**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** |  | | |
| --- | --- | --- | --- |
| Identify | This morning the company’s cybersecurity was notified of an outage within the entire company’s internal network, which compromised systems for about 2 hours. Through thorough investigation by the cybersecurity team, it was discovered that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. The DDoS attack overwhelmed the company’s network, and was the cause of the network outages. | | |
| Protect | In order to prevent future DDoS attacks, the company has chosen to implement the following measures:  **-A new firewall rule to limit the rate of incoming ICMP packets**  **-Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets**  **-An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics** | | |
| Detect | To help prevent these situations before they become detrimental to the entire network , the company has also chosen to implement Network monitoring software (a.k.a SIEM Tools). Network monitoring software allows the cybersecurity team to analyze the packets being sent and received within the company’s network, and detect potential vulnerabilities and attacks before they are exploited. | | |
| Respond | In order to keep the attack surface of future attacks by malicious actors smaller, it would be recommended to segment the internal network by departments. This way if an actor finds an exploit within the network, the potential damages will be kept to a minimum. | | |
| Recover | Recovery from the DDoS Attack should be relatively straightforward, with just a restore needing to be done with the internal network. The most time consuming part is simply waiting for the network to be back online and ready to go. | | |

| Reflections/Notes: |
| --- |