**Assignment : Ethical Hacking**

1.**Explain**This is quite broad. Could you clarify what you'd like explained?

2. What is a Firewall and why is it used?  
A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

* Use:
  + Blocks unauthorized access.
  + Protects sensitive data.
  + Acts as a barrier between trusted and untrusted networks.

3. CIA Triad  
The CIA Triad stands for:

1. Confidentiality: Ensuring information is accessible only to those authorized.
2. Integrity: Ensuring information is accurate and unaltered.
3. Availability: Ensuring information and systems are accessible when needed.

4. Difference between VA (Vulnerability Assessment) and PT (Penetration Testing)

* Vulnerability Assessment: Identifies and lists potential vulnerabilities in a system. It’s passive and does not exploit vulnerabilities.
* Penetration Testing: Actively exploits vulnerabilities to determine the potential damage and assess the effectiveness of defenses.

5. Difference between HIDS and NIDS

* HIDS (Host-Based Intrusion Detection System): Monitors a specific device for suspicious activities.
* NIDS (Network-Based Intrusion Detection System): Monitors entire network traffic to detect intrusions.

6. Explain SSL Encryption  
SSL (Secure Sockets Layer) encryption secures the communication between a web browser and a server by encrypting the data exchanged, preventing unauthorized access.

7. What is Data Leakage?  
Data leakage refers to the unauthorized transmission of sensitive data outside the organization, either intentionally or accidentally.

8. 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 guess login credentials or encryption keys.

* Prevention:
  + Use strong passwords.
  + Enable account lockout mechanisms.
  + Use CAPTCHA or MFA (Multi-Factor Authentication).

9. Explain MITM attack and how to prevent it?  
A MITM (Man-in-the-Middle) attack occurs when an attacker intercepts communication between two parties to steal or manipulate data.

* Prevention:
  + Use SSL/TLS for secure communication.
  + Avoid public Wi-Fi or use VPNs.
  + Verify website certificates.

10. Explain XSS attack and how to prevent it?  
XSS (Cross-Site Scripting): An attacker injects malicious scripts into trusted websites, which execute on users’ browsers.

* Prevention:
  + Validate and sanitize user input.
  + Use Content Security Policy (CSP).
  + Escape data before rendering in the browser.

11. What is a Botnet?  
A botnet is a network of compromised devices controlled by attackers to perform malicious activities like DDoS attacks or spam campaigns.

12. Explain SSL and TLS

* SSL (Secure Sockets Layer): Outdated protocol for encrypting data.
* TLS (Transport Layer Security): Updated, more secure version of SSL.

13. Define Virus, Malware, and Ransomware

* Virus: Malicious code that attaches to files/programs and spreads when executed.
* Malware: General term for harmful software (e.g., viruses, worms, ransomware).
* Ransomware: Encrypts data and demands payment for decryption.

14. What is Phishing? Provide an example.  
Phishing is a social engineering attack where attackers trick users into providing sensitive information (e.g., fake login pages).

* Example: An email pretending to be from your bank asking for login details.

15. Define Encryption and Decryption

* Encryption: Converting data into an unreadable format to protect it.
* Decryption: Reversing encryption to make the data readable again.

16. What is a DDoS attack and how does it work?  
A DDoS (Distributed Denial of Service) attack floods a server or network with excessive traffic, making it unavailable to legitimate users.

17. What is a Zero-Day Vulnerability?  
A security flaw unknown to the vendor or public, leaving systems vulnerable to exploitation until patched.

18. What is Network Sniffing?  
Network sniffing is monitoring and capturing network packets, often used for troubleshooting or malicious purposes like stealing sensitive data.

19. What is a Security Operations Center (SOC)?  
A SOC is a centralized unit that monitors, detects, and responds to security incidents in real-time.

20. Importance of Forensics in Cybersecurity  
Digital forensics helps investigate cybercrimes by analyzing evidence like logs, files, and network activity to determine what happened and prevent future incidents.

21. Future Trends and Skills in Cybersecurity

* Trends: AI in security, zero-trust architecture, quantum cryptography.
* Skills: Ethical hacking, incident response, cloud security, and threat intelligence.

22. Difference between IDS and IPS

* IDS (Intrusion Detection System): Monitors network for malicious activity but does not take action.
* IPS (Intrusion Prevention System): Monitors and actively blocks malicious activity.

Let me know if you’d like further clarification on any of these topics!

**Module : 1 Information Gathering**

**1. What is the meaning of Cyber Security?**  
Cyber security refers to the practice of protecting systems, networks, and data from cyber threats such as hacking, malware, and unauthorized access. It ensures the confidentiality, integrity, and availability of digital assets.

**2. What are the main objectives of Cyber Security?**  
The key objectives of cyber security align with the **CIA Triad**:

1. **Confidentiality:** Protecting sensitive information from unauthorized access.
2. **Integrity:** Ensuring data accuracy and preventing unauthorized modifications.
3. **Availability:** Ensuring systems and data are accessible to authorized users when needed.

\*\*3. What is Offensive and Defensive Cyber Security?

4o

**You said:**

1 what is meaning of cyber security 2.what are the main objectives of cyber security? 3.What is offensive and defensive in cyber security? 4.what is cyberspace and low 5. What is cyber welfare? 6.Explain the Types of Hacker 7.What is the full form of SOC in cyber security 8.What are the Challenges of Cyber Security

**ChatGPT said:**

ChatGPT

Here’s a detailed explanation of each question:

**1. What is the meaning of Cyber Security?**

Cyber security is the practice of protecting computers, servers, networks, and data from unauthorized access, cyberattacks, and damage. It involves implementing measures to safeguard information, ensure privacy, and maintain functionality.

**2. What are the main objectives of Cyber Security?**

The main objectives align with the **CIA Triad**:

1. **Confidentiality:** Ensuring data is accessed only by authorized individuals.
2. **Integrity:** Ensuring that data is accurate, consistent, and unaltered.
3. **Availability:** Ensuring data and systems are accessible to authorized users whenever needed.

Additional objectives include accountability, authentication, and non-repudiation.

**3. What is Offensive and Defensive Cyber Security?**

* **Offensive Cyber Security:** Focuses on proactive measures, such as ethical hacking, penetration testing, and exploiting vulnerabilities to identify weaknesses before attackers do.
* **Defensive Cyber Security:** Focuses on protecting systems and networks by implementing firewalls, intrusion detection systems (IDS), encryption, and other security measures to defend against attacks.

**4. What is Cyberspace and Cyber Law?**

* **Cyberspace:** The virtual environment of interconnected networks where online communication, transactions, and activities occur.
* **Cyber Law:** Legal regulations and practices governing online activities, addressing issues like data protection, privacy, intellectual property, and cybercrimes.

**5. What is Cyber Welfare?**

Cyber welfare refers to efforts aimed at ensuring the safe, ethical, and inclusive use of cyberspace. It includes programs for awareness, digital literacy, and protecting vulnerable groups from cyber threats.

**6. Explain the Types of Hackers**

1. **White Hat Hackers:** Ethical hackers who use their skills to improve security systems.
2. **Black Hat Hackers:** Malicious hackers who exploit vulnerabilities for personal or financial gain.
3. **Gray Hat Hackers:** Operate in the middle, often testing systems without permission but without harmful intent.
4. **Script Kiddies:** Inexperienced individuals using pre-written tools to exploit systems.
5. **Hacktivists:** Hackers with political or social motivations.
6. **State-Sponsored Hackers:** Employed by governments to conduct cyber espionage or warfare.

**7. What is the full form of SOC in Cyber Security?**

**SOC:** **Security Operations Center**  
A centralized facility where teams monitor, detect, and respond to cybersecurity incidents in real-time.

**8. What are the Challenges of Cyber Security?**

1. **Sophisticated Cyber Threats:** Advanced techniques like AI-driven attacks.
2. **Lack of Awareness:** Insufficient knowledge among users about cyber risks.
3. **Rapid Technology Evolution:** Difficulty keeping pace with emerging technologies.
4. **Shortage of Skilled Professionals:** High demand for trained cybersecurity experts.
5. **Insider Threats:** Employees or trusted individuals causing breaches.
6. **Weak Security Policies:** Poor implementation of access controls and outdated systems.
7. **Ransomware and Phishing Attacks:** Increasingly common and costly threats.