**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 multimedia company experienced a ddos attack that compromised the internal network for two hours.  During the attack the network services stopped responding due to an incoming flood of ICMP packets.  No internal network traffic  Incident response team blocked incoming ICMP packets, stopping all noc-critical network services, and restoring critical network services.  The cybersecurity team investigated the security event and found that a malicious actor had sent a flood of ICMP pings to the company network through an unconfigured firewall.  The vulnerability allowed the attack to do a ddos attack | | |
| --- | --- | --- | --- |
| Identify | There should be firewall configuration audits in place to prevent open ports and block incoming icmp packets | | |
| Protect | **Icmp packets should be blocked from the firewall to prevent icmp ddos attacks** | | |
| Detect | Siem tools, proper firewall configuration and antivirus should be used to prevent such risks to the network | | |
| Respond |  | | |
| Recover |  | | |

| Reflections/Notes: |
| --- |