# **Part 1: Cybersecurity Scenario**

Tasks

## **1: Threat Intelligence Report**

## **List the types of attack that could be use**

Answer:

* For Unpatched vulnerability in a web application, different types of attack could be use. For general possibility, here are the some of the attacks
  + Cross-site scripting
  + Cross-site request forgery
  + SQL and command injection
  + Path traversal
* For web server vulnerability, it can have
  + Insecure server configuration

Assumptions:

I am assuming that the application code done by developers are basically scanned using some SAST solutions like Synk, which will help find the vulnerabilities in SAST even before the code are merged in the main branch. So, mostly in production world, we will find unpatched vulnerability mostly on server configuration, which needs to be periodically checked and analyzed. For my remaining Tasks I am going to talk about threat due to Insecure server configuration.

## **Explain how a vulnerability exploited can provide access to the network.**

Answer:

* With Insecure server configuration, it can provide the network address of the server(s) which can be used to exploit the network. With the visibility of the network address, Attackers can scan for open ports and services to find potential entry points. They can also exploit weak access controls to gain unauthorized access to sensitive data or critical systems. This vulnerability can be used to detect disabled security features or improper firewall rules.

## **Suggest preventive measures to avoid similar incidents in the future.**

Answer:

* To prevent similar incidents, first of all we need to establish and maintain baseline configurations for all systems and applications. Regularly apply security patches and updates to all the software applications associated with this web applications. We will also need to perform regular audit and review server configurations to ensure compliance with security best practices. We will need to conduct regular vulnerabilities scans to identify and address outdated software and misconfigurations.
* On top of above server-based settings, for Cloud based security, we can implement AWS Security Hub. AWS security hub can integrate with AWS GuardDuty, Amazon Inspector and AWS WAF which will help to detect web vulnerabilities. We can certainly configure AWS WAF rules to monitor the web applications, and can send the findings as well as logs to Security HUB through CloudWatch integration. Some of the time, we can certainly write custom actions to automate responses to remediate vulnerabilities via Lambda using CloudWatch.

## **2. Incident Response Plan**

## **Outline an incident response plan to address the breach**

## **Include steps for containment, eradication and recovery**

Answer:

* Incident response plan is outlined below

1. Preparation:
   * Incident Response Team: Cybersecurity Division
   * Communication Plan: Use secure channels for internal communication (via encrypted email)
   * Tools and Resources:
     1. AWS Security Config, CloudWatch, IDS/IPS
     2. Documentation: Incident response playbook
2. Identification:
   * Detection:
     1. CloudWatch and AWS security Config detected and alerted for faulty server config which was showing the internal network address of the server.
   * Verification:
     1. Cybersecurity team were able to review the logs, alerts and initial forensic analysis to confirm the vulnerabilities being exposed.
     2. Cybersecurity team were also able to identify the affected systems and potential impact.
   * Containment:
     1. Cybersecurity team were able to isolate the affected systems and disconnected from the network without any affect to the application being deployed.
   * Eradication:
     1. Cybersecurity team were able to analyze the systems and determined the patch was not updated on the affected systems.
     2. Cybersecurity team also verified the autoscaling systems and verified the session token was not draining properly which caused the system still linger in the network.
   * Elimination:
     1. Cybersecurity team applied the security patches and updates to fix the vulnerabilities.
     2. Cybersecurity team ensured the security settings and configurations were correct.
   * Recovery:
     1. Cybersecurity teams conducted the tests to ensure the systems are functioning correctly and securely.
     2. Cybersecurity teams worked with deployment team, and implemented better blue-green-canary deployment plans and testing for autoscaling to kick in correctly for new deployments.
     3. Updated WAF configuration to not expose the network information for our future issues.
   * Monitoring:
     1. Cybersecurity teams intensively monitored the restored systems for any signs of vulnerability for next 24 hours.
   * Lesson Learned:
     1. Created the detailed report, how certain systems did not get the certain patches and server configuration updates, which increased the threat to the systems. In the report, Cybersecurity mentioned the what happened, how it was handled and how we can improve the automation process for our patch management.
     2. Update our testing our deployment methodology to verify our blue-green-canary deployment strategy and make improvements for this type of vulnerability not being exposed.
     3. Re-Analyze our WAF configuration to verify for any extra actions/rules we can put to hide the vulnerabilities on our web applications.
   * Contact information:
     1. Incident response coordinator: [jane.doe@example.com](mailto:jane.doe@example.com)

## **3. Network Security Measures**

## **Recommend network security measures to enhance the organizations defense posture.**

## **Include at least three different security technologies or practices (e.g.: IDS/IPS, firewalls, network segmentation)**

Answer:

* I would like to assume we have two different factors to improve to enhance the organizations defense posture.

1. Technical Changes
   1. Firewalls
      1. Deploying next generation firewalls to monitor and control incoming as well as outgoing network traffic based on the different set of rules.
      2. Implementing DMZ zones for those systems, which needs to be accessed from outside.
      3. Implementing firewall rules to block unauthorized access.
      4. Better log management from firewalls to SIEM devices.
   2. IDS/IPS:
      1. Using IDS to monitor the network traffic for any suspicious activity.
      2. Using IPS to actively block detected threats in real-time.
   3. Network Segmentation:
      1. Implement VPCs and private subnets to create systems with better Network access control list (NACL) to access the subnets. This will help limiting the spread of malware and reduce attach surface.
      2. Ensure VPNs use strong encryption protocols.
   4. Authentication:
      1. Use new micro-tunneling VPNs like Zscaler to securely connect users to organization network based on RBAC.
      2. Implement MFA for all critical systems.
   5. Server Configuration Management:
      1. Make sure to disable unnecessary services and ports in firewall, servers etc.
      2. Ensure systems are regularly audited and patched with secured configuration.
      3. Prioritize critical security patches and updates.
2. Policies and Practices:
   1. Security Policies:
      1. Develop, enforce and audit the security policies covering the business functionality of the company, access controls and data protection. Update the policy as new technology emerges based on the requirements.
   2. User Training:
      1. Implement user training for employees for them to understand and educate the security policies based on their role.
   3. Incident Response Plan:
      1. Develop and maintain an incident response plan to ensure a swift and effective response to security incidents.
   4. Access Controls:
      1. Periodically review and audit the access controls, and implement usage of Least Privilege Access control methods.
      2. Implement Single sign on strategy with RBAC to manage user permissions.
   5. Cloud Policies:
      1. Implement cloud policy as code, to automate secured policies to each and every deployment. Automate using different tools like Terraform, CloudFormation etc.