**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 issue when all network services suddenly stopped working. The cybersecurity team discovered that this disruption was due to a distributed denial of service (DDoS) attack, which flooded the network with a large number of incoming ICMP packets. In response, the team took action by blocking the attack and temporarily halting non-essential network services. This allowed them to focus on restoring critical network services to normal operation. | | |
| --- | --- | --- | --- |
| Identify | A harmful actor or group targeted the company with an ICMP flood attack, impacting the entire internal network. To address this, the team had to secure and restore all critical network resources to their normal functioning state. | | |
| Protect | The cybersecurity team took action by introducing a new firewall rule to control the rate of incoming ICMP packets. Additionally, they implemented an Intrusion Detection System/Intrusion Prevention System (IDS/IPS) to filter out certain ICMP traffic that exhibited suspicious characteristics. | | |
| Detect | The cybersecurity team enhanced security measures by setting up source IP address verification on the firewall. This helps identify and prevent incoming ICMP packets with spoofed IP addresses. Additionally, they installed network monitoring software to spot unusual traffic patterns, adding an extra layer of protection. | | |
| Respond | In future security incidents, the cybersecurity team plans to isolate affected systems to stop further disruptions to the network. They'll work on restoring any critical systems and services that were impacted. After that, the team will analyze network logs to identify any suspicious or abnormal activity. All incidents will be reported to upper management and, if necessary, to the appropriate legal authorities. | | |
| Recover | To recover from an ICMP flood DDoS attack and restore normal network functioning, certain steps can be taken. In the future, external ICMP flood attacks can be prevented by blocking them at the firewall. Following that, halting all non-critical network services can help reduce internal network traffic. Priority should be given to restoring critical network services. Once the flood of ICMP packets has subsided, all non-critical network systems and services can be brought back online. | | |

| Reflections/Notes: |
| --- |