ODUNSI IFEOLUWA PRAISE

ifeoluwapraiseodunsi@gmail.com

Cybersecurity / Network Defense Trainee Test (Internship)

1. Phishing Email

- First of all, I'll check the email headers and sender domain for any signs of impersonation or spoofing.
- I'll also check for social engineering red flags in the mail such as a sense of urgency or poor spellings.
- Then I'll inspect the link URL for the true destination without clicking on it.
- If the employee has interacted with the link, I'll immediately isolate their device from the network to prevent further compromise.
- I'll instruct the user to use the report phishing button to ensure the email is captured for analysis.
- I'll escalate the incident details to the Security Incident Response Team(SIRT).
- I'll perform a search across the organization's email environment to see if other employees received the same message.
- I'll block the malicious domain and URL at the email gateway and firewall.
- I'll verify if any credentials were entered and force a password reset if a compromise is suspected.
- Finally, I'll document the incident to improve future detection and provide feedback to the employee.

2. Malware Infection

- My immediate action would be to isolate the infected computer from the network to contain the malware's spread.
- I would document all observed symptoms, the discovery timeline, and the user's initial actions for a formal incident report.
- I'd then check running processes and system logs to identify the specific malicious executable or script.
- I would reboot the machine into Safe Mode with Networking to conduct remediation in a more controlled environment.
- I would perform a comprehensive scan using up-to-date, enterprise-grade anti-malware and antivirus tools.
- I would quarantine and delete all malicious files found, including associated registry entries.
- If necessary, I would utilize specialized removal tools for persistent threats like rootkits that evade standard removal.
- I'd verify the system's integrity by checking for any modified system files and restoring them to their clean state.
- I would ensure the operating system and all applications are fully patched and updated to close any potential entry points.
- I would force a password reset for the affected user and any administrative accounts that accessed the system.
- I would restore essential user data from a known clean backup to guarantee the data's integrity and complete malware eradication.
- Finally, I would review and enhance endpoint security controls and ensure the user receives mandatory security awareness training.

3. Ransomware attack

- My immediate and critical step would be to isolate the affected server and any directly connected network segments to halt the encryption process.
- I would then notify the incident response team and senior management immediately following the communication plan.
- I would work to determine the initial point of compromise and the specific type of ransomware that has been deployed.
- I would preserve system state, memory dumps, and logs for forensic analysis before attempting any remediation.
- I would verify the integrity and age of all system and file backups to ensure a clean restoration is possible.
- I would refuse to pay the ransom, as there is no guarantee of file recovery and it encourages further criminal activity.
- I would provision a clean, secure environment where recovery from the verified clean backups can take place.
- I would eradicate the infection source and immediately patch the vulnerability that was exploited.
- I would implement stronger access controls, network segmentation, and multi-factor authentication (MFA) to prevent recurrence.
- I would report the incident to relevant law enforcement and regulatory bodies as required by law.

4. Unauthorized Access Attempt

- I would immediately verify the foreign IP address to confirm if it is a known threat or a legitimate, but mistaken, connection.

- I would analyze the Intrusion Detection System (IDS) logs to understand the attack pattern, targeted accounts, and the number of attempts.
- I would review the targeted user accounts for any signs of compromise or subtle malicious activity, even if the logins failed.
- I would block the foreign IP address at the perimeter firewall or the IDS to immediately stop any further brute-force attempts.
- I would force a strong password reset for all targeted user accounts, especially if the attack was persistent.
- I would immediately enable multi-factor authentication (MFA) for all user accounts, especially privileged ones, if not already active.
- I would verify that there are no unnecessary open ports or services exposed externally that could be targeted.
- I would fine-tune the IDS rules and thresholds to improve detection and alerting for future brute-force or dictionary attacks.
- I would implement an account lockout policy to temporarily disable accounts after a small, predefined number of failed attempts.
- I would monitor the network for any new or related activity from the blocked IP range or other foreign sources.
- I would document the entire incident, including logs and mitigation steps, for future security policy review.

5. Data Breach Suspicion

- My first priority is to verify the client's report by locating the confidential files on the public forum they mentioned.
- I would identify the specific type, sensitivity, and volume of the data exposed to assess the full scope and impact of the breach.

- I would contain the breach by immediately revoking access to the compromised system or data source and patching the exploit.
- I would perform an in-depth forensic analysis to precisely determine the method, time, and scope of the data exfiltration.
- I would notify the legal and compliance teams to ensure all regulatory obligations for data breach reporting are met.
- Internally, I would only inform senior management and the incident response team, providing confirmed facts only.
- I would prepare a clear, honest, and legally reviewed external communication statement for the public.
- Externally, I would notify all affected clients and regulatory bodies without undue delay, as required by law.
- I would actively work with the public forum administrator or host to secure the immediate removal of the confidential files.
- I would implement enhanced Data Loss Prevention (DLP) controls and stricter access policies to safeguard the data source.
- I would review and enhance employee security awareness training focused on handling and protecting sensitive client data.
- I would document all findings, actions, and communications for the mandatory post-incident review and audit.

6. Web Application Vulnerability

- I would perform an authenticated and unauthenticated Dynamic Application Security Testing (DAST) scan using professional tools like Burp Suite or OWASP ZAP.
- I would specifically check for all OWASP Top 10 vulnerabilities, with a high priority on Injection Flaws (like SQLi) and Broken Authentication.

- I would review the application's source code for security flaws using a Static Application Security Testing (SAST) tool.
- I would assess the security of all user input fields for Cross-Site Scripting (XSS) and other injection techniques.
- I would examine the session management mechanisms for proper token generation, validity, and secure destruction.
- I would check the configuration of the web server and database for security hardening best practices and default settings.
- I would review all third-party components (e.g., plugins, modules) for known Common Vulnerabilities and Exposures (CVEs).
- I would test all APIs and endpoints for insecure direct object references (IDOR) and unnecessary data exposure.
- I would verify that all data transmission uses secure protocols, like HTTPS, with an HSTS policy enabled.
- I would use tools like Nmap or SSL Labs to check for unnecessary open ports on the hosting server and TLS configuration.
- I would check for proper error handling to prevent the leakage of sensitive system information in error messages.
- I would review the application's logging to ensure all security-relevant events are correctly recorded for auditing.

7. Network Compromise

- I would use a Network Monitoring Tool (NMT) and an Intrusion Detection System (IDS) to confirm the suspicious communication and its destination IP.
- I would specifically examine network flow data (NetFlow/sFlow) to identify the volume and exact nature of the communication.

- I would deploy an Endpoint Detection and Response (EDR) agent on the affected device to analyze active processes and network connections.
- My immediate priority is to isolate the compromised device from the network, either virtually via a host-based firewall or physically by unplugging the cable.
- I would then capture a memory dump and a disk image of the device for detailed forensic analysis using a tool like FTK Imager.
- I would scan the device using multiple trusted antivirus and anti-malware tools in an offline or isolated environment for full remediation.
- I would identify the persistence mechanism used by the malware and remove it to prevent re-infection upon reboot.
- I would determine the initial compromise vector (e.g., phishing link, unpatched vulnerability) to close the security gap.
- I would deploy the latest operating system and application patches on the device after the clean-up and before it is reconnected.
- I would force a password reset for the user and check for any unauthorized account creation or privilege escalation.
- I would monitor the network closely for similar communication patterns post-remediation to confirm complete threat elimination.
- I would update the company's security awareness training to include information on the specific exploit method used.

8. Risk Management & AI Security

- I would initiate the risk assessment by clearly identifying all the AI assistant's assets, including the training data, the model, and all input/output channels.

- I would determine the potential threats to the system, such as adversarial attacks, data poisoning, and unauthorized function calls.
- I would analyze the vulnerabilities in the AI model's architecture, its dependent libraries, and the deployment environment.
- I would assess the potential business impact of a compromise, including the risk of data leakage, reputational damage, and inaccurate outputs.
- I would focus on evaluating the assistant's ability to resist manipulation techniques like "prompt injection."
- I would define a set of technical and procedural controls to mitigate risks, such as strict input validation and output filtering.
- I would specifically test for data leakage, ensuring the assistant cannot be tricked into revealing its proprietary training data.
- I would establish clear accountability for the AI system's actions, errors, and any security incidents that may occur.
- I would mandate ongoing monitoring, regular security audits, and re-assessments as the model and its use cases evolve.
- Prompt Injection means an attacker crafts a malicious input, or a prompt, designed to override the AI model's original, intended system instructions.
- The primary goal of prompt injection is to make the AI perform unauthorized actions, such as revealing confidential information or generating harmful content.
- This is a key security concern because it exploits the nature of large language models to follow instructions, even when those instructions are malicious and conflict with the system's security rules.

9. Security Checklist Exercise

- Input Validation and Sanitization: To prevent common injection flaws like SQLi and XSS by strictly validating and encoding all user input.
- Authentication and Session Management: To ensure strong password requirements, proper session token security and timely session invalidation.
- Secure Configuration Management: To verify that all default settings, unnecessary services, and open ports are disabled on the server and application.
- Access Control (Authorization): To strictly enforce the principle of least privilege, ensuring users can only access the data and functions they are explicitly authorized for.
- Secure Error Handling and Logging: To prevent the disclosure of sensitive system information in error messages and to ensure all security-relevant events are logged for monitoring and auditing.

I would choose to test Input Validation and Sanitization for Cross-Site Scripting (XSS) vulnerabilities:

- My testing process would begin by identifying all user input fields, including URL parameters, search boxes, and form fields.
- I would inject non-persistent XSS payloads like <script>alert('XSS')</script> into these fields and submit them.
- I would then observe if the script executes in the browser, which would confirm a vulnerability exists in the input validation or output encoding.

- To test for persistent XSS, I would save a malicious payload, such as in a profile description or comment section, and check if it executes for other users viewing that content.
- A successful execution of any payload would trigger an immediate bug report for the development team to fix the flaw before the application goes live.

10. Current Affairs in Cybersecurity

a. Kevin Mitnick

- Former American hacker who became a "white hat" security consultant, author, and speaker.
- Famous for his highly publicized hacking exploits in the 80s and 90s, leading to a five-year prison sentence.

b. Eugene Kaspersky

- Russian cybersecurity expert and co-founder/CEO of Kaspersky Lab.
- Known for leading one of the world's largest anti-virus and threat intelligence companies.

c. Linus Torvalds

- Finnish-American software engineer.
- Best known as the creator of the Linux kernel and the distributed version control system Git.

d. Bruce Schneier

- Internationally renowned American cryptographer and computer security specialist.
- Known for his extensive writings on cryptography and security, including the essential book *Applied Cryptography.*

e. Parisa Tabriz

- American computer security expert, best known for her role at Google.
- Served as the Director of Engineering for the Chrome security team, often referred to as Google's "Security Princess."