**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** | Recently, our organization’s network service suddenly stopped responding to packets, after further inspections we found that we experienced a DDoS attack, which compromised the internal network by flooding it with ICMP packets that made the network stop and the incident management team blocked the packets and stopped all non-critical network services, and restoring critical network services | | |
| --- | --- | --- | --- |
| Identify | The incident management team found a lot of ICMP packets in the network that made the internal network service of the organization go down. | | |
| Protect | The team has implemented new firewall rules to limit incoming ICMP packets, they also added firewall checks for spoofed IP addresses and invested in network monitoring software with the IDS/IPS systems to filter out some ICMP traffic based on suspicious characteristics. | | |
| Detect | To detect any kind of DDoS attack we will use the firewall logging and the Intrusion Detection System to monitor for sudden stop of any service in the network. | | |
| Respond | The team blocked all ICMP packets in the network and stopped all non-critical network services and restored critical network services, and all users were notified about the incident. | | |
| Recover | The team checked for any affected servers and they are restarted and up and running like normal. | | |

| Reflections/Notes: |
| --- |