DEPARTMENT OF CYBER SECURITY
U23CBT45 INTRODUCTION TO CYBER SECURITY
TWO MARKS WITH ANSWERS

UNIT 1 INTRODUCTION

1. What is Cybersecurity?

Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks, theft, or damage.

2. When did the Internet first come into existence?

The Internet first came into existence in 1969 as ARPANET, funded by the U.S. Department of Defense.

3. What does the term 'Internet' refer to?

The Internet is a global network of interconnected computers that communicate using standardized protocols.

4. What is the CIA Triad in cybersecurity?

The CIA Triad represents the core principles of cybersecurity: Confidentiality, Integrity, and Availability.

5. What does 'Confidentiality' mean in the CIA Triad?

Confidentiality ensures that information is only accessible to those authorized to view it.

6. What does 'Integrity' mean in the CIA Triad?

Integrity ensures that data remains accurate and unaltered, preventing unauthorized modifications.

7. What does 'Availability' mean in the CIA Triad?

Availability ensures that information and systems are accessible and usable when needed by authorized users.

8. What are the main reasons for cybercrime?

Common reasons for cybercrime include financial gain, personal revenge, political motives, and exploiting vulnerabilities in systems.

9. Why is cybersecurity important?

Cybersecurity is important to protect sensitive data, ensure business continuity, prevent financial loss, and defend against malicious attacks.

10. What is the history of cybercrime?

Cybercrime began in the 1980s with early computer hacking and evolved with the rise of the internet and digital transactions, leading to more sophisticated attacks.

11. Who are cybercriminals?

Cybercriminals are individuals or groups who engage in illegal activities using the internet or other digital platforms to commit crimes such as hacking, identity theft, or fraud.

12. What are the common classifications of cybercrimes?

Cybercrimes can be classified into categories such as hacking, identity theft, phishing, online fraud, cyberbullying, and cyber terrorism.

13. What is hacking in cybercrime?

Hacking involves unauthorized access to or manipulation of a computer system or network.

14. What is phishing?

Phishing is a type of cybercrime where attackers impersonate legitimate institutions to steal sensitive information like passwords and credit card details.

15. What is cyberbullying?

Cyberbullying involves using digital platforms to harass, intimidate, or harm others, especially in social media or online communication.

16. What is a global perspective on cybercrimes?

Cybercrimes have become a global issue, affecting individuals, businesses, and governments worldwide, leading to international cooperation for cybercrime prevention and law enforcement.

17. What are cyber laws?

Cyber laws are legal regulations designed to protect individuals and organizations from cybercrimes and to govern online activities.

18. What is the Indian IT Act of 2000?

The Indian IT Act of 2000 provides a legal framework for electronic governance, digital signatures, cybercrimes, and penalties related to cyber activities in India.

19. What penalties are involved in cybercrime under the Indian IT Act?

The Indian IT Act prescribes penalties such as fines, imprisonment, or both for offenses like hacking, identity theft, and cyber terrorism.

20. What is the role of law enforcement in addressing cybercrimes?

Law enforcement agencies play a crucial role in investigating, prosecuting, and preventing cybercrimes by applying relevant laws, collaborating internationally, and using advanced technology to track cybercriminals.

UNIT II - ATTACKS AND COUNTERMEASURES

1. **What is a cyber-attack?**
   A cyber-attack is a deliberate attempt to exploit computer systems, networks, or applications to steal, alter, or destroy data.

2. **What is a security breach?**
   A security breach occurs when an unauthorized entity gains access to protected data, networks, or systems.

3. **Name two types of malicious attacks.**
   - Phishing
   - Denial of Service (DoS) attack

4. **What is malware?**
   Malware is any software intentionally designed to cause damage to a system, including viruses, worms, and ransomware.

5. **List two common attack vectors.**
   - Email phishing
   - Exploiting software vulnerabilities

6. **What is a social engineering attack?**
   A social engineering attack manipulates people into divulging confidential information through deception.

7. **Give an example of a social engineering attack.**
   Phishing emails trick users into providing login credentials or financial information.

8. **What is a wireless network attack?**
   A wireless network attack targets vulnerabilities in Wi-Fi networks, such as eavesdropping on unencrypted traffic.

9. **Name two types of wireless network attacks.**
   - Evil Twin Attack
   - Man-in-the-Middle (MitM) attack

10. **What is a web application attack?**
    A web application attack exploits vulnerabilities in websites or web applications to steal data or gain unauthorized access.

11. **Give an example of a web application attack.**
    SQL Injection (SQLi) is an attack that injects malicious SQL queries to manipulate databases.

12. **What is a Denial of Service (DoS) attack?**
    A DoS attack overwhelms a system or network with excessive traffic, making it unavailable to users.

13. **What is the difference between a virus and a worm?**
- A **virus** attaches to a file and requires user action to spread.
- A **worm** is self-replicating and spreads without user intervention.

14. **What is ransomware?**
    Ransomware is malware that encrypts a victim's files and demands payment for decryption.

15. **What are botnets?**
    A botnet is a network of compromised computers (bots) controlled remotely to perform attacks like DDoS.

16. **What is an attack tool?**
    Attack tools are software programs used to exploit vulnerabilities, such as Metasploit or Wireshark.

17. **What is SQL Injection (SQLi)?**
    SQL Injection is a cyber-attack where malicious SQL code is inserted into a query to manipulate databases.

18. **What is a brute force attack?**
    A brute force attack repeatedly tries different password combinations to gain unauthorized access.

19. **Name two countermeasures to prevent cyber-attacks.**
- Implementing strong authentication mechanisms
- Regularly updating software and security patches

20. **How does a firewall protect against cyber threats?**
    A firewall monitors and filters incoming and outgoing network traffic to block malicious access.

UNIT III - RECONNAISSANCE

1. What is the purpose of the Harvester tool in cybersecurity?
The Harvester is a tool used for gathering information about a target, such as emails, domain names, and subdomains, by querying search engines, DNS records, and other public sources.

2. What is Whois used for in cybersecurity?
Whois is a protocol used to query databases to obtain information about the registration of a domain, including details like the owner, contact information, and name servers.

3. How does Netcraft help in reconnaissance?
Netcraft is a tool used for identifying web server details, detecting phishing websites, and analyzing hosting providers, helping gather information about domains and their infrastructure.

4. What is meant by 'Host' in the context of network security?
A 'host' refers to any device or computer connected to a network that has a unique IP address, allowing it to communicate within the network.

5. How can information be extracted from DNS?
Information from DNS can be extracted using tools like nslookup or dig, which provide details about domain names, IP addresses, and mail servers associated with a domain.

6. What kind of information can be extracted from email servers?
Information extracted from email servers includes server names, IP addresses, and configuration details like SMTP, IMAP, and POP3 settings, which can assist in identifying potential vulnerabilities.

7. What is Social Engineering Reconnaissance?
Social Engineering Reconnaissance involves gathering information about individuals or organizations to manipulate them into revealing confidential information, often through phishing or pretexting.

8. What is the goal of Port Scanning?
Port scanning aims to identify open ports on a target system to determine which services are running and potentially vulnerable to exploitation.

9. What is Network Scanning?
Network scanning is the process of discovering devices, systems, or services on a network by probing for active IP addresses and identifying vulnerabilities in the network infrastructure.

10. What is Vulnerability Scanning?
Vulnerability scanning is the automated process of searching for security weaknesses and vulnerabilities in systems or applications, often using specialized tools like Nessus or OpenVAS.

11. What is the scanning methodology?
Scanning methodology involves systematic approaches to scanning networks and systems, such as reconnaissance, scanning for open ports, identifying services, and assessing vulnerabilities.

12. What is Ping Sweep?
Ping Sweep is a technique used to identify live hosts within a network by sending ICMP echo requests (ping) to a range of IP addresses and recording responses.

13. What is the Nmap tool used for in network scanning?
Nmap is a network scanning tool used to discover hosts, detect open ports, and determine the services and operating systems running on those hosts.

14. What is the function of the -sP switch in Nmap?
The -sP switch in Nmap is used for a Ping Scan, where Nmap sends ICMP Echo requests to determine which hosts are up on the network.

15. What does the Nmap -O switch do?
The -O switch in Nmap enables OS detection, allowing Nmap to attempt to identify the operating system of a target host based on TCP/IP stack characteristics.

16. What is a vulnerability in the context of scanning?
A vulnerability is a weakness in a system or application that can be exploited by attackers to gain unauthorized access or cause damage.

17. What is the significance of using the -sS switch in Nmap?
The -sS switch in Nmap performs a SYN scan, which is a stealth scan that only sends SYN packets to detect open ports without completing the TCP handshake.

18. What is a SYN Scan in network scanning?
A SYN scan is a scanning technique used by Nmap that sends a SYN packet to a target port. If the port is open, it responds with a SYN-ACK, which indicates that the port is active.

19. What does a successful ping sweep indicate?
A successful ping sweep indicates which IP addresses are active or alive within a given range on the network, helping identify reachable hosts.

20. How does Nmap's -A option enhance scanning?
The -A option in Nmap enables aggressive scanning, which includes OS detection, version detection, script scanning, and traceroute for detailed information about the target system.

UNIT IV - INTRUSION DETECTION

1. What is Host-Based Intrusion Detection System (HIDS)?
HIDS is a security system that monitors and analyzes activities on a specific host or device to detect unauthorized access or malicious activity.

2. What is a Network-Based Intrusion Detection System (NIDS)?
NIDS is a security system that monitors network traffic for suspicious activities and alerts administrators of potential threats.

3. How does a Host-Based IDS differ from a Network-Based IDS?
HIDS monitors activities on a single host, such as file changes and system logs, while NIDS analyzes network traffic to detect threats across multiple devices.

4. What is a Distributed Intrusion Detection System (DIDS)?
DIDS combines multiple HIDS and NIDS components to provide a broader view of network security, enhancing threat detection across multiple systems.

5. What is a Hybrid Intrusion Detection System?
A hybrid IDS combines both host-based and network-based intrusion detection techniques to improve accuracy and reduce false positives.

6. What are the advantages of using a Hybrid IDS?
Hybrid IDS provides better detection accuracy, reduces false alarms, and offers a comprehensive security approach by monitoring both host and network activities.

7. What is the Intrusion Detection Exchange Format (IDXP)?
IDXP is a standard protocol that facilitates the exchange of intrusion detection-related information between different security systems.

8. What is the role of an Intrusion Detection Message Exchange Format (IDMEF)?
IDMEF is a format used to standardize and structure intrusion alerts, making it easier for security tools to exchange and process threat information.

9. What is a Honeypot in cybersecurity?
A honeypot is a decoy system designed to attract and detect attackers by simulating real vulnerabilities and collecting information about attack methods.

10. How do Honeypots help in intrusion detection?
Honeypots lure attackers, allowing security teams to analyze attack patterns, detect threats early, and improve overall defense strategies.

11. What are the types of Honeypots?
The two main types are low-interaction honeypots (simulate limited services) and high-interaction honeypots (fully functional systems that engage attackers for detailed analysis).

12. What is the primary goal of a Honeypot?
The main goal is to detect, analyze, and mitigate cyber threats by attracting malicious actors and studying their behavior.

13. What is Snort?
Snort is an open-source Network Intrusion Detection and Prevention System (NIDS/NIPS) that analyzes network traffic and detects malicious activities based on predefined rules.

14. How does Snort detect intrusions?
Snort uses signature-based, anomaly-based, and protocol-based detection techniques to identify potential threats in network traffic.

15. What are the different modes in which Snort can operate?
Snort operates in three modes: Sniffer Mode (captures traffic), Packet Logger Mode (logs network packets), and Intrusion Detection Mode (analyzes and detects threats).

16. What is the difference between IDS and IPS?
IDS (Intrusion Detection System) detects and alerts on threats but does not block them, whereas IPS (Intrusion Prevention System) actively blocks or mitigates attacks.

17. What are false positives and false negatives in IDS?
False positives occur when benign activity is mistakenly identified as a threat, while false negatives occur when actual threats go undetected.

18. What is anomaly-based intrusion detection?
Anomaly-based IDS detects unusual patterns in system behavior by comparing current activities against a baseline of normal behavior.

19. What are signature-based IDS rules in Snort?
Signature-based IDS rules in Snort define specific patterns of known attacks, allowing the system to detect threats based on predefined signatures.

20. How can Snort be used as an Intrusion Prevention System (IPS)?
Snort can be configured in inline mode to analyze and filter network traffic, blocking malicious packets in real-time, making it function as an IPS.

UNIT V - INTRUSION PREVENTION

1. What is the primary function of a firewall?
A firewall acts as a security barrier that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

2. Why are firewalls needed in network security?
Firewalls are needed to prevent unauthorized access, filter malicious traffic, enforce security policies, and protect internal networks from external threats.

3. What are the key characteristics of a firewall?
Firewalls filter traffic based on rules, provide logging and monitoring, support authentication, and enforce access control policies.

4. What is an access policy in a firewall?
An access policy defines rules and conditions that determine which traffic is allowed or denied through the firewall based on IP addresses, ports, and protocols.

5. What are the different types of firewalls?
The main types of firewalls include packet filtering firewalls, stateful inspection firewalls, proxy firewalls, and next-generation firewalls (NGFWs).

6. What is a packet filtering firewall?
A packet filtering firewall analyzes individual packets and allows or blocks them based on predefined rules, such as IP addresses and port numbers.

7. What is a stateful inspection firewall?
A stateful inspection firewall monitors the state and context of active connections, ensuring that only legitimate traffic is allowed based on session information.

8. What is a proxy firewall?
A proxy firewall acts as an intermediary between users and the internet, filtering traffic by inspecting application-layer data before forwarding requests.

9. What is a Next-Generation Firewall (NGFW)?
An NGFW integrates traditional firewall capabilities with advanced security features like deep packet inspection, application awareness, and intrusion prevention.

10. What is firewall basing?
Firewall basing refers to where the firewall is implemented, such as host-based firewalls (on individual devices) or network-based firewalls (protecting entire networks).

11. What are the common locations for placing firewalls in a network?
Firewalls are commonly placed at network perimeters, between internal networks, and in front of critical servers to control traffic flow and enhance security.

12. What is a Demilitarized Zone (DMZ) in firewall configuration?
A DMZ is a network segment that hosts public-facing services, such as web and email servers, providing an additional layer of protection between external and internal networks.

13. What is a dual-homed firewall?
A dual-homed firewall has two network interfaces—one connected to the internal network and the other to an external network—providing an additional security layer.

14. What is an Intrusion Prevention System (IPS)?
An IPS is a security system that detects and prevents threats by actively blocking malicious traffic in real time before it can harm the network.

15. How does an IPS differ from an IDS?
An Intrusion Detection System (IDS) detects and alerts about suspicious activity but does not take action, whereas an Intrusion Prevention System (IPS) actively blocks threats.

16. What are the types of IPS?
The main types of IPS include Network-based IPS (NIPS), Host-based IPS (HIPS), Wireless IPS (WIPS), and Content-based IPS (CIPS).

17. What are some common techniques used in IPS?
IPS uses techniques like signature-based detection, anomaly-based detection, heuristic analysis, and behavioral analysis to identify threats.

18. What is a Unified Threat Management (UTM) system?
UTM is an integrated security solution that combines multiple security functions, such as firewall, IPS, antivirus, VPN, and content filtering, into a single device.

19. What are some examples of Unified Threat Management (UTM) products?
Examples of UTM products include Fortinet FortiGate, Cisco Meraki, Sophos UTM, Palo Alto Networks, and Check Point UTM.

20. How do firewalls and IPS work together in a security architecture?
Firewalls control and filter network traffic based on rules, while IPS detects and blocks malicious traffic in real time, providing a layered security approach.