**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** | Today the company experienced a DDoS attack, compromising our internal network for two hours. During the attack, our services were unresponsive, and normal internal network traffic could not access any network resources. | | |
| --- | --- | --- | --- |
| Identify | A DDoS attack caused this breach. ICMP packet spam was sent through an unconfigured firewall to the internal network by the malicious actor. The attacker crashed the internal server because the ICMP request overloaded the computer. | | |
| Protect | The team has implemented a new firewall that limits the rate of incoming ICMP packets. Given that this attack was successful due to a high amount of traffic, IT has implemented a network monitoring software to detect abnormal traffic patterns and an IDS/IPS system to filter out the traffic of ICMP based on suspicious characteristics. | | |
| Detect | To detect new unauthorized access attempts and attacks in the future, cybersecurity has configured an IP address verification on the firewall. This configuration ensures that all IP addresses are verified to prevent spoofing (invalid IP addresses) from coming in the incoming ICMP packets | | |
| Respond | In response to the attack, IT blocked incoming ICMP packets from entering the network. This stopped all non-critical network services and restored the service. Our team informed upper management about the attack and they will contact our customers by mail to inform them of the data breach. Management will also need to engage local law enforcement. | | |
| Recover | The team will recover the compromised data by following the Incident and response vulnerability playbook. Team will restore all data lost. | | |

| Reflections/Notes: |
| --- |