**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’s servers were hit with an ICMP flood attack that caused two hours of downtime. The team quickly responded by blocking ICMP to mitigate the attack and bring critical services back online | | |
| --- | --- | --- | --- |
| Identify | An unknown threat actor attacked the servers using ICMP, rendering services unavailable | | |
| Protect | In order to protect the server, the cybersecurity team added a new firewall rule to ratelimit ICMP packets and installed an IDS system to filter out illegitimate ICMP requests | | |
| Detect | The team added a Source IP address verification system to verify IP addresses on ICMP packets and added network monitoring to detect patterns. | | |
| Respond | The future plan is to null route affected systems to prevent disruption to the entire network. Any critical systems will be restored and then network logs will be checked for suspicious activity. All incidents will be forwarded to upper management, as well as law enforcement if necessary. | | |
| Recover | Access to all systems has to be restored, as well as the attack halted or mitigated. Critical systems are the priority. | | |

| Reflections/Notes: Consider contracting with an outside provider, such as Cloudflare and mitigating for other spoofing attacks as well, such as UDP and DNS flooding. Consider disabling ICMP entirely unless needed for services. |
| --- |