**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or just to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to continue practicing applying the NIST CSF framework to different situations you may encounter.

|  |  |
| --- | --- |
| **Summary** | The company faced a security incident when all network services became unresponsive due to a DDoS attack caused by a flood of ICMP packets. The cybersecurity team blocked the attack and halted non-critical services to restore essential ones. |
| Identify | An unsub malicious actor or actors exposed the companies vulnerabilities with an ICMP flood attack. The entire internal network became affected. All critical network resources needed to be secured and restored to a baseline functioning state. |
| Protect | The cybersecurity team implemented a new firewall rule to limit the amount of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics that we recently experienced. |
| Detect | The cybersecurity team set up source IP address verification on the firewall to block spoofed IP addresses and deployed network monitoring software to detect abnormal traffic patterns. |
| Respond | In future security events, the cybersecurity team will isolate affected systems, restore critical services, analyze network logs for suspicious activity, and report incidents to upper management and legal authorities if necessary. |
| Recover | To recover from an ICMP flood DDoS attack, network services must be restored to a normal state. Future ICMP flood DDoS attacks can be blocked at the firewall. Next non-critical services should be stopped to reduce internal traffic, while critical services are prioritized for restoration. Once the ICMP flood attack has ended, non-critical services can be brought back online. |

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