**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 multimedia company's network experienced a Distributed Denial of Service (DDoS) attack that involved a flood of ICMP packets. The attack caused the internal network services to become unresponsive for two hours. The incident was mitigated by blocking incoming ICMP packets, shutting down non-critical network services, and restoring critical services. Investigation revealed that the attack exploited an unconfigured firewall, allowing the attacker to overwhelm the network. Subsequent measures included new firewall rules, source IP address verification, network monitoring software, and an IDS/IPS system. |
| Identify | **Network and System Audits:** Conduct regular audits to assess the configuration of firewalls and other network devices. Ensure that all network infrastructure is correctly configured to prevent exploitation.  **Access Privileges:** Regularly review and update access privileges to ensure that only authorized personnel have access to critical network configurations and systems.  **Risk Assessment:** Perform risk assessments to identify potential vulnerabilities that could be exploited by attackers, such as unconfigured devices or inadequate traffic management policies.  **Actions Taken:**  Identified that the firewall was unconfigured, leading to the vulnerability exploited during the attack. |
| Protect | **Firewall Configuration:** Implement and regularly update firewall rules to limit the rate of incoming ICMP packets and other potential attack vectors.  **IP Verification:** Set up source IP address verification to prevent spoofed IP addresses from being used to overwhelm the network.  **Policies and Procedures:** Develop and enforce policies for network security, including best practices for configuring and maintaining network infrastructure.  **Employee Training:** Provide training for IT staff on network security best practices and response procedures.  **Actions Taken:**  - Applied a new firewall rule to limit ICMP traffic.  - Enabled source IP address verification on the firewall.  - Implemented network monitoring software and IDS/IPS systems. |
| Detect | **Monitoring Tools:** Utilize network monitoring tools to detect unusual traffic patterns and potential signs of a DDoS attack.  **Intrusion Detection Systems (IDS):** Deploy IDS/IPS systems to identify and respond to abnormal network activity and suspicious traffic.  **Incident Alerts:** Set up automated alerts for abnormal traffic spikes or unusual patterns that may indicate an ongoing attack.  **Actions Taken:**  - Installed network monitoring software to identify abnormal traffic patterns.  - Integrated an IDS/IPS system to filter out suspicious ICMP traffic. |
| Respond | **Incident Response Plan:** Develop and refine an incident response plan to ensure quick and effective responses to network attacks.  **Containment and Mitigation:** Execute containment strategies to limit the impact of the attack, such as blocking malicious traffic and shutting down non-critical services.  **Post-Incident Analysis:** Conduct a thorough analysis of the incident to understand the attack vectors and improve future responses.  **Actions Taken:**  - Blocked incoming ICMP packets to stop the attack.  - Took non-critical network services offline to preserve critical services.  - Restored network services and investigated the source of the attack. |
| Recover | **Restoration of Services:** Restore affected network services and systems to normal operation as quickly as possible.  **Data Integrity Checks:** Verify the integrity of data and systems that may have been affected by the attack.  **Improvement and Adaptation:** Update security measures and incident response procedures based on lessons learned from the incident.  **Actions Taken:**  - Restored critical network services.  - Implemented improvements to firewall rules and network monitoring to prevent future attacks. |

|  |
| --- |
| Reflections/Notes: -   * Regularly reviewing and updating firewall configurations is crucial to maintaining network security. * Implementing comprehensive network monitoring and IDS/IPS systems enhances the ability to detect and respond to attacks promptly. * Continuous training and updating of security policies and incident response plans are essential for adapting to new threats and improving overall security posture. |