#Task One:

#

#Part 1: Cybersecurity Scenario (30 points)

#Objective: Assess the candidate's understanding of security operations, cyber defense, threat intelligence, and incident response.

#Scenario: You are a security analyst at a financial company. Recently, your organization experienced a security breach. The attack vector was an unpatched vulnerability in a web application that allowed attackers to gain unauthorized access to the network.

1. Threat Intelligence Report

Types of Attacks

- SQL Injection: Malicious SQL statements are inserted into an entry field for execution.
- Cross-Site Scripting (XSS): Attackers inject malicious scripts into content from otherwise trusted websites.
- Remote Code Execution (RCE): Attackers execute arbitrary code on a target machine or in a target process.
- Directory Traversal: Attackers access directories and execute commands outside of the web server’s root directory.
- Zero-Day Exploits: Attackers exploit vulnerabilities that are not yet known to the software developers.

Exploitation of Vulnerability

A vulnerability in a web application can be exploited to gain access to the network in several ways:

1. Initial Access: The attacker identifies and exploits a vulnerability in the web application, such as an unpatched SQL injection flaw, to gain initial access.
2. Privilege Escalation: Once inside, the attacker may use privilege escalation techniques to gain higher-level access, and strategic actions to reduce the chances of being detected.
3. Lateral Movement: The attacker moves laterally across the network, exploiting other vulnerabilities or using stolen credentials.
4. Data Exfiltration: Sensitive data is extracted from the network.
5. Persistence: The attacker establishes backdoors or other mechanisms to maintain access over time.

Preventive Measures

- Regular Patching and Updates: Ensure all software, especially web applications, are regularly updated with the latest security patches.
- Vulnerability Management: Implement a robust vulnerability management program that includes regular scanning and remediation.
- Web Application Firewalls (WAFs): Deploy WAFs to protect against common web exploits.
- Security Awareness Training: Train employees to recognize phishing and other social engineering attacks that could lead to initial access.

- Access Control: Implement strong access controls and ensure least privilege principles are followed.
- Multi-Factor Authentication (MFA): Enforce MFA for all critical systems and applications.

2. Incident Response Plan

Incident Response Plan Outline

Preparation:
- Develop and maintain an incident response policy.
- Train the incident response team on their roles and responsibilities.
- Conduct regular incident response drills.

Identification:
- Detect the breach through logs, IDS/IPS alerts, or anomaly detection systems.
- Validate the breach by cross-referencing alerts with threat intelligence feeds.

Containment:
- Short-term: Isolate affected systems to prevent further spread.
- Long-term: Identify and mitigate the root cause of the vulnerability.

Eradication:
- Remove the attacker's presence from the network by eliminating backdoors and malicious software.
- Patch the exploited vulnerability.
- Conduct a thorough scan to ensure no traces of the attacker remain.

Recovery:
- Restore affected systems from clean backups.
- Monitor systems closely for any signs of residual malicious activity.
- Reconnect systems to the network after ensuring they are secure.

Lessons Learned:
- Conduct a post-incident review to identify what went wrong and how to prevent future incidents.
- Update the incident response plan based on the lessons learned.

3. Network Security Measures

Recommended Security Measures

1. Intrusion Detection and Prevention Systems (IDS/IPS):
   - Deploy IDS/IPS to monitor and analyze network traffic for suspicious activity.
   - Example tools: Snort (open-source), Suricata (open-source).

2. Network Segmentation:

- Segment the network into different zones to contain and limit the spread of an attack.
- Use VLANs and subnetting to create isolated segments.

3. Firewalls:
   - Implement both perimeter and internal firewalls to control incoming and outgoing traffic.
   - Ensure proper firewall rules are in place to block unauthorized access.

4. Multi-Cloud Forensic Analysis:
   - Use tools like CloudMapper and Prowler for mapping and auditing cloud environments.
   - Implement Pulumi for infrastructure as code to ensure consistent and secure cloud deployments.
   - Leverage cloud-native security services such as Azure Defender and AWS Security Hub for continuous monitoring and threat detection.

5. Endpoint Detection and Response (EDR):
   - Deploy EDR solutions to monitor endpoint activities and detect malicious behavior.
   - Example tools: CrowdStrike, SentinelOne.

6. Security Information and Event Management (SIEM):
   - Implement a SIEM system to aggregate and analyze logs from various sources.
   - Use the SIEM for real-time alerting, correlation of events, and historical analysis.
   - Example tools: Splunk, ELK Stack (Elasticsearch, Logstash, Kibana).

7. Runtime Application Self-Protection (RASP) and Cloud Native Application Protection Platform (CNAPP):
   - Deploy RASP tools to monitor and protect applications during runtime by detecting and blocking malicious behavior in real time.
   - Example RASP tools: Contrast Security Protect, Waratek, Imperva (Prevoty) RASP.
   - Utilize CNAPP tools like Prisma Cloud and Dynatrace with Runtime Protection features to close zero-day security gaps and protect against exploits in operational and production environments.

8. Data Loss Prevention (DLP), Managed Detection and Response (MDR), Cloud Security Posture Management (CSPM), and Active Threat Protection:
   - Implement DLP solutions to monitor and protect sensitive data from unauthorized access or transfer.
   - Example DLP tools: Symantec DLP, McAfee Total Protection for Data Loss Prevention.
   - Use MDR services to provide continuous threat monitoring, detection, and response capabilities.
   - Example MDR services: CrowdStrike Falcon Complete, Rapid7 Managed Detection and Response.
   - Employ CSPM tools to continuously assess and manage cloud security posture.
   - Example CSPM tools: Prisma Cloud, AWS Security Hub.

- Deploy Active Threat Protection to monitor for, detect, and respond to active threats in real time.
- Example tools: Microsoft Defender ATP, FireEye Endpoint Security.

9. Application Security Posture Management (ASPM):
   - Use open-source ASPM tools like Archery to focus on signal versus noise in DevSecOps scanning environments.
   - Reduce the burden of noise by identifying and prioritizing actual threats based on duplicative vulnerabilities.

10. Cybersecurity Mesh Architecture (CSMA):
   - Implement CSMA to create a scalable and flexible security framework that integrates various security tools and technologies.
   - Example: DeepWatch Open Security Architecture, which leverages SIEM, SOAR, cloud logs, EDR, MDR, CSPM, and other tools to provide comprehensive threat detection, or other custom developed similar aggregate threat detection, management and response system.

11. Continuous Monitoring, Continuous Compliance, Continuous Risk Management and Continuous Control Attestation:
   - Establish continuous monitoring to detect and respond to threats in real-time.
   - Implement continuous control attestation to ensure ongoing compliance with security policies and standards.
   - Utilize AI-powered continuous risk management tools that combine and leverage data from SIEM, SOAR, cloud logs, EDR, MDR, CSPM, IDS/IPS, DLP, and other sources.
   - Automate compliance and control with tools that integrate and correlate data, such as custom scripts using Boto3 and terraform and cloud formation, aws config, aws inspector, aws auditor or pulumi governance as code for AWS inventories, Pulumi for cloud deployments (Policy and Governance as code), and other automation tools for on-premise and on-device endpoint protection.

By incorporating these comprehensive measures, the financial organization can significantly enhance its security posture, effectively respond to incidents, and protect sensitive information from various threats, ensuring a robust defense against potential breaches and exploits.