**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 recently experienced a DDoS attack which rendered the internal network unavailable for two hours. The attack was an ICMP flood attack which overwhelmed the system leaving no resources for normal traffic. It was determined a malicious actor was able to flood the company’s network through an unconfigured firewall. | | |
| --- | --- | --- | --- |
| Identify | After an audit was performed on the systems related to the attack it was determined a malicious actor used an unconfigured firewall to send ICMP pings and flood the internal network leaving it with no resources and unusable for normal traffic for two hours. | | |
| Protect | The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets as well as Source IP address verification to check for spoofed IP addresses on incoming ICMP packets. Going forward the company will also use network monitoring software to detect abnormal traffic patterns and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. | | |
| Detect | To detect future attacks the team will use network monitoring software and an IDS/IDP system to detect and filter out suspicious traffic. | | |
| Respond | The incident management team responded by blocking incoming ICMP packets and stopping all non-critical network services offline. | | |
| Recover | Once the ICMP packets were blocked they were able to restore critical network services. | | |

| Reflections/Notes: |
| --- |