**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 experienced a security event when all network services suddenly stopped functioning. The cybersecurity team found the disruption of services was caused by a DDoS attack via ICMP packet flooding. The team responded by blocking all non-critical network services, so the critical network services could be restored immediately. |
| Identify | A malicious actor targeted the company with an ICMP flood attack. The entirety of the internal network was affected. All critical resources needed to be secured and restored to a functioning state. |
| Protect | The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious patterns. |
| Detect | The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns. |
| Respond | For future events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities when required. |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services needs to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked by the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have time out, all non-critical systems and services can be brought back online. |

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