**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** | A problem with the network occurred today causing a disruption in accessing company resources. This impacted the business where the network service was unresponsive for approximately 2 hours.  Throughout the course of the investigation the cybersecurity team discovered that a continuous transmission of ICMP packets was flooding the network through an unconfigured firewall. This indicated that a bad actor took advantage of our security flaws via a DDOS attack.  The incident management team managed to block all ICMP traffic where they gradually restored critical network services. | | |
| --- | --- | --- | --- |
| Identify | The incident management team throughout their investigation performed an analysis where they identified that a DDOS attack was occurring throughout the network. | | |
| Protect |  | | |
| Detect |  | | |
| Respond |  | | |
| Recover |  | | |

| Reflections/Notes: |
| --- |