**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

| **Summary** | The scenario consists of a multimedia company, Idealt with a DDoS attack that crippled your network for two hours. The attack, caused by a flood of ICMP packets, halted network services and blocked internal traffic. The incident management team mitigated the attack by blocking incoming ICMP packets, shutting down non-essential services, and restoring critical ones. An investigation revealed that the attacker exploited an unconfigured firewall to launch the ICMP flood. | | |
| --- | --- | --- | --- |
| Identify | In this scenario, the attack was a distributed denial of service (DDoS) attack. This kind of attack overwhelms a network or website by sending a massive amount of traffic from various sources, rendering it inaccessible to users. | | |
| Protect | Given the scenario, here are some systems or procedures that can be improved to enhance the security of the organization's assets:  Conducting regular audits of internal networks, systems, devices, and access privileges can help identify potential security gaps and address them proactively before they can be exploited.  Deploying network monitoring software can identify unusual traffic patterns quickly, enhancing the detection of potential security incidents. Establishing security training and awareness programs can educate employees on the significance of security and offer guidelines for the secure use of networks and devices, reducing the risk of incidents due to human error.  The firewall configuration can be reviewed and updated to block all incoming ICMP packets and prevent the possibility of DDoS attacks in the future. Also, the firewall can be configured to check for spoofed IP addresses on incoming ICMP packets, which will help mitigate the possibility of malicious traffic.  By making these changes, the organization can bolster its security posture and lower the chances of similar incidents in the future. | | |
| Detect | Security teams have various methods to monitor and analyze network traffic, applications, track user access, and detect unusual activities. Here are a few examples:  Network Monitoring: Using tools like firewalls, IDS/IPS, and NTA, security teams can detect and analyze traffic, identify suspicious behaviors, and prevent unauthorized access.  Application Monitoring: APM tools allow security teams to monitor applications for vulnerabilities and malicious activities, addressing issues attackers might exploit.  User Activity Monitoring: UAM solutions help track user activities, detect anomalies, and alert security teams to potential threats.  Identity and Access Management (IAM): IAM tools manage user access, enforce security policies, and provide visibility into user activities.  Security Information and Event Management (SIEM): SIEM tools collect, analyze, and correlate security events, helping detect incidents, investigate them, and provide real-time alerts.  Implementing these techniques enables security teams to protect their assets, detect incidents, and respond effectively to threats. | | |
| Respond | **Containing Cybersecurity Incidents and Affected Devices**:   * Isolate compromised devices from the network to stop the attack's spread. * Shut down impacted services or applications to prevent further harm. * Deploy firewalls and access control lists to block traffic from malicious sources. * Change passwords and revoke access for compromised user accounts.   **Neutralizing Cybersecurity Incidents**:   * Use intrusion prevention and detection systems to spot and block attacks. * Perform forensic analysis on affected systems to find the incident's root cause. * Patch vulnerabilities and update security controls to prevent future incidents. * Collaborate with law enforcement to trace and apprehend attackers.   **Analyzing the Incident**:   * Review network logs and traffic data to trace the attacker's source and patterns. * Examine system logs for unusual activity on affected devices. * Analyze configuration data to identify weaknesses in security controls. * Collect reports from employees who observed suspicious behavior before the incident.   **Improving Recovery Processes**:   * Develop and test incident response plans to clarify roles and responsibilities. * Implement backup and recovery procedures to ensure quick data restoration. * Create communication plans for employees, customers, and stakeholders during incidents. * Conduct regular security awareness training to keep employees informed about the latest threats and responses. | | |
| Recover | To help the organization bounce back from the cybersecurity incident, follow these steps:  **Identify the affected systems**: Pinpoint which systems were hit by the attack to prioritize recovery efforts.  **Isolate affected systems**: Once identified, separate these systems from the network to prevent further damage.  **Assess the damage**: Evaluate the extent of the damage and identify compromised data.  **Restore data from backups**: Recover lost or corrupted data from clean backups, ensuring they are malware-free.  **Apply security updates**: After restoring systems, apply all security patches and updates to guard against future attacks.  **Educate employees**: Inform employees about the incident and preventive measures to avoid future occurrences.  For immediate recovery, maintain up-to-date backups of all critical data to enable quick restoration without data loss or ransom payments.  The organization should maintain a documented incident response plan that outlines steps during a security incident, regularly reviewed and updated as needed. This plan should detail the roles and responsibilities of key personnel and third-party support services.  Additionally, a disaster recovery plan should be in place, detailing steps to restore critical systems, recover data, and resume business operations in the event of a major incident. | | |

| Reflections/Notes: |
| --- |