**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** | A distributed denial-of-service (DDoS) attack targeted a multimedia company that provides web design, graphic design, and social media marketing solutions. The attack overwhelmed the network with ICMP packets, causing an internal network outage for two hours. The company’s incident management team quickly responded by blocking incoming ICMP packets and restoring critical network services. After investigation, it was determined that an unconfigured firewall allowed the attack. The organization implemented various security measures, including new firewall rules and an intrusion detection/prevention system (IDS/IPS). |
| Identify | The DDoS attack exploited a vulnerability caused by an unconfigured firewall, highlighting the need for continuous risk identification. Moving forward, the organization should focus on:   * Regular audits of network configurations and firewall settings. * Identifying vulnerable services such as ICMP that can be targeted by DDoS attacks. * Ensuring that all network services and devices are regularly reviewed for potential weaknesses. * Maintaining an up-to-date inventory of all network assets and their associated vulnerabilities. |
| Protect | The lack of proper firewall configuration exposed the network to an ICMP flood attack. To prevent such incidents in the future, the following protection measures were implemented:   * Firewall Configuration: Implementing a firewall rule to limit the rate of incoming ICMP packets reduces the likelihood of the network being overwhelmed. * IP Address Verification: By checking for spoofed IP addresses, the firewall can better filter out malicious traffic. * Training and Awareness: Ensuring that employees responsible for managing firewalls and network infrastructure understand the importance of secure configurations. * Network Segmentation: Isolating critical services from public-facing services could protect vital systems during a similar attack. |
| Detect | The DDoS attack went undetected until the network was overwhelmed. This suggests a lack of proper monitoring or alerting mechanisms for abnormal traffic patterns. To enhance detection:   * IDS/IPS Implementation: An intrusion detection/prevention system (IDS/IPS) can filter out ICMP traffic based on suspicious characteristics, providing an early warning of potential attacks. * SIEM Implementation: Implementing a Security Information and Event Management system software to continuously monitor network traffic logs for anomalous patterns/trends and alert of potential threats before they escalate. |
| Respond | The incident management team’s response involved blocking incoming ICMP packets and shutting down non-critical network services to stop the attack. Moving forward:   * **Playbook**: The organization could develop or update its playbook to ensure a quick and coordinated response to DDoS attacks and other cyber incidents. |
| Recover | After stopping the DDoS attack, the company restored its critical network services and implemented security improvements to mitigate future incidents. Recovery actions should include:   * **System Restoration**: Ensuring that all network services return to normal functionality after the attack, with a focus on minimizing downtime. * **Data QA Checks**: Verifying that no data was corrupted or lost during the attack. * **Backup and Redundancy**: Having proper backups and redundancy systems can help reduce recovery times in future incidents. |

|  |
| --- |
| Reflections/Notes: This DDoS incident exposed gaps in the company’s firewall configuration and network monitoring processes. By applying the NIST CSF, the company can improve its ability to identify, protect, detect, respond, and recover from such incidents. Moving forward, continuous auditing, enhanced monitoring, and a robust incident response plan will help mitigate future cybersecurity threats. |