**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** | On July 3rd, the organization experienced a Distributed Denial of Service (DDoS) attack targeting its internal network systems. The attack consisted of a flood of ICMP packets that overwhelmed network services and caused a total disruption for approximately two hours. The attack exploited a misconfigured firewall that did not adequately restrict ICMP traffic. The cybersecurity incident response team successfully mitigated the attack by blocking ICMP traffic, shutting down non-critical services, and restoring critical systems. Subsequent investigation identified the root cause, and new preventive measures were implemented to avoid recurrence. | | |
| --- | --- | --- | --- |
| Identify | The security team conducted an audit of the internal network, firewall configuration, and access policies. It was determined that the attacker exploited an unconfigured firewall that allowed unrestricted ICMP traffic. The organization's internal business services and communication systems were rendered inoperable during the incident, affecting employees who rely on uninterrupted network access to perform their work. | | |
| Protect | Following the incident, the organization implemented new firewall rules to rate-limit ICMP traffic and verify the source IP of incoming packets. Policies were updated to include mandatory configuration checks for all network-facing devices. Employee training will be enhanced to raise awareness of network-based threats. Protective technologies such as updated firewalls and access control policies have been established to mitigate similar risks in the future. | | |
| Detect | To improve detection capabilities, network monitoring software was deployed to identify anomalous traffic patterns in real time. An Intrusion Detection and Prevention System (IDS/IPS) has been implemented to scan for and respond to suspicious ICMP traffic. These tools provide visibility into future attacks and enable quicker identification and response to potential threats. | | |
| Respond | During the attack, the team blocked incoming ICMP packets and shut down non-essential services to contain the threat. Communications were coordinated internally to inform affected employees and stakeholders. A root cause analysis was conducted, and the lessons learned were documented. Procedures have been updated to ensure faster incident response in future DDoS scenarios. | | |
| Recover | All critical network services were restored progressively following the containment of the attack. Business operations resumed after two hours of downtime. A review of recovery procedures has been conducted, and improvements were implemented to ensure full network resilience, including regular system backups and documented restoration protocols. | | |

| Reflections/Notes: This incident emphasized the need for rigorous firewall configuration, proactive monitoring, and comprehensive response planning. By aligning with the NIST CSF, the organization has strengthened its cybersecurity posture and enhanced its capacity to manage similar incidents in the future. |
| --- |