**Term 4 :- Ethical Hacking**

1. **Explain CIA triad.**

* The CIA triad refers to confidentiality, integrity and availability, describing a model designed to guide policies for information security (infosec) within an organization.

1. **What is a Firewall and why is it used?**

* Firewalls are network security systems that prevent unauthorized access to a network. It can be a hardware or software unit that filters the incoming and outgoing traffic within a private network, according to a set of rules to spot and prevent cyberattacks.

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

**PT(Penetration Testing)?**

* Understanding the difference between vulnerability assessments (VAs) and penetration testing (PT) is essential for effective cybersecurity. VAs are automated scans identifying potential weaknesses, while PT simulates real-world attacks to uncover exploitable vulnerabilities.

1. **What is the difference between HIDS and NIDS?**

* The simple answer is that HIDS protects against host-level attacks while NIDS (Network-Based Intrusion Detection System) protects against attacks to a network segment. Both intrusion systems operate by examining event and log messages generated by the system**.**

**5. Explain SSL Encryption**

* SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.

**6. What is Data Leakage?**

* The unauthorized transmission of data from an organization to any external source is known as data leakage. This data can be leaked physically or electronically via hard drives, USB devices, mobile phones, etc., and could be exposed publicly or fall into the hands of a cyber criminal.

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

* A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.

**8. Explain MITM attack and how to prevent it?**

* To prevent MITM attacks on your network, you need to: Use secure communication protocols, such as HTTPS, SSL/TLS, SSH, SFTP, and VPN. Conduct security audits to find vulnerabilities in encryption protocols. You can use tools such as sslscan, which is a fast SSL/TLS scanner.

**9. Explain XSS attack and how to prevent it?**

* Cross-site scripting (XSS) is a web security issue that sees cyber criminals execute malicious scripts on legitimate or trusted websites. In an XSS attack, an attacker uses web-pages or web applications to send malicious code and compromise users' interactions with a vulnerable application.

**10. What is a Botnet?**

* A botnet is a group of Internet-connected devices, each of which runs one or more bots. Botnets can be used to perform distributed denial-of-service attacks, steal data, send spam, and allow the attacker to access the device and its connection. The owner can control the botnet using command and control software.

**11. Explain SSL and TLS**

* SSL/TLS stands for secure sockets layer and transport layer security. It is a protocol or communication rule that allows computer systems to talk to each other on the internet safely. SSL/TLS certificates allow web browsers to identify and establish encrypted network connections to web sites using the SSL/TLS protocol.

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

* Malware is any software used to gain unauthorized access to IT systems in order to steal data, disrupt system services or damage IT networks in any way. Ransomware is a type of malware identified by specified data or systems being held captive by attackers until a form of payment or ransom is provided.

**13. What is Phishing? Provide an example.**

* In this case, an attacker attempts to obtain confidential information from the victims. Attackers use the information to steal money or to launch other attacks. A fake email from a bank asking you to click a link and verify your account details is an example of deceptive phishing.

**14. Define the terms Encryption and Decryption.**

* Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used.

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

* DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites

**16. What is a zero-day vulnerability?**

* A zero-day vulnerability is an undiscovered flaw in an application or operating system, a gap in security for which there is no defense or patch because the software maker does not know it exists—they've had “zero days” to prepare an effective response.

**17. What is network sniffing**

* Network sniffing is a process that involves capturing, examining, and observing data packets as they travel through a network. This method is frequently employed by network administrators to detect network problems, oversee bandwidth consumption, and address performance issues.

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

* A security operations center, or SOC, is a team of IT security professionals that protects the organization by monitoring, detecting, analyzing, and investigating cyber threats.

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

* Assisting in Cybercrime Investigations: Digital forensics plays a vital role in investigating cybercrimes such as hacking, identity theft, and online fraud. It can help in tracing the origin of a cyber-attack and identifying the source of a leak.

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

* Artificial Intelligence and Machine Learning Artificial intelligence and machine learning revolutionize cybersecurity. These technologies help detect threats quickly, reduce workloads, and raise the efficiency of security solutions.

**21. What is the difference between IDS and IPS?**

* An IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action. An IPS, on the other hand, takes action itself to block the attempted intrusion or otherwise remediate the incident.