**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** | I’m a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses received a DDoS attack which compromised the internal network for 2 hours. | | |
| --- | --- | --- | --- |
| Identify | The identified cause was a flood of ICMP packets to the network server. This was the cause for the network to not have access to the internet. After further investigation, a malicious actor sent a flood of ICMP pings through a firewall that wasn’t properly configured. | | |
| Protect | **Incident response team block incoming ICMP packets, rendering the network offline, then restoring critical network services.** | | |
| Detect | **Implementation of a new firewall configuration, source IP verification to filter potential IP spoofs,** implementation of Network monitoring software, and addition of IDS/IPS system to filter out ICMP traffic based on suspicious characteristics. | | |
| Respond | Test the newly implemented software by having a team pentester spoof their IP, and attempt to flood the server with ICMP packets. Testing the functionality of the newly implemented Network protection features is imperative to make sure they’re properly up and running. | | |
| Recover | Restoring webservices once the issue is address and it is know that the network has recovered from the attack, and now has new network features in place to mitigate malicious attacks from coming in. | | |

| Reflections/Notes: |
| --- |