DHANALAKSHMI SRINIVASAN ENGINEERING COLLEGE (AUTONOMOUS)

DEPARTMENT OF
ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

III YEAR – VI SEMESTER

U23AIV31 CYBER SECURITY

QUESTION BANK ACADEMIC YEAR 2025-2026

UNITIINTRODUCTION
Cyber Security – History of Internet – Impact of Internet – CIA Triad; Reason for Cyber Crime – Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes – A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.

PART-A- 2 MARK QUESTIONS

1. What is Cyber Security?
Answer:
Cyber Security is the practice of protecting computer systems, networks, and data from unauthorized access, attacks, damage, or theft.

---

2. What is meant by the History of the Internet?
Answer:
The Internet originated from ARPANET in the late 1960s, developed by the US Department of Defense to enable secure communication between computers.

---

3. Mention any two important milestones in the history of the Internet.
Answer:
Development of ARPANET (1969)
Introduction of the World Wide Web (1991)

---

4. State any two positive impacts of the Internet.
Answer:
Fast communication through email and social media
Easy access to information and online services

---

5. Mention any two negative impacts of the Internet.
Answer:
Increase in cybercrimes
Privacy and data security issues

---

6. What is the CIA Triad in Cyber Security?
Answer:
The CIA Triad represents **Confidentiality, Integrity, and Availability**, which are the core principles of information security.

---

7. Define Confidentiality in the CIA Triad.
Answer:
Confidentiality ensures that information is accessible only to authorized users and protected from unauthorized disclosure.

---

8. What is Integrity in Cyber Security?
Answer:
Integrity ensures that data remains accurate, complete, and unaltered during storage or transmission.

---

9. Explain Availability in the CIA Triad.
Answer:
Availability ensures that information and resources are accessible to authorized users whenever required.

---

10. State any two reasons for cybercrime.
Answer:
Financial gain
Lack of awareness and weak security systems

---

11. Why is there a need for Cyber Security?
Answer:
Cyber Security is needed to protect sensitive data, prevent cyber attacks, ensure privacy, and maintain trust in digital systems.

---

12. What is meant by the History of Cyber Crime?
Answer:
Cybercrime began with early computer misuse in the 1970s and increased rapidly with the growth of the Internet and digital technologies.

---

13. Who are Cybercriminals?
Answer:
Cybercriminals are individuals or groups who use computers and networks to commit illegal activities such as hacking, fraud, and data theft.

---

14. Mention any two types of cybercriminals.
Answer:
Hackers
Cyber terrorists

---

15. What is meant by Classification of Cybercrimes?
Answer:
Cybercrimes are classified based on the target, such as crimes against individuals, organizations, or governments.

---

16. Give two examples of cybercrimes against individuals.
Answer:
Identity theft
Cyber stalking

---

17. What is meant by a global perspective on cyber crimes?
Answer:
Cyber crimes are borderless in nature and affect individuals, organizations, and governments across the world.

---

18. What are Cyber Laws?
Answer:
Cyber laws are legal frameworks designed to regulate activities on the Internet and protect users from cyber offenses.

---

19. What is the Indian Information Technology (IT) Act?

Answer:
The IT Act, 2000 is India's primary cyber law that provides legal recognition to electronic transactions and defines cybercrime offenses.

20. What is meant by Cybercrime and Punishment under the IT Act?
Answer:
The IT Act specifies penalties such as fines and imprisonment for offenses like hacking, data theft, and cyber fraud.

PART–B-16 MARK QUESTIONS

1. Explain Cyber Security in detail. Discuss its objectives and importance in the modern digital world.

---

2. Trace the history of the Internet and explain the major milestones in its development.

---

3. Discuss the impact of the Internet on society, business, and government. Mention both positive and negative effects.

---

4. Explain the CIA Triad in detail with suitable examples for Confidentiality, Integrity, and Availability.

---

5. Discuss the reasons for cybercrime and analyze why cybercrimes are increasing rapidly.

---

6. Explain the need for Cyber Security in today's Internet-based and digital environment.

---

7. Trace the history of cybercrime and explain how cyber threats have evolved over time.

---

8. Who are cybercriminals? Explain the different types of cybercriminals with examples.

---

9. Explain the classification of cybercrimes with suitable examples.

---

10. Discuss cybercrimes from a global perspective. Explain why cybercrime is considered a worldwide threat.

---

11. Explain Cyber Laws and discuss their role in controlling cybercrime.

---

12. Explain the Indian Information Technology Act, 2000. Discuss its objectives and scope.

---

13. Describe important cybercrimes and punishments under the IT Act, 2000.

---

14. Discuss the challenges in enforcing cyber laws at national and international levels.

---

15. Explain the relationship between cybercrime and punishment. Suggest measures to reduce cybercrime.

UNIT II ATTACKS AND COUNTERMEASURES

OSWAP; Malicious Attack Threats and Vulnerabilities: Scope of Cyber-Attacks – Security Breach – Types of Malicious Attacks – Malicious Software – Common Attack Vectors – Social engineering Attack – Wireless Network Attack – Web Application Attack – Attack Tools – Countermeasures

PART–A- 2 MARK QUESTIONS

1. What is OWASP?
Answer:
OWASP (Open Web Application Security Project) is a global non-profit organization that improves web application security by providing tools, standards, and documentation.

---

2. What is meant by a malicious attack?
Answer:
A malicious attack is an intentional action to damage, disrupt, or gain unauthorized access to systems or data.

---

3. Define threat in cyber security.
Answer:
A threat is a potential danger that can exploit a vulnerability and cause harm to a system or network.

---

4. What is a vulnerability?
Answer:
A vulnerability is a weakness in hardware, software, or human processes that can be exploited by attackers.

---

5. What is the scope of cyber-attacks?
Answer:
The scope of cyber-attacks includes individuals, organizations, governments, financial systems, and critical infrastructure.

---

6. What is a security breach?
Answer:
A security breach occurs when unauthorized access to confidential data or systems takes place.

---

7. Mention any two types of malicious attacks.
Answer:
Denial of Service (DoS) attack
Man-in-the-Middle attack

---

8. What is malicious software (malware)?
Answer:
Malware is software designed to harm systems, steal data, or disrupt normal operations.

---

9. Name any two types of malware.
Answer:
Virus
Ransomware

---

10. What is an attack vector?
Answer:
An attack vector is the method or pathway used by attackers to enter a system.

---

11. Give two examples of common attack vectors.
Answer:
Phishing emails
Malicious websites

---

12. What is a social engineering attack?
Answer:
A social engineering attack tricks users into revealing sensitive information by manipulating human psychology.

---

13. Give one example of social engineering.
Answer:
Phishing through fake emails or websites.

---

14. What is a wireless network attack?
Answer:
A wireless network attack targets Wi-Fi networks to intercept data or gain unauthorized access.

---

15. Name any two wireless network attacks.
Answer:
Evil Twin attack
Wi-Fi sniffing

---

16. What is a web application attack?
Answer:
A web application attack exploits vulnerabilities in web applications to steal data or disrupt services.

---

17. Name any two web application attacks.
Answer:
SQL Injection
Cross-Site Scripting (XSS)

---

18. What are attack tools?
Answer:
Attack tools are programs used to scan, exploit, or compromise systems and networks.

---

19. Name any two attack tools.
Answer:
Metasploit
Nmap

---

20. What are countermeasures?
Answer:
Countermeasures are security controls used to prevent, detect, and respond to cyber-attacks.

PART–B-16 MARK QUESTIONS

1. Explain OWASP in detail. Discuss the objectives and importance of OWASP Top 10 vulnerabilities.

---

2. Explain malicious attack threats and vulnerabilities. Discuss the scope of cyber-attacks.

3. What is a security breach? Explain its causes, consequences, and preventive measures.

4. Explain the different types of malicious attacks with suitable examples.

5. Describe malicious software (malware). Explain different types of malware and their impact on systems.

6. Explain common attack vectors used by cyber attackers with real-world examples.

7. Explain social engineering attacks in detail. Discuss types and countermeasures.

8. Explain wireless network attacks. Describe common wireless attacks and their prevention techniques.

9. Explain web application attacks with reference to OWASP vulnerabilities.

10. Explain the role of attack tools in cyber-attacks. Discuss commonly used attack tools.

11. Explain Denial of Service (DoS) and Distributed DoS attacks with suitable examples.

12. Explain Man-in-the-Middle (MITM) attacks and their countermeasures.

13. Explain phishing and spoofing attacks and methods to prevent them.

14. Discuss countermeasures used to protect systems from malicious attacks.

16. Explain the complete lifecycle of a cyber-attack, highlighting attack stages and defense mechanisms.

UNIT III RECONNAISSANCE
Harvester – Whois – Netcraft – Host – Extracting Information from DNS – Extracting Information from E-mail Servers – Social Engineering Reconnaissance; Scanning – Port Scanning – Network Scanning and Vulnerability Scanning – Scanning Methodology – Ping Sweer Techniques – Nmap Command Switches – SYN – Stealth – XMAS – NULL – IDLE – FIN Scans – Banner Grabbing and OS Finger printing Techniques

PART–A- 2 MARK QUESTIONS

1. What is The Harvester tool?
Answer:
The Harvester is an open-source reconnaissance tool used to gather emails, subdomains, IPs, and hosts from public sources.

---

2. What is WHOIS?
Answer:
WHOIS is a protocol used to obtain registration details of domain names, IP addresses, and owners.

---

3. What information can be obtained using WHOIS?
Answer:
Domain owner name, registrar details, IP address range, and registration dates.

---

4. What is Netcraft?
Answer:
Netcraft is an online service used to identify website hosting details, operating systems, and server technologies.

---

5. What is meant by host information gathering?
Answer:
Host information gathering involves identifying live systems, IP addresses, and services in a target network.

---

6. What is DNS reconnaissance?
Answer:
DNS reconnaissance is the process of extracting domain-related information such as name servers and IP mappings.

---

7. Mention any two DNS record types.
Answer:
A record
MX record

---

8. What is extracting information from email servers?
Answer:
It involves gathering email server details such as MX records, mail server IPs, and mail configurations.

---

9. What is social engineering reconnaissance?

Answer:
It is the process of collecting sensitive information by manipulating people rather than technical systems.

---

10. What is scanning in cyber security?
Answer:
Scanning is the process of identifying live hosts, open ports, and vulnerabilities in a network.

---

11. What is port scanning?
Answer:
Port scanning is the technique of checking open, closed, or filtered ports on a target system.

---

12. What is network scanning?
Answer:
Network scanning identifies active hosts and network topology within a given IP range.

---

13. What is vulnerability scanning?
Answer:
Vulnerability scanning detects known security weaknesses in systems or applications.

---

14. What is scanning methodology?
Answer:
Scanning methodology is a systematic approach to scanning that includes host discovery, port scanning, and vulnerability analysis.

---

15. What is a Ping Sweep?
Answer:
A ping sweep is a technique used to identify live hosts by sending ICMP echo requests to multiple IP addresses.

---

16. What is Nmap?
Answer:
Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing.

---

17. What is SYN scan?
Answer:
A SYN scan sends SYN packets to detect open ports without completing the TCP handshake.

---

18. What is a Stealth scan?
Answer:
A stealth scan attempts to avoid detection by firewalls and IDS while scanning ports.

---

19. What is XMAS scan?
Answer:
An XMAS scan sets FIN, PSH, and URG flags to identify open or closed ports.

---

20. What is banner grabbing?
Answer:
Banner grabbing is a technique used to collect information about services, software versions, and operating systems.

PART–B-16 MARK QUESTIONS

1. Explain information gathering (reconnaissance) in detail. Discuss tools such as The Harvester, WHOIS, and Netcraft.

2. Explain The Harvester tool. Describe its features, working, and importance in reconnaissance.

3. Explain WHOIS and Netcraft as information-gathering tools. Compare the information obtained from both.

4. Describe the process of host discovery and host information gathering in cyber attacks.

5. Explain in detail the methods of extracting information from DNS servers.

6. Explain how information is extracted from e-mail servers and discuss its security implications.

7. Explain social engineering reconnaissance. Describe different techniques used by attackers.

8. Define scanning and explain its role in the attack lifecycle.

9. Explain port scanning in detail. Discuss different port states and their significance.

10. Explain network scanning and vulnerability scanning with suitable examples.

11. Explain the scanning methodology followed by attackers with a neat diagram.

12. Explain Ping Sweep techniques and their use in identifying live hosts.

13. Explain Nmap command switches and discuss different scan types such as SYN, NULL, FIN, XMAS, IDLE, and Stealth scans.

14. Explain banner grabbing techniques and their importance in information gathering.

15. Explain OS fingerprinting techniques. Distinguish between active and passive OS fingerprinting.

UNIT IV INTRUSION DETECTION
Host -Based Intrusion Detection – Network -Based Intrusion Detection – Distributed or Hybrid Intrusion Detection – Intrusion Detection Exchange Format – Honeypots – Example System Snort.

PART–A- 2 MARK QUESTIONS

1. What is an Intrusion Detection System (IDS)?
Answer:
An IDS is a security system that monitors network or system activities to detect unauthorized access or malicious behavior.

---

2. What is Host-Based Intrusion Detection System (HIDS)?
Answer:
HIDS monitors activities on individual hosts by analyzing system logs, files, and processes.

---

3. Mention one advantage of HIDS.
Answer:
HIDS can detect insider attacks and unauthorized changes to system files.

---

4. What is Network-Based Intrusion Detection System (NIDS)?
Answer:
NIDS monitors network traffic to detect suspicious activities across the network.

---

5. Mention one limitation of NIDS.
Answer:
NIDS may fail to analyze encrypted network traffic.

---

6. What is Distributed Intrusion Detection System?
Answer:
A distributed IDS uses multiple sensors deployed across the network and hosts to collect and analyze intrusion data.

---

7. What is Hybrid Intrusion Detection System?
Answer:
A hybrid IDS combines features of both host-based and network-based IDS.

---

8. What is Intrusion Detection Exchange Format (IDEF)?
Answer:
IDEF is a standard format used to share intrusion detection information between different IDS tools.

---

9. What is the purpose of IDEF?
Answer:
IDEF enables interoperability and standardized reporting of intrusion events.

---

10. What is a honeypot?
Answer:
A honeypot is a decoy system designed to attract attackers and study their behavior.

---

11. State one objective of a honeypot.
Answer:
To detect, analyze, and gather information about cyber attacks.

---

12. What are low-interaction honeypots?
Answer:
Low-interaction honeypots simulate limited services and are easier to deploy and maintain.

---

13. What are high-interaction honeypots?
Answer:
High-interaction honeypots provide real systems for attackers to interact with, allowing deeper analysis.

---

14. What is Snort?
Answer:
Snort is an open-source network-based intrusion detection and prevention system.

---

15. What type of IDS is Snort?
Answer:
Snort is primarily a Network-Based IDS (NIDS).

---

16. Mention two features of Snort.
Answer:
Real-time traffic analysis
Signature-based detection

---

17. What is signature-based detection?
Answer:
It detects intrusions by matching network traffic against known attack signatures.

---

18. What is anomaly-based detection?
Answer:
It detects intrusions by identifying deviations from normal behavior.

---

19. What is an IDS alert?
Answer:
An IDS alert is a notification generated when suspicious or malicious activity is detected.

---

20. Give one difference between IDS and IPS.
Answer:
IDS detects attacks, while IPS detects and actively blocks attacks.

PART–B-16 MARK QUESTIONS

1. Explain Intrusion Detection Systems (IDS) in detail. Discuss their objectives and importance in network security.

---

2. Explain Host-Based Intrusion Detection Systems (HIDS) with architecture, working, advantages, and limitations.

3. Explain Network-Based Intrusion Detection Systems (NIDS) with neat diagrams and suitable examples.

4. Compare Host-Based IDS and Network-Based IDS in detail.

5. Explain Distributed Intrusion Detection Systems and discuss their advantages.

6. Explain Hybrid Intrusion Detection Systems and describe how they combine HIDS and NIDS.

7. Describe the architecture and working of a Distributed IDS.

8. Explain the Intrusion Detection Exchange Format (IDEF) and discuss its role in IDS interoperability.

9. What are honeypots? Explain their objectives, types, and benefits in intrusion detection.

10. Explain low-interaction and high-interaction honeypots with suitable examples.

11. Explain Snort as an Intrusion Detection System with its architecture and working.

12. Discuss the features and advantages of Snort in detecting network intrusions.

13. Explain signature-based and anomaly-based intrusion detection techniques with examples.

14. Discuss the role of IDS in identifying and responding to security threats in modern networks.

16. Explain the limitations and challenges of intrusion detection systems and suggest possible solutions.

UNIT V INTRUSION PREVENTION
Firewalls and Intrusion Prevention Systems: Need for Firewalls – Firewall Characteristics and Access Policy – Types of Firewalls – Firewall Basing – Firewall Location and Configurations – Intrusion Prevention Systems – Example Unified Threat Management Products.

PART–A- 2 MARK QUESTIONS

1. What is a firewall?
Answer:
A firewall is a network security device that monitors and controls incoming and outgoing traffic based on predefined security rules.

---

2. Why is a firewall needed?
Answer:
A firewall is needed to prevent unauthorized access, protect internal networks, and enforce security policies.

---

3. What is meant by firewall access policy?
Answer:
A firewall access policy defines rules that permit or deny network traffic based on IP address, port, and protocol.

---

4. Mention any two characteristics of a firewall.
Answer:
Centralized security control
Traffic filtering based on rules

---

5. What is packet filtering firewall?
Answer:
A packet filtering firewall examines packets and allows or blocks them based on source/destination IP and port numbers.

---

6. What is a stateful inspection firewall?
Answer:
A stateful firewall tracks the state of active connections and allows packets that are part of a valid session.

---

7. What is an application-level firewall?
Answer:
An application-level firewall inspects traffic at the application layer to detect malicious content.

---

8. What is a proxy firewall?
Answer:
A proxy firewall acts as an intermediary between users and external networks to filter requests and responses.

---

9. What is meant by firewall basing?
Answer:
Firewall basing refers to implementing firewall rules based on security policies, trust levels, and network zones.

---

10. What is a hardware firewall?
Answer:
A hardware firewall is a physical device used to protect a network by filtering traffic.

---

11. What is a software firewall?
Answer:
A software firewall is installed on a host system to protect individual devices.

---

12. What is firewall location?
Answer:
Firewall location refers to where the firewall is placed in the network, such as at the network perimeter or internal segments.

---

13. What is a DMZ in firewall configuration?
Answer:
A DMZ (Demilitarized Zone) is a network segment that hosts public-facing services while isolating the internal network.

---

14. What is intrusion prevention system (IPS)?
Answer:
An IPS is a security system that monitors traffic and actively blocks detected threats in real time.

---

15. How does IPS differ from IDS?
Answer:
IPS blocks malicious traffic automatically, while IDS only detects and alerts.

---

16. Mention any two types of IPS.
Answer:
Network-based IPS (NIPS)
Host-based IPS (HIPS)

---

17. What is Unified Threat Management (UTM)?
Answer:
UTM is an integrated security solution that combines firewall, IPS, antivirus, and other security features in one device.

---

18. Give two examples of UTM products.
Answer:
FortiGate
Sophos UTM

---

19. What is firewall configuration?
Answer:
Firewall configuration involves setting rules, policies, and network interfaces to control traffic flow.

---

20. State one advantage of using UTM.
Answer:
UTM simplifies security management by providing multiple security functions in a single platform.

PART–B-16 MARK QUESTIONS

1. Explain the need for firewalls in network security. Discuss the objectives and benefits of using firewalls.

2. Explain firewall characteristics in detail and discuss how they help in securing a network.

3. What is a firewall access policy? Explain the components and rule-base structure of a firewall access policy.

4. Describe the different types of firewalls with neat diagrams and suitable examples.

5. Explain packet filtering, stateful inspection, and application-level firewalls in detail.

6. Explain the concept of firewall basing. Discuss security zones and trust levels in firewall basing.

7. Discuss firewall location and configurations in a network with suitable diagrams (perimeter firewall, internal firewall, and DMZ).

8. Explain the architecture and working of a firewall with a neat block diagram.

9. What is an Intrusion Prevention System (IPS)? Explain its working and advantages over IDS.

10. Explain the types of Intrusion Prevention Systems (NIPS, HIPS, WIPS) with examples.

11. Compare firewalls and Intrusion Prevention Systems with respect to functionality, deployment, and limitations.

12. Explain Unified Threat Management (UTM) in detail. Discuss its features and advantages.

13. Describe popular UTM products and explain their security services (firewall, IPS, antivirus, VPN, web filtering).

14. Discuss the role of firewalls and IPS in preventing modern cyber attacks such as malware, DoS, and intrusion attempts.

15. Explain firewall rule management and best practices for effective network security.