**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or just to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to continue practicing applying the NIST CSF framework to different situations you may encounter.

|  |  |
| --- | --- |
| **Summary** | The company’s services suddenly stopped responding. The incident seems to be the effect of a DDoS attack using ICMP packet flooding. Stopping all additional services can help keep the critical services online. |
| Identify | An adversary(s) launched an ICMP flood attack. Critical network services were under threat of going offline. |
| Protect | The team upgraded the firewall to limit the rate of incoming ICMP packets and an installed IDS to prevent future attacks. |
| Detect | The source of the attack was identified using network logs. The nature of the attack was determined as DDoS using ICMP flooding. |
| Respond | Isolation of affected systems can prevent the spread of the attack to the rest network. Then critical systems and services that were disrupted by the event have to be restored. |
| Recover | To recover from a DDoS attack, critical network services need to be restored. All non-critical network services should be paused to do so. After preventing the inflow of any more malicious packets, all non-critical network systems and services can be brought back online. |

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