**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** |  | | |
| --- | --- | --- | --- |
| Identify | organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. | | |
| Protect | Incoming ICMP packets were blocked, non-critical network services were taken offline and critical network services were restored. | | |
| Detect | There was an unconfigures firewall that allowed malicious attackers to overwhelm company’s network through DDOS attack. | | |
| Respond | A new firewall was put inplace to limit the rate of incoming ICMP packets. Source IP address verification on the firewall was implemented to check for spoofed IP addresses on incoming ICMP packets. Network monitoring software was implemented to detect abnormal traffic patterns and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. | | |
| Recover | Ensured that all the network security devices are properly set in place and are functioning. | | |

| Reflections/Notes:Need to make sure that security measures are carefully put in place, there shouldn’t be any unconfigured firewalls, also security hardening should be done regularly. |
| --- |