**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 encountered a security incident when all network services abruptly ceased functioning. The cybersecurity team discovered that the disruption resulted from a distributed denial of service (DDoS) attack, manifesting as an influx of incoming ICMP packets. In response, the team blocked the attack and halted all non-essential network services to restore critical network functionality. |
| Identify | A malicious actor or group targeted the company with an ICMP flood attack, impacting the entire internal network. It was essential to secure and restore all critical network resources to ensure they returned to a functional state. |
| Protect | The cybersecurity team established a new firewall rule to restrict the rate of incoming ICMP packets and deployed an IDS/IPS system to filter specific ICMP traffic based on identified suspicious characteristics. |
| Detect | The cybersecurity team configured the firewall to verify source IP addresses, ensuring protection against spoofed IP addresses in incoming ICMP packets. Additionally, they implemented network monitoring software to identify and detect abnormal traffic patterns. |
| Respond | For future security incidents, the cybersecurity team plans to isolate affected systems to prevent additional disruption to the network. They will work to restore any critical systems and services impacted by the event. Following this, the team will analyze network logs to identify any suspicious or abnormal activity. Additionally, all incidents will be reported to upper management and relevant legal authorities, if necessary. |
| Recover | To recover from a DDoS attack caused by ICMP flooding, it is essential to restore access to network services to a normal operational state. Moving forward, external ICMP flood attacks can be blocked at the firewall. Following this, all non-essential network services should be halted to minimize internal network traffic. Next, critical network services should be prioritized for restoration. Finally, once the influx of ICMP packets has subsided, all non-critical network systems and services can be reactivated. |

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