**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 DDoS(Distributed Denial of Service) attack.  The internal network service stopped working for two hours due to a flood of incoming ICMP packets. The incident management team responded by blocking the incoming ICMP packets, stopping all non-critical network services and restoring critical network services. | | |
| --- | --- | --- | --- |
| Identify | The entire internal network was compromised. Critical network services were disrupted. Attack vector caused by an unconfigured firewall. | | |
| Protect | The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IPS/IDS system to filter out suspicious ICMP traffic. | | |
| Detect | The network security team implemented network monitoring software to detect abnormal traffic patterns and configured source IP address verification on the firewall to check for spoofed IP addresses. | | |
| Respond | For future events, the affected system will be isolated to prevent further network disruption. Critical network services will be prioritized for restoration, non-critical network services will be turned off if necessary. The security team will analyse network logs for abnormal activities. The team will also report the incidents to upper management and the appropriate legal team. | | |
| Recover | To recover from a DDoS attack. The malicious packet flood will be blocked by the firewall. Critical network services need to be restored first. Non-critical network services will be stopped to reduce internal network traffic to maintain critical network services. Once the attack has been contained, non-critical network services can be brought back online. | | |

| Reflections/Notes: |
| --- |