**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** | A multimedia company had a DDoS attack which lasted 2 hours, the threat actor gained access through an unconfigured fire wall and sent loads of ICMP packets to shut down the server. | | |
| --- | --- | --- | --- |
| Identify | The attack was a DDoS type of attack that shut off all services for 2 hours. | | |
| Protect | In the future adding regular security audit checks to ensure that all firewalls are configured and up to date, adding penetration testing is a good idea too. | | |
| Detect | Now that the firewall is filtering and shows irregularities, checking the SIEM tool regularly to check for unusual traffic patterns to prevent this | | |
| Respond | Identify the situation faster to be able to respond faster. Locking all incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services are some ways to respond. | | |
| Recover | Go through any devices that might have been infected and wipe them properly, but mainly ensure the website service is back up ASAP. | | |

| Reflections/Notes: |
| --- |