Interview Questions - Cyber Security

1. **What is data leakage?**

   Ans: Data leakage is also known as data loss. It is the unauthorized transmission of data from within an organization to an external destination or recipient. It can occur electronically or physically. For example: Someone uploads a file to a public cloud storage bucket without realizing it contains sensitive information, or an employee lost the working laptop.

2. **What is Ransomware?**

   Ans: Ransomware is a type of malicious software that blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker(In crypto). A real-life example of ransomware is the WannaCry outbreak of 2017, which impacted various organizations and demonstrated the potential profitability of such attacks.

3. **Define a Phishing attack and how to prevent it.**

   Ans: Phishing is a type of cyber attack where scammers use fraudulent emails or messages to trick individuals into revealing sensitive information, such as passwords and credit card numbers. To prevent phishing, you should be cautious of unknown sender emails, avoid clicking on suspicious links, and use security software with anti-phishing features.

4. **What is the difference between hashing and encryption?**

   Ans: Hashing is used to check Integrity of the file, It's not reversible. Examples like MD5, SHA256. Whereas, Encryption is used for Security and confidentiality. There are two ways, symmetric and asymmetric encryption. Examples like RSA and AES.

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

   Ans: In simple terms, an Intrusion Detection System (IDS) is like a security camera that alerts you when it detects a threat, while an Intrusion Prevention System (IPS) is like a security guard that not only detects the threat but also takes action to stop it. A recent real-life example is the use of an IDS to alert a company about a potential cyber-attack, and an IPS to block the attack from reaching the company's network

6. **What is the difference between SIEM and a syslog server?**

   Ans : In simple terms, a syslog server collects and stores log messages, while a SIEM provides real-time threat analysis and response capabilities. An example of this difference in action is when a syslog server collects log data from various network devices, and a SIEM analyzes this data to detect and respond to security threats, such as a potential ransomware attack.

7. **Why is a defense-in-depth or layering approach important?**

   Ans: A defense-in-depth or layering approach is important because it uses multiple layers of security to protect against cyber threats. This means that if one layer is breached, there are additional layers that can provide protection. A recent real-life example of the importance of a layering approach is the ransomware attack on the Colonial Pipeline in 2021. The company's failure to have a robust defense-in-depth strategy in place allowed the attackers to exploit a single point of failure and disrupt the fuel supply on the East Coast of the United States.

8. **Why does an Incident Response team need playbooks?**

   Ans: An incident response team needs playbooks to provide standard procedures and steps for responding to and resolving incidents in real time. Playbooks help ensure that everyone on the team responds to incidents consistently, even in times of stress.

9. **What is the difference between an antivirus signature-based system and an EDR behavior-based system?**

   Ans: The main difference between an antivirus signature-based system and an EDR behavior-based system lies in their detection methods. Antivirus systems rely on static threat signatures and patterns to recognize known threats, while EDR systems use behavior-based monitoring to detect known or unknown threats in real time by identifying anomalous behavior at network endpoints

10. **What's the difference between Vulnerability Assessment and Penetration Test?**

    Ans: Vulnerability assessment is focused on detecting and categorizing vulnerabilities in a system, while penetration testing involves exploiting vulnerabilities to draw insights about them. Vulnerability assessment is mostly automated, while penetration testing requires manual intervention on top of automated scanning.

11. **How would you define cryptography?**

    Ans: Cryptography is the practice of hiding information to ensure that only the intended recipient can read it. It involves using mathematical concepts and algorithms to encrypt and decrypt messages, making them difficult for unauthorized parties to decipher. Example of cryptography is the use of end-to-end encryption in messaging apps like WhatsApp, which ensures that only the sender and the recipient can read the messages.

12. **What's a brute force attack, and how can it be prevented?**

    Ans: A brute force attack is a type of cyber attack that uses a trial-and-error method to guess all possible combinations of a credential. To prevent this, we can take several measures, including enforcing a strong password policy, limiting failed login attempts, implementing account lockouts, and using multi-factor authentication.

13. **What is a DDoS attack?**

    Ans: A distributed denial-of-service (DDoS) attack is a cyber-attack in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and Web sites.

14. **What is a honeypot?**

    Ans: A honeypot is a network-attached system set up to lure cyber attackers and study hacking attempts. It is designed to detect and gather information about hackers. It's one step to stay ahead of malicious actors.

15. **Explain risk, vulnerability, and threat.**

    Ans: In simple terms, a vulnerability is a weakness or gap in a system's defenses, a threat is a potential danger that could exploit a vulnerability (Hacker, Group), and risk is the likelihood that a threat will exploit a vulnerability, resulting in harm or damage. A recent real-life example is the Royal Mail falling victim to a ransomware attack, where the ransomware (threat) exploited a vulnerability in their system, resulting in the loss of international shipments (risk).

16. **Give me an example of each mechanism typically implemented for each one of the CIA principles.**

    Ans: **Confidentiality**: Confidentiality is about preventing unauthorized access to sensitive information. For instance, Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols designed to provide secure communications over a computer network.

    Integrity: Integrity ensures that data is accurate and complete, and nobody can modify it. For example, Hashing is a mechanism often used to maintain data integrity. A hash function takes an input and returns a fixed-size string of bytes. The output, known as the hash value, is unique to the unique input. Any change in the input, even a minor one, will produce a different hash value. This allows for the detection of any alteration in the data.

    Availability: Availability means that authorized users should be able to access data when needed. For example, in cloud computing, data is often stored in multiple locations to ensure its availability even if one data center experiences an outage.

17. **What do you think about SALTING a hash?**

    Ans: Salting a hash is like adding a secret ingredient to a recipe to make it more secure. In the context of password security, a "salt" is a random string that is added to a password before it's hashed. This makes it much harder for attackers to guess the original password.

18. **What is more important, a strong password or MFA (Multi-Factor Authentication)?**

    Ans: In simple terms, both a strong password and MFA (Multi-Factor Authentication) are important for protecting your online accounts. A strong password is like a sturdy lock on your front door, while MFA is like having a security guard who asks for your ID in addition to the key. Just like a strong lock and a security guard work together to keep you safe, a strong password and MFA work together to keep your accounts safe from cyber attacks.

19. **Can you explain the concept of threat intelligence and its significance in a SOC environment?**

    Ans: Threat intelligence is the process of identifying, analyzing, and understanding cyber threats. Imagine a security team learns about a new type of ransomware that is spreading quickly. With this information, they can quickly update their defenses to block the ransomware before it affects their organization. This proactive approach can save time, money, and prevent data loss.

In a Security Operations Center (SOC) environment, threat intelligence is crucial because it helps the team work more efficiently. It allows them to focus on the most important risks, which can reduce the time it takes to respond to an incident. The combination of threat intelligence and SOC can ultimately improve the overall security of the organization.

20. **How do you prioritize security incidents in a SOC, and what criteria do you use?**

    Ans: In a Security Operations Center (SOC), incidents are prioritized based on the potential impact and urgency.

    Impact: Assess the potential damage the incident could cause.

    Urgency: Determine how quickly the incident needs to be resolved.

    For example, if a SOC detects a breach in which customer data has been compromised, this would be prioritized as high impact and high urgency, requiring immediate attention. Conversely, if a low priority incident is detected, such as a routine malware alert on a less critical system, it might be addressed with less urgency.

21. **Explain the MITRE ATT&CK framework and its relevance in cybersecurity operations.**

    Ans: The MITRE ATT&CK framework is like a playbook of known tactics and techniques used by cyber attackers. It helps cybersecurity teams understand, identify, and mitigate threats more effectively.

    For instance, let's say a company experiences a ransomware attack. By referencing the MITRE ATT&CK framework, the security team can quickly identify the specific techniques used by the attackers, such as email phishing or exploiting remote services. This allows them to respond more efficiently and implement targeted defenses to prevent similar attacks in the future.

22. **What role does network traffic analysis play in identifying security threats in a SOC?**

    Ans: Network traffic analysis in a SOC involves examining the data moving across a network to identify normal and abnormal behavior. It helps in detecting security threats such as malware, unauthorized access, or data exfiltration.

    For example, suppose an organization's network traffic analysis reveals a large volume of data being sent to an unknown external server. This could indicate a potential data exfiltration attempt by an insider threat or an external attacker. By recognizing this abnormal behavior through network traffic analysis, the SOC can quickly investigate and respond to the potential threat.

23. **Describe the process of log analysis and its importance in detecting and investigating security incidents.**

    Ans: Log analysis involves reviewing and interpreting system logs to identify any abnormal or suspicious activities. This is important in detecting and investigating security incidents as it provides a detailed record of events happening within an IT environment.

For example, suppose a company experiences a data breach. By analyzing server logs, the security team may discover unusual login attempts from an unknown IP address, indicating a potential unauthorized access. This insight from log analysis allows the team to trace the source of the breach and take appropriate action to mitigate the incident.

24. **Can you discuss the concept of zero-day vulnerabilities and their impact on cybersecurity?**

    Ans: Zero-day vulnerabilities refer to security flaws that are exploited by attackers before the software or system developers are aware of them. These vulnerabilities are dangerous because there are no patches or fixes available, leaving systems at risk.

    For example, in 2021, the "PrintNightmare" vulnerability in Windows was exploited by attackers before Microsoft could release a patch. This allowed unauthorized access to systems, demonstrating the significant impact of zero-day vulnerabilities on cybersecurity, as they can lead to widespread and unexpected security breaches.

25. **How do you stay updated with the latest cybersecurity trends, threats, and technologies?**

    Ans: I follow established cybersecurity blogs such as darkreading, thehackernews.com etc, industry leaders on X(Twitter), and attend virtual / in-person security conferences to stay informed about the most recent security developments. Honestly, my best resource to stay up-to-date is X.

26. **Explain the concept of "least privilege" and its importance in access control.**

    Ans: "Least privilege" is a principle in cybersecurity that ensures individuals have only the minimum level of access needed to perform their job functions. This helps limit the potential impact of a security breach by reducing unnecessary access rights.

    For example, an employee unintentionally downloaded malware onto their system. Due to "least privilege" access control, the malware's impact was minimized because the employee did not have unnecessary access to critical systems or data.

27. **What steps would you take to secure a network against insider threats?**

    Ans:

    Access Control: Implement the principle of least privilege to limit employees' access only to necessary resources.

    Monitoring and Zero-Trust: Utilize network traffic analysis and log monitoring to detect anomalous behavior that may signal an insider threat.

    User Behavior Analytics: Use tools to analyze employee behavior, identifying any deviations from normal patterns that may indicate malicious intent. Nowadays modern SIEM solutions provide this solution. Such as SUMO logic.

    Training and Awareness: Provide regular security awareness training to employees to educate them about potential insider threats and how to report suspicious activity.