean (true/false) responses.
- Time-Based Blind SQLi: Infer data through response delay (SLEEP() or WAITFOR DELAY).
- Union-Based SQLi: UNION SELECT statement appended to retrieve data from other tables.
- Error-Based SQLi: Trigger database errors that reveal schema information.
- Tools: sqlmap (automated SQLi exploitation), Havij, Burp Suite.
- Defense: Use parameterized queries (prepared statements), input validation, WAF.

4.2.3 Cross-Site Scripting (XSS)

XSS attacks inject malicious scripts into web pages that are then executed in other users' browsers:

- Stored XSS (Persistent): Malicious script stored on the server (e.g., in a database) and served to all visitors.
- Reflected XSS (Non-Persistent): Script reflected off the server in an HTTP response — requires tricking user into clicking a crafted URL.
- DOM-Based XSS: Vulnerability in client-side JavaScript that modifies the DOM.
- Impact: Cookie theft, session hijacking, keylogging, phishing, malware delivery.
- Defense: Output encoding, Content Security Policy (CSP), HttpOnly cookies, input validation.

4.3 Tools for Web Attackers and Security Testers

Tool	Purpose	Category
Burp Suite	Web application security testing platform — intercept/modify HTTP requests	Web Testing Suite
OWASP ZAP	Free web application security scanner with active/passive scanning	Web Scanner
Nikto	Web server vulnerability scanner — checks for 6700+ issues	Web Server Scanner
sqlmap	Automated SQL injection detection and exploitation tool	SQL Injection
Metasploit Framework	Exploitation framework with thousands of modules for known CVEs	Exploitation
Gobuster / Dirb	Directory and file brute forcing for hidden web resources	Directory Enumeration
Wfuzz	Web application fuzzer — parameter fuzzing, directory discovery	Fuzzing
Hydra	Fast online password brute-forcing tool for many protocols	Password Attack

4.4 Hacking Wireless Networks

Wireless networks present unique security challenges because radio signals extend beyond physical boundaries, making them accessible to anyone within range.

4.4.1 Components of a Wireless Network

Component	Description
Access Point (AP)	Hardware device that creates the wireless network and bridges wireless to wired LAN
SSID	Service Set Identifier — the name of the wireless network broadcast by the AP
BSSID	Basic Service Set Identifier — the MAC address of the access point
WPA/WPA2/WPA3	Wi-Fi Protected Access — wireless security protocols (WPA3 is current standard)
TKIP	Temporal Key Integrity Protocol — WPA encryption (now deprecated/insecure)
AES/CCMP	Advanced Encryption Standard — WPA2/3 encryption (currently secure)
802.11 Standards	Wi-Fi standards: 802.11a/b/g/n/ac/ax (Wi-Fi 6) defining speed and frequency

4.4.2 Wireless Security Protocols

Protocol	Encryption	Status	Vulnerability
WEP	RC4 (40/104-bit)	Broken — completely insecure	Crackable in minutes using aircrack-ng
WPA	TKIP with RC4	Deprecated — insecure	TKIP vulnerabilities, dictionary attacks
WPA2	AES-CCMP (128-bit)	Current standard — secure if configured properly	KRACK attack, PMKID, dictionary attacks
WPA3	AES-256 with SAE	Latest — most secure	Implementation vulnerabilities (Dragonblood)

4.5 Wardriving

Wardriving: The practice of driving around in a vehicle with a laptop and wireless adapter to discover and map Wi-Fi networks. Also called warwalking, warbiking, or warchalking.

Wardriving tools and techniques:

- Kismet: Wireless network detector, sniffer, and IDS — works in monitor mode.
- inSSIDer: Wireless network scanner showing SSID, channel, signal strength, security type.
- NetStumbler: Windows-based wireless scanner.
- Wigle.net: Crowdsourced database of wireless networks discovered during wardriving.
- GPS Integration: Tools integrate with GPS to map network locations geographically.

4.6 Wireless Hacking Techniques

4.6.1 WEP Cracking

WEP encryption is completely broken and can be cracked in minutes:

40. Enable monitor mode: airmon-ng start wlan0
41. Capture traffic: airodump-ng -c <channel> --bssid <AP_MAC> -w capture wlan0mon
42. Inject traffic (to generate IVs): aireplay-ng -3 -b <AP_MAC> wlan0mon
43. Crack the key: aircrack-ng capture-01.cap (requires ~50,000-100,000 IVs)

4.6.2 WPA/WPA2 Cracking

- 4-way Handshake Capture: Deauthenticate a client to force reconnection and capture the WPA handshake.
- Dictionary/Brute Force: aircrack-ng -w wordlist.txt -b <BSSID> capture.cap
- PMKID Attack: Capture PMKID from a single EAPOL frame — does not require a client to be present.
- Evil Twin Attack: Create a fake AP with the same SSID — force clients to connect and steal credentials.
- WPS PIN Attack: Exploit the Wi-Fi Protected Setup PIN feature (if enabled) using Reaver.

4.6.3 Additional Wireless Attacks

- Rogue Access Point: Set up an unauthorized AP inside an organization to intercept traffic.
- Deauthentication Attack: Send forged 802.11 deauth frames to disconnect clients (used in capture attacks).
- MITM via Wireless: Use tools like ettercap or bettercap to intercept wireless traffic.
- Bluetooth Attacks: Bluejacking, Bluesnarfing, BlueSmack — targeting Bluetooth-enabled devices.

4.7 Tools of the Trade

Tool	Category	Purpose
aircrack-ng Suite	Wireless	Monitor, capture, and crack WEP/WPA wireless keys
Kali Linux	OS/Platform	Dedicated security testing OS with 600+ pre-installed tools
Metasploit Framework	Exploitation	Exploit known vulnerabilities, create and deploy payloads
Wireshark	Network Analysis	Packet capture and protocol analysis
John the Ripper	Password Cracking	Offline password hash cracking — dictionary and brute force
Hashcat	Password Cracking	GPU-accelerated password cracking — very fast

Netcat (nc)	Network	TCP/UDP connections, port scanning, file transfer, backdoors
Mimikatz	Credential Theft	Extract plaintext passwords and hashes from Windows memory
BeEF	Browser Exploitation	Browser Exploitation Framework — XSS hook attacks
Empire / PowerShell Empire	Post-Exploitation	Post-exploitation framework using PowerShell agents

Unit IV — Review Questions

44. What is directory traversal? Provide an example of a malicious path.
45. Explain SQL Injection. What is the difference between classic SQLi and blind SQLi?
46. What is Stored XSS? How does it differ from Reflected XSS?
47. Describe the four wireless security protocols (WEP, WPA, WPA2, WPA3) and their security status.
48. What is wardriving? List three tools commonly used for wardriving.
49. Explain the four steps to crack WEP using the aircrack-ng suite.
50. What is an Evil Twin Attack? How does it work?
51. What is Mimikatz used for in post-exploitation?

UNIT V
NETWORK PROTECTION SYSTEMS

5.1 Access Control Lists (ACLs)

Access Control List (ACL): A set of rules (permit/deny entries) applied to a router interface or firewall that controls which traffic is allowed or blocked based on specified criteria.

ACLs are the fundamental building block of network security policy. They are implemented on routers, firewalls, and switches to filter traffic.

5.1.1 Types of ACLs

ACL Type	Cisco Numbering	Match Criteria	Best Placed
Standard ACL	1–99, 1300–1999	Source IP address only	Close to destination
Extended ACL	100–199, 2000–2699	Source IP, destination IP, protocol, port	Close to source
Named ACL	Named string	Same as extended — more readable	Flexible placement
Dynamic ACL	Lock-and-key	User authenticates, then temporary permit added	Remote access
Reflexive ACL	Session-based	Automatically permit return traffic	Stateful-like filtering

5.1.2 ACL Rules and Best Practices

- Implicit Deny: Every ACL ends with an implicit 'deny any any' — if traffic does not match any rule, it is dropped.
- Top-Down Processing: ACL rules are processed from top to bottom — first match wins.
- Most Specific First: Place more specific rules before general ones to prevent premature matching.
- Inbound vs Outbound: Inbound ACL filters traffic entering an interface; outbound filters traffic leaving.
- Minimize Rules: Too many rules reduce performance — consolidate where possible.
- Document ACLs: Always include remarks explaining the purpose of each rule.

5.1.3 Extended ACL Example Logic

An extended ACL might include rules such as:

- Permit TCP from 192.168.1.0/24 to any port 80 — allow internal users to browse the web.
- Permit TCP from any to 10.0.0.5 port 443 — allow HTTPS to the web server.

- Deny ICMP from any to any — prevent ping-based reconnaissance.
- Deny TCP from any to any port 23 — block Telnet (insecure protocol).

5.2 Cisco Adaptive Security Appliance (ASA) Firewall

The Cisco ASA is a market-leading enterprise firewall and security appliance. It provides stateful packet inspection, VPN, intrusion prevention, and application-aware security.

5.2.1 Security Levels

Cisco ASA uses security levels (0–100) to determine trust between interfaces:

Interface	Default Security Level	Description
Inside (LAN)	100	Most trusted — internal corporate network
DMZ	50	Semi-trusted — servers accessible from Internet (web, email, DNS)
Outside (Internet)	0	Least trusted — untrusted public network

By default, traffic from higher security levels to lower is permitted (inside to outside). Traffic from lower to higher is denied unless explicitly permitted by an ACL.

5.2.2 DMZ Architecture

A DMZ (Demilitarized Zone) is a network segment that sits between the trusted internal network and the untrusted Internet:

- Hosts public-facing services: Web servers, email servers, DNS, FTP.
- If a DMZ server is compromised, the attacker cannot directly reach the internal network.
- The ASA applies different security policies to traffic flowing between the three zones.

5.2.3 Key ASA Features

- Stateful Inspection: Tracks all active TCP/UDP connections — automatically permits return traffic.
- Network Address Translation (NAT/PAT): Hides internal IP addresses from external networks.
- VPN Termination: Site-to-site IPsec VPN and remote access SSL/AnyConnect VPN.
- Application Inspection: Deep packet inspection for specific protocols (HTTP, FTP, SIP, SMTP).
- URL Filtering: Block access to malicious or inappropriate websites.
- Botnet Traffic Filter: Detect and block known botnet command-and-control communication.

5.3 Configuration and Risk Analysis Tools for Firewalls and Routers

Tool	Purpose

Cisco Security Manager (CSM)	Centralized management for Cisco ASA, IPS, and router security policies
Nipper Studio	Firewall and router configuration auditing — identifies misconfigurations
FireMon	Firewall rule analysis, risk assessment, and compliance reporting
AlgoSec	Firewall policy management and security risk analysis
Tufin	Network security policy management across multi-vendor environments
Skybox Security	Network vulnerability and attack surface analysis

5.4 Intrusion Detection and Prevention Systems

IDS (Intrusion Detection System): A system that monitors network or host activity, analyzes it for suspicious patterns or known attacks, and generates alerts — but does NOT block traffic.

IPS (Intrusion Prevention System): An active security system that monitors traffic, detects attacks (like an IDS), AND automatically takes action to block or drop malicious traffic in real time.

Feature	IDS	IPS
Mode of Operation	Passive — monitors and alerts	Inline — monitors and blocks
Placement	Network tap or SPAN port (out of band)	Inline — all traffic passes through
Response	Alerts only — no automatic blocking	Drops packets, resets connections, blocks IPs
Risk of False Positives	Generates alert (less disruptive)	Can block legitimate traffic (more disruptive)
Performance Impact	Minimal — not inline	Some latency — all traffic inspected

5.4.1 IDS/IPS Detection Methods

Method	Description	Advantage / Disadvantage
Signature-Based	Compares traffic to a database of known attack signatures	Accurate for known attacks; cannot detect zero-days
Anomaly-Based	Establishes a baseline of normal behavior; flags deviations	Detects unknown attacks; high false positive rate
Stateful Protocol Analysis	Compares protocol behavior	Effective for protocol abuse;

	against expected standards	resource intensive
Heuristic-Based	Uses rules and algorithms to identify suspicious behavior	Catches new variants; may miss highly novel attacks

5.4.2 Types of IDS/IPS

- Network-Based IDS/IPS (NIDS/NIPS): Monitors all traffic on a network segment. Examples: Snort, Suricata, Cisco Firepower.
- Host-Based IDS/IPS (HIDS/HIPS): Monitors activity on a specific host — file integrity, log analysis, process activity. Examples: OSSEC, Wazuh, Tripwire.
- Wireless IDS/IPS (WIDS/WIPS): Monitors wireless networks for rogue APs, unauthorized clients, wireless attacks.
- Network Behavior Analysis (NBA): Analyzes network traffic flows to detect anomalies at scale.

5.4.3 Snort — Open Source IDS/IPS

Snort is the world's most widely deployed open-source IDS/IPS. It operates in three modes:

- Sniffer Mode: Simply reads and displays network packets.
- Packet Logger Mode: Logs packets to disk for later analysis.
- NIDS/NIPS Mode: Analyzes traffic in real time and alerts/blocks based on rules.

A Snort rule format: alert tcp any any -> 192.168.1.0/24 80 (msg:"HTTP Traffic"; sid:1001; rev:1;)

5.5 Network-Based and Host-Based IDSs and IPSs

Comparing NIDS and HIDS

Aspect	NIDS/NIPS	HIDS/HIPS
Scope	Monitors the entire network segment	Monitors only the individual host
Visibility	All traffic on the segment	All activity on the host (processes, files, logs)
Encrypted Traffic	Cannot inspect encrypted traffic	Can inspect since it runs on the endpoint
Resource Use	Dedicated appliance — no host impact	Uses host CPU and memory
Examples	Snort, Suricata, Cisco Firepower NGIPS	OSSEC, Wazuh, Carbon Black, CrowdStrike

5.6 Web Filtering

Web Filtering: A technology that restricts or controls the websites that users can access. It is used to block malicious websites, enforce acceptable use policies, and reduce bandwidth consumption.

Web Filtering Methods

- URL Filtering: Maintain a database of blocked and allowed URLs/domains — block by category (gambling, adult, malware).
- Content Filtering: Inspect the content of web pages for inappropriate or malicious material.
- DNS Filtering: Block malicious domains at the DNS resolution level (e.g., Cisco Umbrella, Cloudflare Gateway).
- SSL/TLS Inspection: Decrypt HTTPS traffic for inspection, then re-encrypt — requires certificate management.
- Application Layer Filtering: Inspect and control specific application-layer protocols and behaviors.

Web Filtering Solutions

- Cisco Umbrella: Cloud-based DNS-layer security blocking malicious domains.
- Zscaler Internet Access: Cloud-delivered web proxy and security platform.
- Palo Alto Networks: Next-generation firewall with integrated URL filtering.
- Squid Proxy: Open-source web proxy with URL filtering capabilities.

5.7 Security Incident Response Teams (SIRT/CSIRT)

CSIRT: Computer Security Incident Response Team — a group of security professionals responsible for responding to cybersecurity incidents including breaches, malware infections, and DoS attacks.

5.7.1 Incident Response Process

Phase	Name	Key Activities
Phase 1	Preparation	Develop IR plan, train team, deploy monitoring tools, establish communication channels
Phase 2	Identification	Detect and classify the incident — determine scope, affected systems, and initial impact
Phase 3	Containment	Short-term containment (isolate affected systems), long-term containment (patch/rebuild)
Phase 4	Eradication	Remove malware, close attack vectors, eliminate root cause
Phase 5	Recovery	Restore systems from clean backups, validate systems, monitor closely
Phase 6	Lessons Learned	Document findings, update IR plan, improve defenses

5.7.2 Incident Response Tools

- SIEM (Security Information and Event Management): Splunk, IBM QRadar, Microsoft Sentinel — centralized log analysis and correlation.
- EDR (Endpoint Detection and Response): CrowdStrike Falcon, Carbon Black, SentinelOne — endpoint threat detection and investigation.
- SOAR (Security Orchestration, Automation and Response): Automate repetitive IR tasks using playbooks.
- Digital Forensics: Volatility (memory forensics), Autopsy (disk forensics), FTK (Forensic Toolkit).
- Network Forensics: Wireshark, NetworkMiner, Zeek (Bro) — analyze captured network traffic.

5.8 Honeypots

Honeypot: A decoy computer system intentionally set up to attract attackers. It contains fake data and services, allowing security teams to study attacker behavior, techniques, and tools without risk to real systems.

5.8.1 Types of Honeypots

Type	Description	Use Case
Low-Interaction Honeypot	Simulates limited services and OS — easy to deploy and safe	Detect automated attacks, worms, and scanners
High-Interaction Honeypot	Full real operating system — attacker can interact deeply	Study advanced attacker TTPs (Tactics, Techniques, Procedures)
Pure Honeypot	Real production-like system with monitoring at the network level	Maximum realism for research
Honeynet	A network of multiple honeypots simulating an entire organization	Study coordinated and advanced attacks
Spam Honeypot (Spamtrap)	Email addresses used to trap spam senders	Anti-spam research, blacklisting

5.8.2 Honeypot Deployment Strategies

- Production Honeypots: Deployed within the production environment to detect internal threats and attackers who have already breached the perimeter.
- Research Honeypots: Deployed in separate networks to study attacker behavior and emerging threats without risk to production systems.
- Internal Honeypots: Detect insider threats and lateral movement after an initial breach.
- Canary Tokens: Fake files, URLs, or credentials that trigger an alert when accessed — lightweight honeypot concept.

5.8.3 Honeypot Tools

- Honeyd: Open-source tool for simulating virtual honeypot systems.
- KFSensor: Windows-based honeypot and port listener.
- Glastopf: Web application honeypot simulating vulnerable web applications.
- Dionaea: Honeypot that captures malware samples exploiting known vulnerabilities.
- T-Pot: All-in-one honeypot platform running multiple honeypot daemons in Docker containers.

5.8.4 Advantages and Limitations of Honeypots

Advantages	Limitations
Provide early warning of attacks	Can be identified by sophisticated attackers
Gather intelligence on attacker tools and techniques	Require ongoing monitoring and maintenance
Divert attacker attention from real systems	Legal implications if attacker uses honeypot to attack others
Detect new zero-day exploits	Provide no protection — purely detection-based
Low false positive rate — any activity is suspicious	Risk of being used as a launching pad if not secured

Unit V — Review Questions

52. What is an ACL? Explain the difference between a Standard ACL and an Extended ACL.
53. What is an implicit deny? Why is it important in ACL design?
54. Explain the concept of security levels in Cisco ASA. What is a DMZ?
55. Differentiate between an IDS and an IPS. What are the advantages of each?
56. Compare signature-based and anomaly-based detection methods for IDS/IPS.
57. What is Snort? What are its three modes of operation?
58. What is CSIRT? Describe the six phases of the Incident Response process.
59. Define honeypot. Distinguish between low-interaction and high-interaction honeypots.

Course Summary

This learning material has covered all five units of the Ethical Hacking course (U23CBT63). Below is a concise summary of key concepts from each unit:

Unit I — Introduction

Ethical hacking is the authorized practice of probing systems to identify vulnerabilities. Key concepts include the five phases of hacking (reconnaissance, scanning, gaining access, maintaining access, clearing tracks), types of hackers (white/black/grey hat), TCP/IP layers, IP addressing, the TCP three-way handshake, network attack categories, and malware types with corresponding defenses.

Unit II — Footprinting, Reconnaissance and Scanning

Footprinting collects information before attacking — through search engines (Google Dorking), web services (WHOIS, Shodan, Netcraft), social networks (LinkedIn, GitHub), and social engineering. Network scanning uses Nmap with various scan types (SYN, FIN, XMAS, NULL, ACK, UDP) to map attack surfaces. IDS evasion techniques include fragmentation, decoys, idle scanning, and slow scanning.

Unit III — Enumeration and Vulnerability Analysis

Enumeration actively extracts system details — user accounts, shares, services — through protocols including NetBIOS (ports 137-139), SNMP (port 161), LDAP (port 389), NTP (port 123), and SMTP (port 25). Vulnerability assessment identifies and scores weaknesses using CVSS without exploiting them. Windows (EternalBlue, RDP, NTLM), Linux (Shellshock, Dirty COW), and embedded OS vulnerabilities are critical areas.

Unit IV — System Hacking

Web server attacks include directory traversal, SSRF, and misconfiguration exploits. OWASP Top 10 vulnerabilities (SQLi, XSS, Broken Access Control) are the most critical web threats. Wireless hacking targets WEP (crackable in minutes), WPA/WPA2 (handshake attacks, PMKID), and WPA3. Tools including aircrack-ng, Burp Suite, sqlmap, Metasploit, and Mimikatz are used in web and wireless attack scenarios.

Unit V — Network Protection Systems

Network protection includes ACLs (standard/extended, implicit deny), Cisco ASA firewalls with security levels and DMZ architecture, IDS/IPS systems (signature vs anomaly-based, NIDS vs HIDS, Snort), web filtering (URL/DNS/SSL inspection), CSIRT incident response (6 phases), and honeypots (low/high interaction, honeynet) for attacker intelligence gathering.

Recommended References

60. EC-Council. (2022). Certified Ethical Hacker (CEH) v12 Course Materials. EC-Council Press.
61. Harper, A., et al. (2011). Gray Hat Hacking: The Ethical Hacker's Handbook (3rd ed.). McGraw-Hill.
62. Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The Penetration Tester's Guide. No Starch Press.
63. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing (2nd ed.). Syngress.
64. Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.
65. OWASP Foundation. OWASP Top 10. https://owasp.org/www-project-top-ten/
66. Nmap Documentation. https://nmap.org/docs.html
67. Kali Linux Documentation. https://www.kali.org/docs/
68. Snort Documentation. https://www.snort.org/documents
69. NIST Cybersecurity Framework. https://www.nist.gov/cyberframework