**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** | Our company had experienced a DDoS attack and compromised the internal network for two hours until it was resolved. The team and I found that our organization’s network services suddenly halted due to an incoming flux of ICMP packets. We responded by blocking all incoming ICMP packets, all non-critical network services offline, and restoring critical network services. |
| Identify | A malicious actor targeted the company using a ICMP flood attack. |
| Protect | **The cybersecurity team implemented a new firewall to stop the incoming ICMP packets, and suspended network services until they were fixed.** |
| Detect | The cybersecurity team checked for spoofed IP adddress on the incoming ICMP packets, as well as implement network monitoring software to detect future abnormal traffic patterns. |
| Respond | The Cybersecurity team will implement a new firewall to limit the rate of incoming ICMP packets, Network monitor all future logs to check for further suspicious activity. |
| Recover | In order to recover from this DDoS attack by ICMP flooding, all the network services need to be restored to normal. The new firewall should be in place to avoid any new or further ICMP flood attacks. Once it is evaluated as safe, we can now continue all non-critical network services. |

|  |
| --- |
| Reflections/Notes: After reviewing and comparing the completed exemplar to my own analysis, there is still much details, understanding of the concepts, and category placements that I must continue to review and work on. |