**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 cybersecurity incident involved a distributed denial of service (DDoS) attack on the organization's network, resulting in a disruption of services for two hours. The attack was initiated through an unconfigured firewall, allowing the attacker to flood the network with ICMP packets. The incident management team responded by blocking incoming ICMP packets, taking non-critical network services offline, and restoring critical services. The cybersecurity team investigated the event and implemented several measures to address the security vulnerabilities, including new firewall rules, source IP address verification, network monitoring software, and an IDS/IPS system. |
| Identify | Regular audits of internal networks, systems, devices, and access privileges should be conducted to identify potential security gaps. In this incident, the lack of proper firewall configuration allowed the attacker to exploit the network. Additionally, a thorough review of network traffic patterns and logs might have revealed abnormal activities prior to the attack. |
| Protect | To protect internal assets, policies and procedures should be established for configuring and maintaining firewalls and other security devices. Proper training should be provided to network administrators to ensure they are aware of best practices for network security. Implementing tools such as intrusion detection and prevention systems can help mitigate cybersecurity threats by identifying and blocking malicious activities in real-time. |
| Detect | Improving monitoring capabilities is crucial for detecting potential security incidents promptly. Network monitoring software should be deployed to detect abnormal traffic patterns and alert security teams to potential threats. Additionally, setting up alerts and notifications within the IDS/IPS system can help in identifying suspicious ICMP traffic and other anomalous behavior. |
| Respond | In the event of a security incident, it's essential to have a well-defined response plan in place. The incident management team should be trained to respond quickly to contain and neutralize threats. In this scenario, the response involved blocking incoming ICMP packets, taking non-critical network services offline, and restoring critical services. Implementing improvements to the security process based on lessons learned from the incident is also crucial to prevent similar attacks in the future. |
| Recover | After the incident is contained, efforts should focus on recovering affected systems to normal operation. This may involve restoring systems data and assets that have been compromised or affected by the incident. Additionally, conducting a post-incident analysis can help identify areas for improvement and enhance the organization's overall cybersecurity posture. |

|  |
| --- |
| * Reflections/Notes: Regular security audits and vulnerability assessments are essential for identifying and addressing potential security risks before they are exploited by attackers. * Training and awareness programs should be ongoing to ensure all employees understand their roles and responsibilities in maintaining network security. * Continuous monitoring and timely incident response are key components of an effective cybersecurity strategy. * Learning from past incidents and implementing necessary changes can help strengthen the organization's resilience against future cyber threats. |