**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 which impacted the entire internal network. |
| Protect | As a preventative and security hardening measure the nework security team configured the firewall rules to control the flow of inbound ICMP data packets. |
| Detect | Network monitoring software was implmented in order to detect irregularities with abnormal network traffic. IDS/ IPS system will be implemented in order to filter traffic that we deem as suspicious. |
| Respond | Once the organisation based on their analysis from network monitoring software dtermines that an attack pattern is occuring incoming ICMP traffic will be blocked. Non-critical services will be taken down and were took offline. |
| Recover | During the IT restauration process the cybersecurity team returned crtical network services back to normal operations. |

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