**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** | Due to an incoming flood of ICMP packets during the DDoS attack, the organization’s network services suddenly stopped. The internal network has been comprmised for two hours. | | |
| --- | --- | --- | --- |
| Identify | Upon the investigation of security event, the company’s cybersecurity team found that a malicious actor had send a flood of ICMP pings into the company’s network through an unconfigured firewall. Through a distributed denial of service (DDoS) attack, this vulnerability allowed the unknown attackers to overwhel, the company’s network service. | | |
| Protect | To protect the organization from being vulnerable again to DDoS attacks, a new firewall rule that limits the rate of incoming ICMP packets has been implemented. Source IP address verification on the firewall, network monitoring software, and an IDS/IPS system have also been implemented. | | |
| Detect | To check for the possible spoofed IP addresses on incoming ICMP packets, detect abnormal traffic patterns, and filter out ICMP traffic based on suspicious characteristics, the source ip address verification on the firewall, network monitoring software, and an IDP/IPS system will be utilized by the company. | | |
| Respond | For the improvement of the security level of internal network of the company, the employees and interns will be trained on how to use and implement new firewall rule, source IP address verification feature, network monitoring software, and IDS/IPS system for them to become familiarized on how to resolve issues related to malicious attacks. The team will analyze network logs to check for any abnormal activities by using network monitoring software. Once an incident happens, this will be reported to appropriate legal authorities. | | |
| Recover | To recover for the upcoming or possible attacks, ICMP packets must be blocked, all non-critical network services offline must be stopped, and critical network services must be restored once everything has been resolved. | | |

| Reflections/Notes: It is essential to have a plan made from templates like this so that the interns and employees will be familiarized about solving cybersecurity-related issues that might come along the way. |
| --- |