**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** | During a cybersecurity incident, the organization's network services experienced a sudden disruption caused by a distributed denial of service (DDoS) attack employing a flood of incoming ICMP packets. The security team promptly responded by blocking the attack and temporarily halting non-critical network services to restore critical network operations. | | |
| --- | --- | --- | --- |
| Identify | Malicious actors initiated a DDoS attack using an influx of ICMP packets, resulting in a complete halt of internal network services. The incident necessitated the prompt mitigation of the attack and restoration of network functionality. | | |
| Protect | In response, the cybersecurity team implemented a new firewall rule to curtail the influx of incoming ICMP packets and deployed an IDS/IPS system to identify and filter suspicious ICMP traffic patterns. | | |
| Detect | To bolster detection capabilities, source IP address verification was instituted on the firewall to thwart spoofed IP addresses in incoming ICMP packets. Furthermore, network monitoring software was adopted to promptly identify anomalies in network traffic patterns. | | |
| Respond | To better respond to future incidents, the security team devised a strategy to isolate affected systems, restore critical services, and scrutinize network logs for signs of aberrant activity. Incidents will be reported to upper management and relevant legal authorities as needed. | | |
| Recover | To recover from a DDoS attack involving ICMP flooding, the organization will execute a step-by-step process. This involves blocking external ICMP flood attacks at the firewall, temporarily suspending non-critical network services to alleviate internal network congestion, prioritizing the restoration of critical network services, and subsequently resuming non-critical services once the ICMP packet flood subsides. | | |

| Reflections/Notes: |
| --- |