**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 experienced a security breach when all network services suddenly  stopped responding. The sudden stoppage was caused  by a distributed denial of services (DDoS) attack through a flood of incoming  ICMP packets. The team responded by blocking the attack and stopping all  non-critical network services, so that critical network services could be  restored. Furthermore, they also went a step ahead and addressed the security event and implemented a new firewall, source Ip verification, network monitoring, and new IDS/IPS system. |
| Identify | A malicious actor(s) attacked the company with an ICMP flood attack.  The entire internal network was affected. All critical network resources needed  to be secured and restored to a functioning state. |
| Protect | **To prevent and protect this attack, the team implemented a new firewall to limit the rate of incoming rate of ICMP packets. They also added Source IP address verification on the firewall to check for spoofed IP addresses on coming ICMP packets.** |
| Detect | Implemented a network monitroing software to detect abnormal traffic patterns. They also implemented an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics |
| Respond | For security incidents, the team isolates affected systems, restores critical services, investigates logs, and reports to management and authorities as needed. |
| Recover | To recover from ICMP flood DDoS attacks, first block floods at the firewall while stopping non-critical services. Restore essential operations first, then reactivate other services once the attack ends. |

|  |
| --- |
| Reflections/Notes: |