**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 company faced a security incident where network services abruptly stopped responding. The cybersecurity team determined that a distributed denial of service (DDoS) attack, caused by a flood of ICMP packets, was responsible for the disruption. To mitigate the issue, the team blocked the attack and paused all non-critical network services, allowing them to prioritize the restoration of critical services. |
| Identify | A threat actor flooded the company with ICMP packets. Their services were affected resulting into a 2 hour compromise. There is need for restorage and security updates. |
| Protect | The cybersecurity team implemented a new firewall with rules to limit the rate of incoming ICMP packets and a IDS/IPS system. |
| Detect | The cybersecurity team configured source IP address verification on firewall to check for IP spoofing. |
| Respond | For future events, the team will isolate any affected systems. They will attempt to restore the critical services affected. After that, the team will analyze and record the incident. |
| Recover | To recover from an ICMP flood DDoS attack and restore network services to normal operation, begin by blocking external ICMP flood attacks at the firewall. Then, stop all non-critical network services to minimize internal network traffic. Prioritize the restoration of critical network services first. Once the ICMP packet flood has subsided, gradually bring non-critical network systems and services back online. |

|  |
| --- |
| Reflections/Notes: |