Name :- patel nandinee jatinkumar

assienment :- Ethical Hacking

1.Explain CIA triad.

Ans:-Confidentiality: Protects sensitive information.

Integrity: Ensures data is accurate and unaltered.

Availability: Keeps systems running.

2. What is a Firewall and why is it used?

Ans:- A firewall is a security system that prevents unauthorized access to a computer network. Firewalls are used to stop internet users from accessing private networks, or intranets, that are connected to the internet.

Here are some types of firewalls:

Hardware-based firewalls

These appliances act as a secure gateway between devices inside and outside a network.

Software-based firewalls

These firewalls run on a server or other device.

Next-generation firewalls (NGFWs)

These firewalls process network traffic and apply rules to block potentially dangerous traffic. NGFWs also include other network device filtering functions, such as inline application control, an integrated intrusion prevention system (IPS), and threat prevention

3. What is the difference between VA(Vulnerability Assignment) and

PT(Penetration Testing)?

Ans:-The main difference between a vulnerability assessment (VA) and penetration testing (PT) is that a VA identifies potential weaknesses, while a PT simulates a real-world attack to test the effectiveness of those weaknesses:

Vulnerability assessment

A VA uses automated tools to scan systems for known weaknesses, such as software

versions and configurations. VAs are non-intrusive, meaning they don't attempt to exploit vulnerabilities or disrupt system operations.

Penetration testing

A PT simulates a real-world attack by having ethical hackers try to exploit vulnerabilities. PTs are in-depth and potentially disruptive, and may involve temporarily taking systems offline. PTs are more expensive than VAs because they are often done manually.

4. What is the difference between HIDS and NIDS?

Ans:-The main difference between a Host-based Intrusion Detection System (HIDS) and a Network-based Intrusion Detection System (NIDS) is what they monitor:

HIDS

Monitors individual devices or hosts for suspicious activity. HIDS analyzes system logs, file integrity, and user behavior. It monitors inbound and outbound packets from the device.

NIDS

Monitors network traffic for suspicious activity. NIDS works in real-time, monitoring the packets that are going across the network

5. Explain SSL Encryption

Ans:-SSL (Secure Sockets Layer) encryption is a cryptographic protocol that protects data sent between a client and a server by scrambling the original message with two different keys:

Encryption

Uses public key cryptography to encrypt a message with a public key, which anyone can use. The intended recipient can decrypt the message with the private key, which is kept secret

6. What is Data Leakage?

Ans:-The definition of data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically.

7. What is a Brute Force Attack? How can you prevent it?

Ans:-Brute force attacks occur when a bad actor attempts a large amount of combinations on a target. These attacks frequently involve multiple attempts on account passwords with the hopes that one of them will be valid. It’s a bit like trying all of the possible combinations on a padlock, but on a much larger scale.

Passwords are not the only resource that can be brute forced: Links and directories, usernames, and emails are other common targets.

1 - Use Strong Passwords

2 - Restrict Access to Authentication URLs

3 - Limit Login Attempts

4 - Use CAPTCHAs

5 - Use Two-Factor Authentication (2FA)

8. Explain MITM attack and how to prevent it?

Ans:-A man-in-the-middle (MITM) attack is a cyberattack that allows an attacker to steal data by inserting themselves between two parties in a communication channel. MITM attacks can lead to identity theft, illegal fund transfers, and unapproved password changes.

Here are some ways to prevent MITM attacks:

Use strong passwords

Use long, unique passwords that include a combination of uppercase and lowercase letters, numbers, and special characters.

Use a VPN

A virtual private network (VPN) encrypts your online activity, making it difficult for someone to eavesdrop.

Avoid public Wi-Fi

Public Wi-Fi networks can be used to target users who aren't cyber-aware. When connecting to public Wi-Fi, use a VPN.

Use HTTPS connections

Avoid websites that don't have an HTTPS connection indicated in the address.

Use multi-factor authentication (MFA)

MFA helps prevent issues if a cybercriminal obtains credentials.

Use a certificate management system

A certificate management system can help ensure that expired SSL certificates are remediated in a centralized way.

Monitor your network

Constant monitoring can help detect and neutralize MITM attacks before they cause significant damage.

Use intrusion detection and prevention systems (IDPS)

IDPS can help detect anomalous network traffic.

9. Explain XSS attack and how to prevent it?

Ans:- Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application

To prevent XSS attacks, web APIs should implement input validation and output encoding.

10. What is a Botnet?

Ans:-A botnet is a network of computers, devices, or other internet-connected devices that are infected with malware and controlled by a single attacker. The attacker, known as the "bot-herder", can use the botnet to carry out malicious activities, such as:

Cyberattacks

Botnets can be used to launch coordinated attacks, such as distributed denial-of-service (DDoS) attacks, phishing campaigns, and account takeover.

11. Explain SSL and TLS

Ans:-Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are both communication protocols that encrypt data between devices and applications on a network:

SSL

The original protocol, developed by Netscape in 1995 to keep communication secure over

the World Wide Web. However, SSL has been compromised by several vulnerabilities.

TLS

The upgraded version of SSL, developed in 1999 by the Internet Engineering Task Force (IETF) without Netscape's involvement. TLS fixes the vulnerabilities of SSL and authenticates more efficiently.

12. Define the terms Virus, Malware, and Ransomware.

Ans:-Virus

A type of malware that replicates itself by modifying other programs and inserting its own code. Viruses can spread through infected email attachments, removable media, networks, and file sharing methods.

Malware

A general term for any software used to gain unauthorized access to a computer system, steal data, or disrupt system services. Malware can spread through emails, data installation, web surfing, and exploitation of system vulnerabilities.

Ransomware

A type of malware that encrypts a victim's data and demands payment to regain access. Ransomware can spread through phishing emails, malvertising, and exploit kits.

13. What is Phishing? Provide an example.

Ans:-Phishing is a cyberattack that uses email, websites, or text messages to trick people into giving away personal information:

Email phishing

An attacker may send an email that appears to be from a reputable organization, such as a financial institution or credit card company, and request account information.

Spear phishing

A targeted attack on a specific person or group, often using information that's relevant to the target, such as current events or financial documents.

Clone phishing

A fake email or message that looks almost identical to a legitimate one. The attacker may

impersonate the original sender and use the copycat email to trick victims.

14. Define the terms Encryption and Decryption.

Ans:-Encryption is the process of converting readable text into an unreadable form, while decryption is the process of converting the unreadable text back to its original form:

Encryption: The process of converting plain text into ciphertext, which appears to be random and meaningless.

Decryption: The process of converting ciphertext back to plaintext.

15. What is a DDoS attack and how does it work?

Ans:-Distributed Denial-of-Service (DDoS) attack is a cybercrime that overwhelms a server, website, or network resource with malicious traffic to make it inaccessible to legitimate users.

Here's how a DDoS attack works:

Malicious traffic

The attacker sends a large number of requests to the target from multiple IP addresses, often using a botnet.

Overloaded system

The target's system is overloaded with requests and can't process them all.

Inaccessible target

The target becomes inaccessible or crashes, preventing legitimate users from accessing it.

16. What is a zero-day vulnerability?

Ans:- A zero-day vulnerability is a security flaw in software or hardware that is unknown to the vendor or antivirus vendors. The term "zero-day" refers to the fact that there are zero days since a patch was released.

Zero-day vulnerabilities are considered a severe security threat because they are difficult to defend against. Attackers can exploit these vulnerabilities to gain unauthorized access to systems or steal sensitive information.

17. What is network sniffing

Ans:-Network sniffing is a technique that involves capturing and analyzing data packets

that pass through a network:

How it works

A packet sniffer, either a hardware device or software application, captures all data packets that pass through a network interface. The sniffer then decodes protocols and examines the headers and payloads for information.

Uses

Network sniffing can be used for legitimate purposes, such as troubleshooting network problems, analyzing network performance, and overseeing bandwidth consumption. However, it can also be used for malicious purposes, such as spying on other users' activities or stealing their sensitive data.

Risks

Network sniffing can expose personal information, login credentials, and other sensitive data. Attackers can use this information for identity theft, gaining unauthorized access to accounts, or committing fraudulent activities.

18. What is a Security Operations Center (SOC)?

Ans:-A Security Operations Center (SOC) is a centralized unit within an organization that monitors, detects, and responds to cyber threats. SOCs are staffed by IT security professionals who use a variety of tools and techniques to protect an organization's networks, systems, and applications.

19. What is the importance of forensics in cyber security?

Ans:- Cybersecurity forensics is important because it helps organizations respond to cyberattacks and prevent future incidents. It also helps ensure legal compliance and provides evidence for prosecution.

20.Discuss the future trends in cyber security. Which skills are important for cyber

security professionals?

Ans:-Networking and System Administration.

Security Incident Handling and Response.

Understanding of Operating Systems.

Network Security Control.

Malware Prevention and Detection.

Mastery in Coding and Encryption.

Implementation and Management of Cloud Systems.

21. What is the difference between IDS and IPS?

Ans:-The main difference between an intrusion detection system (IDS) and an intrusion prevention system (IPS) is that an IDS monitors for threats while an IPS automatically prevents them:

IDS

Monitors network traffic for suspicious activity, such as unauthorized access or policy violations, and alerts administrators. IDS doesn't directly alter network traffic.

IPS

Analyzes network traffic to identify potential threats and automatically takes action, such as blocking malicious software or vulnerability exploits. IPS operates directly in the traffic flow.