**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** | There was a security event that caused network services to stop working. An investigation into the event found that there was a flood of ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored. | | |
| --- | --- | --- | --- |
| Identify | The company's internal network was affected by an ICMP attack. | | |
| Protect | The cybersecurity Team implemented a new firewall that Limits the rate of incoming ICMP packets. | | |
| Detect | The cyber security team also implemented a network monitoring software to detect abnormal traffic patterns as well as configured source IP address verification on the previously mentioned firewall to check for spoofed IP addresses on incoming ICMP packets | | |
| Respond | For future security 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, if applicable. | | |
| 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: |
| --- |