COLLECTION OF SCENARIO-BASED AND TECHNICAL CYBERSECURITY ANALYST INTERVIEW QUESTIONS & ANSWERS

BY IZZMIER IZZUDDIN

QUESTION (Q) & ANSWERS (A)

1. Q: Imagine it's a Saturday afternoon, and external users start having problems accessing our organization's public websites. Over the next hour, nearly every access attempt fails. What steps would you take to diagnose and mitigate this issue?

A: First, I would check the alerts from the Internet border router for any unusual activity. I'd then analyse the traffic to identify any high volumes of requests coming from a single external IP address. If all DNS requests from that address are coming from the same source port, it would indicate a potential DoS attack. To mitigate this, I would contact our Managed Security Service Provider or Website Hosting Company regarding the suspicious external IP address. I would then implement initial containment measures and monitor our internal hosts for any unusual activity. Finally, I would block the offending IP address at the firewall and notify relevant stakeholders.

2. Q: Now, suppose our network administrators detect that nine internal hosts are also attempting the same unusual requests to the DNS server. How does this change your handling of the incident?

A: This new information suggests that our internal hosts might be compromised. My immediate action would be to isolate these affected internal hosts to prevent further spread of the attack. I would then conduct a thorough investigation to check for any compromise on all internal hosts and review logs to trace the origin and extent of the compromise. Additionally, I would implement extra endpoint protection measures to secure our network.

3. Q: What measures are in place to prevent a DNS DoS attack and limit its impact?

A: To prevent and limit the impact of a DNS DoS attack, we can implement both external and internal measures. Externally, we can use multiple redundant DNS servers to handle high traffic volumes, implement rate limiting on DNS queries, and use cloud-based DNS protection services that can absorb and mitigate DoS traffic. Internally, continuous monitoring by MSSPs is crucial, along with deploying endpoint protection solutions on internal devices, maintaining and regularly reviewing firewall logs, and implementing network segmentation to limit the spread of an attack.

4. Q: It's Monday morning, and we receive a call from the Bukit Aman PDRM regarding suspicious activity involving our systems. Sensitive documents reportedly belonging to our organization have been publicly posted. How would you gather evidence to assist in the investigation?

A: To gather evidence, I would collect information from various sources, including change management logs to track recent changes, surveillance records to monitor physical access, access control logs to check who accessed the documents, and Data Loss Prevention (DLP) logs to track document exfiltration. It's important to ensure that the evidence is acquired and stored securely following best practices, with forensic evidence collected by qualified personnel and stored offline to prevent tampering.

5. Q: Now, how would the handling of this incident change if we identify an internal host responsible for the leaks?

A: If an internal host is identified as responsible for the leaks, I would immediately isolate that host to prevent further leaks. I would then conduct a forensic analysis of the host to determine the extent of the compromise and review access logs to identify the person responsible and their actions. Following the organization's incident response plan, I would notify relevant stakeholders and authorities and work on mitigating the issue.

6. Q: How would you handle the situation if a rootkit was found on the compromised internal host?

A: If a rootkit is found on the compromised internal host, I would first isolate the affected host from the network to prevent further compromise. I would then perform a thorough forensic analysis to identify the rootkit and understand its capabilities. Next, I would scan all other systems in the network for the presence of the rootkit and rebuild the compromised host from a known good backup to ensure complete removal. Finally, I would implement additional security measures such as enhanced endpoint protection and regular integrity checks to prevent future rootkit infections.

7. Q: Imagine our SIEM has detected a suspicious PowerShell script execution on a critical server. What steps would you take to investigate this incident?

A: First, I would collect initial details from the SIEM alert, including the script's command line, the user account that executed it, and the time of execution. Next, I would:

1. **Contain:** Isolate the affected server to prevent any potential spread of the threat.
2. **Analyse:** Review the PowerShell logs and the script itself to understand its purpose and actions. Check for any outbound connections or data exfiltration attempts.
3. **Investigate:** Determine how the script was executed – whether it was an insider threat, a phishing attack, or another method. Look at user activity and access logs for any anomalies.
4. **Remediate:** Depending on the findings, remove any malicious code, update system patches, and change compromised credentials.
5. **Report:** Document the incident, findings, and actions taken. Report to relevant stakeholders and consider implementing additional security measures based on the root cause.

8. Q: Can you explain the principle of least privilege and its importance in cybersecurity?

A: The principle of least privilege means granting users and systems the minimum level of access necessary to perform their tasks. Its importance in cybersecurity includes:

1. **Reduced Risk:** Minimizes the potential damage from compromised accounts or systems by limiting access.
2. **Containment:** Limits the scope of an attack, as attackers have fewer privileges to exploit.
3. **Compliance:** Helps meet regulatory requirements for access control and data protection.
4. **Accountability:** Easier to track user actions and identify the source of security incidents.
5. **Best Practices:** Encourages good security hygiene by regularly reviewing and updating access controls.

9. Q: How do you stay current with the latest cybersecurity threats and trends?

A: I stay current with the latest cybersecurity threats and trends by:

1. **Reading Industry Publications:** Regularly following blogs, journals, and news sites like Krebs on Security, Threatpost, and Dark Reading.
2. **Attending Webinars and Conferences:** Participating in cybersecurity webinars, workshops, and conferences like Black Hat and DEF CON.
3. **Engaging in Online Communities:** Active participation in forums and communities like Reddit's /r/netsec and LinkedIn groups.
4. **Continuous Learning:** Enrolling in online courses and certifications, such as those offered by SANS Institute and Coursera.
5. **Networking:** Building connections with other professionals in the field to share knowledge and insights.
6. **Threat Intelligence Feeds:** Subscribing to threat intelligence feeds and alerts from sources like the Cyber Threat Alliance and government agencies.

10. Q: Imagine you have discovered unauthorized access to a critical system. What steps would you take to handle this situation?

A: First, I would immediately isolate the affected system to prevent further unauthorized access. Then, I would:

1. **Identify and Contain:** Verify the scope of the breach and contain the incident by isolating compromised accounts and devices.
2. **Investigate:** Perform a forensic analysis to determine how the unauthorized access occurred, including reviewing logs and user activity.
3. **Eradicate:** Remove any malicious code or tools used by the intruder and close any security gaps that were exploited.
4. **Recovery:** Restore the system to a secure state from backups, ensuring no backdoors or vulnerabilities remain.
5. **Report:** Document the incident, actions taken, and findings. Report to relevant stakeholders and possibly law enforcement if necessary.
6. **Follow-Up:** Conduct a post-incident review to identify lessons learned and implement additional security measures to prevent future incidents.

11. Q: How would you handle a situation where a phishing email has successfully compromised a user's credentials?

A: Upon discovering a phishing compromise, I would:

1. **Contain:** Immediately disable the compromised user account to prevent further unauthorized access.
2. **Notify:** Inform the user and relevant IT/security teams about the compromise.
3. **Investigate:** Analyse the phishing email and determine the extent of the compromise. Check for any secondary actions taken by the attacker.
4. **Eradicate:** Remove any malware or malicious links associated with the phishing attack. Ensure that no backdoors or additional compromises exist.
5. **Recover:** Assist the user in changing their passwords and reviewing their account for any unauthorized changes.
6. **Educate:** Provide training to the user and the organization on recognizing phishing attempts and improving email security awareness.
7. **Follow-Up:** Implement additional email filtering and security measures to prevent future phishing attacks. Conduct a post-incident review to identify areas for improvement.

12. Q: Can you explain the concept of zero-trust architecture and its importance in cybersecurity?

A: Zero-trust architecture is a security model based on the principle of "never trust, always verify." It assumes that threats can exist both inside and outside the network, and therefore, no user or system should be trusted by default. Key aspects of zero-trust include:

- **Strict Access Controls:** Implementing least privilege access and verifying every access request.
- **Continuous Monitoring:** Continuously monitoring user activities and network traffic for anomalies.
- **Micro-Segmentation:** Dividing the network into smaller segments to limit lateral movement of threats.
- **Strong Authentication:** Using multi-factor authentication (MFA) to verify user identities.

Zero-trust is important because it:

- **Reduces Risk:** Minimizes the impact of a breach by limiting access and controlling the movement of threats.
- **Improves Visibility:** Provides better visibility into user activities and potential threats.
- **Enhances Compliance:** Helps meet regulatory requirements for data protection and access controls.
- **Adaptable:** Applies to various environments, including cloud, on-premises, and hybrid networks.

13. Q: What steps would you take to secure a new cloud environment being set up for our organization?

A: To secure a new cloud environment, I would:

1. **Understand Requirements:** Gather security requirements and compliance needs specific to the organization.
2. **Identity and Access Management:** Implement strong identity and access management (IAM) controls, including MFA and least privilege access.
3. **Network Security:** Set up virtual private networks (VPNs), firewalls, and network segmentation to protect cloud resources.
4. **Data Protection:** Encrypt data at rest and in transit, and implement DLP policies to prevent data loss.
5. **Monitoring and Logging:** Enable logging and monitoring to track activities and detect potential threats.
6. **Vulnerability Management:** Regularly scan for vulnerabilities and apply patches to keep systems secure.
7. **Incident Response:** Develop and test an incident response plan specific to the cloud environment.
8. **Security Best Practices:** Follow cloud provider security best practices and guidelines to ensure comprehensive security coverage.

14. Q: Your organization has recently experienced a data breach where sensitive customer information was accessed. What immediate steps would you take upon discovering the breach?

A: Upon discovering a data breach, I would take the following immediate steps:

1. **Containment:** Isolate affected systems to prevent further unauthorized access.
2. **Assessment:** Determine the scope and impact of the breach, including what data was accessed and how.
3. **Notification:** Inform senior management and relevant stakeholders, including legal and compliance teams.
4. **Investigation:** Begin a forensic investigation to understand how the breach occurred and identify the entry point.
5. **Communication:** Prepare communication for affected customers, following legal and regulatory requirements.
6. **Eradication:** Remove any malicious code or access points used by the attackers.
7. **Recovery:** Restore systems from clean backups and ensure all security patches are applied.
8. **Documentation:** Document all actions taken and findings from the investigation.
9. **Post-Incident Review:** Conduct a thorough review to identify security gaps and improve defences to prevent future breaches.

15. Q: How would you secure a wireless network in an enterprise environment?

A: To secure a wireless network in an enterprise environment, I would implement the following measures:

1. **Strong Encryption:** Use WPA3 encryption to secure wireless communications.
2. **Authentication:** Implement robust authentication mechanisms such as RADIUS with EAP-TLS for user and device authentication.
3. **Segmentation:** Segment the wireless network into different SSIDs for different purposes (e.g., guest access, internal use) and apply appropriate access controls.
4. **Network Access Control (NAC):** Use NAC solutions to ensure that only authorized and compliant devices can connect to the network.
5. **Monitoring:** Continuously monitor the wireless network for suspicious activities and unauthorized access attempts.
6. **Firmware Updates:** Regularly update the firmware of wireless access points and controllers to patch vulnerabilities.
7. **SSID Management:** Disable SSID broadcasting for non-public networks and use meaningful names that do not reveal the organization's identity.
8. **MAC Filtering:** Implement MAC address filtering to restrict access to known devices, although this should not be relied upon as the sole security measure.
9. **Physical Security:** Ensure physical security of access points to prevent tampering or unauthorized access.

16. You have been notified that a critical server has been infected with malware. How do you proceed to minimize damage and restore operations?

A: To handle a malware infection on a critical server, I would:

1. **Isolate:** Immediately isolate the infected server from the network to prevent the spread of malware.
2. **Identify:** Determine the type of malware and its behaviour through analysis of logs, network traffic, and malware characteristics.
3. **Contain:** Implement measures to contain the malware, such as blocking associated IP addresses, disabling affected services, and removing malicious files.
4. **Eradicate:** Use antivirus and anti-malware tools to remove the infection from the server. If necessary, rebuild the server from a clean backup.
5. **Recovery:** Restore any affected data from backups and verify its integrity. Ensure the server is fully patched and secure before reconnecting it to the network.
6. **Notification:** Inform relevant stakeholders about the incident and actions taken.
7. **Investigation:** Conduct a thorough investigation to identify the root cause and entry point of the malware.
8. **Preventive Measures:** Implement additional security measures, such as enhanced monitoring, user training, and updated security policies, to prevent future infections.
9. **Documentation:** Document the incident, findings, and remediation actions for future reference and compliance purposes.

17. Q: Your organization has been hit by a ransomware attack. What steps would you take to respond to and recover from this incident?

A: First, I would disconnect the affected systems from the network to prevent the ransomware from spreading further. Then, I would notify the incident response team and relevant stakeholders immediately.

Next, I would assess the type and scope of the ransomware attack, including which systems and data are affected. To contain the attack, I would implement measures such as blocking associated IP addresses and isolating compromised systems.

I would then analyse logs and network traffic to determine the attack vector and any potential persistence mechanisms. Using antivirus and anti-malware tools, I would remove the ransomware from affected systems.

For recovery, I would restore systems and data from clean backups and verify the integrity of restored data. Communication is crucial, so I would inform employees, customers, and possibly regulatory bodies about the incident, following legal and regulatory requirements.

Lastly, I would conduct a thorough post-incident review to identify gaps in security and improve defences, update security policies, and conduct training to prevent future incidents.

18. Q: How do you configure rules within a SIEM to identify potential security incidents? Provide an example.

A: To configure rules within a SIEM, I first analyse past security incidents to identify common indicators of compromise (IOCs). For example, at XYZ company, we faced an increase in sophisticated phishing attacks.

I developed SIEM rules by analysing incidents and identifying patterns such as multiple failed login attempts, logins from unregistered IP addresses, and changes in IP location. Based on this analysis, I created SIEM rules, such as triggering an alert for five login attempts within 10 minutes from the same IP and flagging logins from unusual locations or times.

I tested and refined these rules based on the results and feedback from the incident response team. As a result, the incident response team quickly identified and mitigated three phishing attacks within the first month.

19. Q: Now, describe a situation where you had to handle a zero-day vulnerability. How did you address it?

A: In one instance, a zero-day vulnerability was discovered in a widely-used software application within our organization, putting sensitive data at risk. I immediately informed the security team and senior management about the vulnerability and

conducted a risk assessment to understand which systems were affected and the potential impact.

To mitigate the risk, I implemented temporary measures such as disabling vulnerable features, applying network segmentation, and increasing monitoring for signs of exploitation. I also worked closely with the software vendor to obtain information on potential workarounds and the timeline for a patch release.

I communicated with relevant teams to ensure they were aware of the risk and actions being taken. As soon as the vendor released the patch, we applied it to fully resolve the issue. Afterward, we conducted a post-incident review to improve our response to future zero-day vulnerabilities, including enhancing our threat intelligence and monitoring capabilities.

20. Q: Explain the differences between IDS and IPS. How do they integrate into a network security architecture?

A: An Intrusion Detection System (IDS) monitors network traffic for suspicious activity and alerts administrators but does not take direct action to block threats. An Intrusion Prevention System (IPS), on the other hand, monitors network traffic and can automatically take action to block or prevent detected threats.

The main differences are:

- **Response:** IDS provides alerts for further investigation, while IPS can automatically block malicious traffic.
- **Position:** IDS is often placed outside the firewall to monitor all inbound and outbound traffic, whereas IPS is usually placed in-line within the network to actively block threats.
- **Resource Usage:** IDS typically has lower resource requirements since it only monitors and logs traffic, while IPS requires more resources to inspect and potentially block traffic in real-time.

In terms of integration, IDS and IPS are deployed at strategic points within the network, such as between the internal network and the internet, to monitor critical traffic flows. Both systems are managed through centralized consoles, which provide visibility and control over detected threats and blocked traffic. IDS and IPS can be integrated with other security tools, such as SIEM systems, to provide a comprehensive view of the organization's security posture and facilitate coordinated responses to incidents. Regularly updating IDS/IPS signatures and policies ensures they can detect and block the latest threats.

21. Q: We have received reports of a suspected phishing attack targeting our employees. A few staff members have reported receiving suspicious emails asking for their login credentials. As a cybersecurity analyst, how would you handle this situation?

A: First, I would follow a structured approach to handle this phishing attack:

1. **Initial Assessment**:
    - I would immediately verify the legitimacy of the reported emails. This involves analysing the email headers, checking for any suspicious links or attachments, and reviewing the sender's information.
    - I would gather all reported instances and look for common indicators of compromise (IoCs).
2. **Containment**:
    - I would notify the IT department to block any malicious domains or IP addresses associated with the phishing emails.
    - I would also recommend temporarily disabling any affected accounts to prevent further unauthorized access.
3. **Communication**:
    - I would inform all employees about the phishing attempt, providing them with guidance on identifying such emails and advising them not to interact with suspicious messages.
    - I would set up a dedicated communication channel for employees to report any similar incidents.
4. **Investigation**:
    - I would conduct a thorough analysis of the phishing emails, including examining the email content, sender's address, and any embedded links or attachments.
    - I would check logs and monitoring systems for any signs of compromised accounts or unusual activities related to the phishing emails.
5. **Remediation**:
    - If any accounts were compromised, I would initiate password resets and ensure multi-factor authentication (MFA) is enabled for all users.
    - I would work with the IT team to implement additional email filtering rules to block similar phishing attempts in the future.
6. **Reporting**:
    - I would document the entire incident, including the timeline, actions taken, and the outcome. This report would be shared with relevant stakeholders and used to improve future incident response plans.
7. **Training and Awareness**:
    - Finally, I would organize training sessions for employees to educate them about phishing attacks, how to recognize them, and what to do if they encounter suspicious emails.

22. Q: During your investigation, you find a suspicious link in the email. How would you analyse it to determine if it's malicious?

A: To analyse the suspicious link, I would take the following steps:

1. **URL Inspection**:
    - I would examine the URL structure to look for any obvious signs of phishing, such as misspelled domain names or unusual subdomains.
    - I would use URL inspection tools, such as VirusTotal or URLScan, to check the reputation of the link.

2. **Sandbox Analysis**:
    - I would use a sandbox environment to safely open the link and observe its behaviour. This helps in understanding if the link leads to a malicious website or triggers any downloads.
3. **Checking Redirects**:
    - I would follow any redirects associated with the URL to see where it ultimately leads and check if those destinations are flagged as malicious.
4. **Content Analysis**:
    - If the link points to a webpage, I would analyse the content of the page for signs of phishing, such as login forms asking for sensitive information.
    - I would also look at the source code of the webpage for any hidden malicious scripts.
5. **Network Traffic Monitoring**:
    - While analysing the link in a controlled environment, I would monitor the network traffic to see if it attempts to communicate with any known malicious IP addresses or domains.
6. **Collaboration with Threat Intelligence**:
    - I would check threat intelligence feeds and databases to see if the URL has been reported as malicious by other organizations or security researchers.

23. Q: If the investigation confirms that several employees have already submitted their credentials through this phishing link, what immediate actions would you take?

A: If credentials have been compromised, I would take the following immediate actions:

1. **Account Lockdown**:
    - I would immediately disable the affected accounts to prevent unauthorized access and further damage.
2. **Password Reset**:
    - I would initiate a password reset process for the compromised accounts, ensuring new passwords are strong and unique.
    - I would also recommend resetting passwords for other accounts using similar credentials as a precaution.
3. **Multi-Factor Authentication (MFA)**:
    - I would ensure that MFA is enabled for all user accounts, adding an extra layer of security.
4. **Forensic Analysis**:
    - I would conduct a forensic analysis of the affected accounts to determine the extent of the compromise and any unauthorized activities.
5. **Notify Stakeholders**:
    - I would inform the affected employees and relevant stakeholders about the compromise, providing them with steps to secure their accounts and any additional actions they need to take.
6. **Update Security Measures**:
    - I would review and enhance our email filtering and security policies to prevent similar incidents in the future.

    - I would also update our incident response plan based on lessons learned from this incident.
7. **Communication and Training**:
    - I would communicate the incident to all employees, emphasizing the importance of vigilance against phishing attacks.
    - I would organize additional training sessions to reinforce best practices for identifying and reporting phishing emails.

24. Q: In the event of a malware outbreak, I would follow a structured approach to contain and mitigate the threat:

A: Immediate Containment:

- **Isolation**: I would immediately isolate infected systems from the network to prevent further spread of the malware. This could involve disconnecting systems from the network, disabling network interfaces, or segmenting the affected part of the network.
- **Blocking Communication**: I would update firewall rules and intrusion prevention systems (IPS) to block any known malicious IP addresses, domains, or command-and-control (C2) servers that the malware is using to communicate.

Identification and Analysis:

- **Malware Identification**: I would use anti-malware tools and threat intelligence feeds to identify the type of malware and understand its behaviour, propagation methods, and potential impact.
- **Log Analysis**: I would analyse logs from various sources (e.g., network traffic, endpoint security, system logs) to trace the malware's origin and determine the extent of the infection.

Eradication:

- **Scanning and Cleaning**: I would run comprehensive malware scans on all infected and potentially infected systems using up-to-date anti-malware software. I would also use specialized tools to remove the malware.
- **Patching and Updates**: I would ensure all systems are patched and updated to close any vulnerabilities that the malware may have exploited.

Recovery:

- **Restoration**: I would restore systems from clean backups where necessary, ensuring the backups are free from malware.
- **System Hardening**: I would implement additional security measures, such as enabling endpoint protection, application whitelisting, and network segmentation, to prevent future infections.

Communication:

- **Incident Notification**: I would inform relevant stakeholders, including IT teams, management, and affected users, about the malware outbreak, the steps being taken to address it, and any actions they need to take.
- **User Guidance**: I would provide guidance to users on recognizing malware symptoms and reporting any suspicious activity.

Post-Incident Review:

- **Root Cause Analysis**: I would conduct a thorough review to determine how the malware entered the network and identify any security gaps.
- **Lessons Learned**: I would document the incident, including the response actions and lessons learned, to improve future incident response efforts.

Training and Awareness:

- **User Education**: I would organize training sessions to educate users about malware threats, safe computing practices, and how to avoid falling victim to malware attacks.
- **Security Awareness Programs**: I would enhance ongoing security awareness programs to keep users informed about emerging threats and best practices.

25. Q: During the containment phase, you discover that the malware is using encrypted communications to a remote server. How would you approach decrypting and analysing this traffic?

A: Analysing encrypted malware communications can be challenging, but I would take the following steps:

1. **Traffic Capture**:
    - **Packet Capture**: I would capture network traffic using tools like Wireshark or tcpdump to gather data on the encrypted communications.
    - **Network Monitoring**: I would use network monitoring tools to identify patterns and anomalies in the traffic that could provide clues about the malware's behaviour.
2. **Decryption Efforts**:
    - **SSL/TLS Inspection**: If the communication uses SSL/TLS, I would implement SSL/TLS inspection on the network perimeter devices, such as firewalls or proxy servers, to decrypt and inspect the traffic.
    - **Certificate Analysis**: I would analyse the SSL/TLS certificates used by the malware to identify any patterns or known malicious certificates.
3. **Behavioural Analysis**:
    - **Sandboxing**: I would run the malware in a controlled sandbox environment to observe its behaviour and capture the decrypted communication for analysis.
    - **Endpoint Forensics**: I would perform forensic analysis on infected endpoints to identify any decryption keys or mechanisms used by the malware.

4. **Threat Intelligence**:
    - **External Resources**: I would consult threat intelligence feeds and databases to see if the malware's encryption methods and C2 servers have been documented by other researchers.
    - **Collaboration**: I would collaborate with other security analysts and organizations to share information and gather insights on decrypting the malware's communications.
5. **Custom Tools and Scripts**:
    - **Developing Tools**: If necessary, I would develop or use custom tools and scripts to attempt to decrypt the malware's traffic, leveraging any known weaknesses in the encryption implementation.
6. **Reporting and Mitigation**:
    - **Document Findings**: I would document all findings from the decryption and analysis process, including any indicators of compromise (IoCs) and insights into the malware's behaviour.
    - **Mitigation Steps**: Based on the analysis, I would implement additional mitigation steps, such as blocking specific IP addresses, domains, or signatures identified during the analysis.