SOC ANALYST L1 INTERVIEW QUESTIONS AND ANSWERS

BY IZZMIER IZZUDDIN

QUESTIONS AND ANSWERS

1. **What is the difference between a Web Application Firewall (WAF) and an Intrusion Prevention System (IPS)?**
    - A WAF primarily protects web applications by filtering and monitoring HTTP/S traffic, focusing on threats like SQL injection and cross-site scripting. An IPS, on the other hand, protects the entire network by identifying and preventing known and unknown threats across multiple protocols. While WAF is more specialised, IPS has a broader scope.
2. **What potential risks and challenges might a company face if it relies solely on an IPS and removes its WAF?**
    - If a company removes its WAF, it becomes vulnerable to application-layer attacks such as SQL injection, XSS and OWASP Top 10 vulnerabilities. IPS solutions don't offer the granular protection needed for web applications, leading to potential data breaches and downtime.
3. **How does a firewall differ from a proxy server in terms of functionality and purpose?**
    - A firewall filters traffic based on security policies to protect the network, while a proxy server acts as an intermediary between users and the internet, mainly to hide client identities, cache content and apply user-based access controls.
4. **What is the difference between logs generated by a firewall and those generated by a proxy server?**
    - Firewall logs focus on traffic flow, blocked requests and rule enforcement. Proxy logs, on the other hand, provide details about user activities, such as websites accessed, time spent and data transferred.
5. **What are VPN records and what protocols are commonly used in VPNs?**
    - VPN records log connection details such as timestamps, user activity, IP addresses and bandwidth usage. Common VPN protocols include OpenVPN, IPsec, L2TP and PPTP.
6. **What are DNS records and what protocols are used to handle DNS operations?**
    - DNS records, like A, MX and CNAME, map domain names to IP addresses or other resources. DNS operations are handled using protocols like UDP and TCP over port 53.

7. **What is email header analysis and what key elements are examined during the analysis?**
    - Email header analysis involves examining metadata like the sender's IP address, SPF/DKIM/DMARC results and the path an email takes through servers to identify phishing, spoofing or other malicious activities.
8. **How can you verify externally whether SPF and DKIM checks have passed for an email?**
    - I use tools like MXToolBox or perform manual checks using the command line to query DNS records and validate SPF and DKIM configurations for the sender's domain.
9. **What is a Message-ID in email communication and why is it important?**
    - A Message-ID is a unique identifier for an email, crucial for tracking and differentiating messages, especially in forensic analysis.
10. **What is an Envelope-ID in email transactions and how does it differ from a Message-ID?**
    - The Envelope-ID is used during email transmission to track bounce messages and delivery status. Unlike the Message-ID, it is not visible in the email headers.
11. **Which port numbers are commonly used for VPN connections?**
    - Common VPN ports include 1194 for OpenVPN, 500 and 4500 for IPsec and 1723 for PPTP.
12. **What is normalisation in the context of log management and how does it differ from log parsing?**
    - Normalisation standardises log data into a consistent format for easier analysis, while log parsing extracts specific fields from raw logs for further processing.
13. **What are the differences between normalisation and log parsing?**
    - Log parsing focuses on breaking down raw data into usable fields, while normalisation ensures the data from different sources aligns to a common format or schema.
14. **What is the latest version of the HTTP protocol and what are its key enhancements?**

- The latest version is HTTP/3, which uses QUIC instead of TCP, offering faster performance, reduced latency and improved security.

15. **What types of logs are typically generated by a firewall?**

- Firewall logs include information on allowed or denied connections, source and destination IPs, port numbers and protocol details.

16. **What types of logs are generated by endpoint systems and how are they used in security analysis?**

- Endpoint systems generate logs like login attempts, process activity, file access and malware detections, which are vital for identifying threats and unauthorised activity.

17. **What tools and technologies are commonly used by attackers to launch DDoS attacks? Provide a real-world example.**

- Attackers use botnets, amplification tools like NTP or DNS and stress-testing software. For example, the Mirai botnet leveraged IoT devices to launch massive DDoS attacks on Dyn DNS in 2016.

18. **What are SSL and TLS and how do they ensure secure communication?**

- SSL and TLS are cryptographic protocols that encrypt data between clients and servers, ensuring confidentiality, integrity and authentication.

19. **What are the key differences between SSL and TLS?**

- TLS is the successor to SSL, offering stronger encryption algorithms, improved performance and resistance to modern attacks like BEAST and POODLE.

20. **What are the latest versions of SSL and TLS and what improvements do they bring?**

- TLS 1.3 is the latest version, providing enhanced security, reduced handshake time and deprecation of weak algorithms. SSL is obsolete and no longer used.

21. **In Splunk, what is the purpose of the eval command and how is it used in queries?**

- The eval command in Splunk is used to calculate and manipulate field values dynamically. For instance, I might use it to create new fields or apply transformations to existing ones during a search.