**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’s network services became unresponsive when it was flooded with ICMP packets. The team responded by blocking the incoming ICMP packets and stopping all non-critical network services, and restoring critical network services. | | |
| --- | --- | --- | --- |
| Identify | A malicious actor(s) launched a DDoS attack by taking advantage of an unconfigured firewall, flooding its network with ICMP pings causing it to become unresponsive. The entire internal network was affected so all critical network resources needed to be secured and restored to a functioning state. | | |
| Protect | The cybersecurity team implemented the originally unconfigured firewall by limiting the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. | | |
| 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. | | |
| Respond | For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. The team will attempt to restore any critical systems and services that were disrupted by the event. The team will then analyze network logs to look for suspicious and abnormal activity and finally report all incidents to upper management and appropriate authorities. | | |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at 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 timed out, all non-critical network systems and services can be brought back online.. | | |

| Reflections/Notes: |
| --- |