**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** | The company experienced network services suddenly stopped. Based on investigation from the cybersecurity team it happened because of a DDoS attack which compromised the internal network. The attack itself was due to an incoming flood of ICMP packets and because of that normal internal network traffic could not access any network resources. The team found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. | | |
| --- | --- | --- | --- |
| Identify | a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. | | |
| Protect | the network security team implemented:   * 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 * Network monitoring software to detect abnormal traffic patterns * An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics | | |
| Detect | The team investigates the source IP addresses on incoming ICMP packets and uses network traffic tools to look at the network traffic. | | |
| Respond | blocking incoming ICMP packets. | | |
| Recover | stopping all non-critical network services offline, and restoring critical network services. | | |

| Reflections/Notes: |
| --- |