**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** | All the network services of the organization was working smoothly until they suddenly stopped responding. The normal internal network was not able to access any of the network resources. The incident management team was called upon to rescue and they found out that it was a result of an incoming flood of ICMP Packets. The organization had experienced a DDoS attack which resulted in the disruption of the internal network for two hours after which it was resolved. The team upon further investigation found out that a malicious actor had sent a flood of ICMP pings into the company’s network. The cybersecurity team responded by blocking incoming ICMP packets and restoring critical network services. |
| Identify | The incident management team audited the systems, devices, and access  policies involved in the attack to identify the gaps in security. The team found  that it has been a DDoS attack , the attacker has flooded the company’s network with the ICMP pings. It happened because the firewall was not configured correctly to limit the rate of incoming ICMP packets. |
| Protect | The security team has implemented the following security hardening improvements to protect the organization from further attacks:   * 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 * Network monitoring software to detect abnormal traffic patterns * An IPS system to filter out some ICMP traffic based on suspicious characteristics |
| Detect | To detect flooding attacks like these the organization will deploy SIEM tools which will monitor the traffic and an IDS system which will detect the abnormal packets and alert the concerned authorities. |
| Respond | The cybersecurity team responded by blocking incoming ICMP packets and restoring critical network services. They also informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws. |
| Recover | After blocking the traffic and configuring the port the network services got back to their normal functioning. For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. The employees were told not to panic and were made aware that in future if they witness an unusual activity like this, they should inform the Incident response department immediately. This ensures business continuity. |

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