**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** | A DDoS attack overwhelmed the servers by flooding it with many ICMP packets. This caused the internal network being compromised, and critical services stopped working. This alerted the cybersecurity team to investigate and resolve the issue. By investigating further, it was known to the team that the DDoS attack is occurring; hence, the team responded by blocking the ICMP packets receiving and restarting all critical services. Then, they updated firewall rules to prevent this type of attack in the future, and set an IDS/IPS system alongside a network monitoring software to better detect such attacks in the future. | | |
| --- | --- | --- | --- |
| Identify | The servers were overwhelmed by an attack that caused the internal network being compromised. The cybersecurity team stepped in by investigating the cause of overwhelm. The cause was found to be a decentralized ICMP flooding, a subcategory of DDoS attacks. | | |
| Protect | To address this security event, the network security team implemented:   * A new firewall rule to limit the rate of incoming ICMP packets * Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets * Network monitoring software to detect abnormal traffic patterns * An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics | | |
| Detect | To detect better for future, the team has launched an IDS/IPS system alongside network monitoring system. | | |
| Respond | The team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. | | |
| Recover | The only thing needed to be recovered was the critical network services that were restored right after all non-critical services stopped. | | |

| Reflections/Notes: |
| --- |