**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** | Our company’s internal networks were compromised for 2 hours recently. It has been observed that a DdoS attack was performed by the attacker by flooding the server with ICMP packets through a vulnerability in an unconfigured firewall. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| Identify | The incident management team audited the systems, docs and the available resources and found out the security gaps due to which the attack was possible. They found out that the attacker sent ICMP packets through an unconfigured wall. The internal services were down for at least 2 hours |
| Protect | * The team has implemented techniques like adding a new firewall rule to limit * the rate of incoming ICMP packets, Source IP address verification on the * firewall to check for spoofed IP addresses on incoming ICMP packets to tackle DdoS attacks of the same type. |
| Detect | * The team will be using Network monitoring software to detect abnormal traffic patterns and An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Respond | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services  need to be restored to a normal functioning state. In the future, external ICMP  flood attacks can be blocked at the firewall. Then, all non-critical network  services should be stopped to reduce internal network traffic. Next, critical  network services should be restored first. Finally, once the flood of ICMP  packets have timed out, all non-critical network systems and services can be  brought back online. |

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