***ETHICAL HACKING INTRODUCTION:-***

**1. Explain CIA triad.**

**ANS: The CIA triad is a model for information security that stands for confidentialiti integrity and availability.**

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

**ANS: A firewall is a security device that protects a network from unauthorized access by monitorinn and controlling incoming and outgoing network traffic, it acts as a barrier between a trusted internal network and an barrier between a trusted internal network and an untrusted external network data packets based on predefined security policies, use protect against cyber threats, enforce security policies, prevent data loss, safeguard system integrity, monitor traffic.**

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

**ANS: A vulnerability assessment VA identifies potenatial vulnerabilities potential in a system while a penetration test PT assesses how exploitable those vulnerbilities are.**

**PT(Penetration Testing)?**

**ANS: A pt is a manual process that simulates cyber attacks to exploit vulnerabilities in a detailed report on how serious the vulnerability provides insight into the potential consequences of a succesful attack identify weakneses in security controls is almost always a manual process user data safe from cyber attackers.**

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

**ANS: HIDS protects adainst host-level attacks while NIDS network-based intrusion detection system protects against attacks to a network segment.**

**5. Explain SSL Encryption**

**ANS: SSL secure sockets layer encryption is a protocol used to secure communication between devices over a network typically the internet though SSL itself has been a cryptographic protocol that protects data sent between a client and a server.**

**6. What is Data Leakage?**

**ANS: Data leakage refers to the unauthorized transmission or exposure of sensitive confidential or private data to unintended parties this can lead to severe consequences such as financial loss reputational damage legal penalties and loss of trust,**

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

**ANS: A brute froce attack is a methode used by attackers to again unauthorized accss to a system acount or encrypted data by systematically trying every possible combination of credentials e.g. passwords or encryption of keys until the correct one is found it is a trial-and-error approach that exploits weak or poorly secured authentication mechanisms.**

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

**ANS: A man-in-the-meddle MITM attack occurs when a malicious actor secretly intercepts and possibly alters the communication between two parties without their knowledege this type of attack can compromise sensitive data such as login credentials credit card information or confidential mesages.**

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

**ANS: cross-site scripting XSS is a type of security vulnerability found in web application it occures when an attacker injects malicious scripts into webpages viewed by other users these scripts are often written in javascript and can perform various maliicious action such as stealing control of a victim's account.**

**10. What is a Botnet?**

**ANS: A botnet is a network of compromised computers devices or servers known as bots or zombies that are controlled by a central enttity often referred to are typically infected with malware control them without the ownrs knowledge.**

**11. Explain SSL and TLS**

**ANS: SSL was the original encryption protocol devlopment by netscape in the 1990s, ssl is now considered dute to vulnerabilities, TLS is the successor to SSL introduced in 1999 with version 1.0., it is more secure and efficient than SSL fixing several flaws in the SSL protocol Although TLS is the staandard many pepol stile refer to it as SSL in casual usage.**

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

**ANS: A virus is a type of malware which is a general term for malicious software ransomware is a type of malware that encrypts a victim's until a ransom is paid.**

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

**ANS: phishing is a cyber attack that uses deceptive emails texts or phone calls to trick pepole into giving away sensitive information, a fake email from bank asking you to click a link and verify your account details.**

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

**ANS: Encryption and decryption are processes that protect infromation by converting readable data into an unreadable format and back again, Encryption is the process of converting plaintext into ciphertext using an algoritham and an encryption is to confidentialityinformation, Decryption is the revers process of encryption it invloves converting the original plaintext from using decryption key allows authorized parties.**

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

**ANS: A cybercrime that floods a website server or network with malicious traffic to make it inaccessible, botnet creation, attack execution, result.**

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

**ANS: A zero-day vulnerbility is a security flaw in a system or device that is unknown to the vendor and has no oatch available.**

**17. What is network sniffing**

**ANS: Network sniffing is the process of monitoring and capturing data packets traveling over a computer network it is typically done using software tools or hardware devices called network sniffing,a technique that monitors network traffic to capture data packets.**

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

**ANS: A security operation center SOC is a team that monitors and responds to cyber threats to an organization information system the SOC operation as a hub for maintaining the security of an orgnization IT networks devices systems and data.**

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

**ANS: cybersecurity forensics is important because it helps organization identify and respond to cyberattacks and it can help prosecurity cybercriminals.**

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

**security professionals?**

**ANS: Cybersecurity professionals need to be able to adapt to new technologies identify and manage risks and communicate effectively, they also need to be able to work well with others and responds quckly to security incidents response, network security, adaptability, risk analysis, communication, risk managememt vulnerability assessment, coding.**

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

**ANS: An intrusion detection system IDS monitors network traffic for suspicious activity and alerts administrators while an intrusion prevention system IPS monitiors and automattically prevents threats.**