**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 Organization experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. The company’s cyber security team then investigated the security event.  The Organization’s network services stopped responding due to an incoming flood of ICMP packets. Normal internal traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline and restoring critical network services.  They found that a malicious actor sent a flood of ICMP pings into the company’s network through an unconfigured firewall, this vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed DDoS attack. |
| Identify | The company’s cybersecurity team found out that a **malicious actor** has sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) |
| Protect | **To address this security event, the network security team implemented:**   * **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 IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.** |
| Detect | To detect potential threats in the future, the team will implement 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, implement IDS and IPS system to filter out some ICMP traffic based on suspicious characteristics. IDS/IPS will provide real-time alerts to detect unusual ICMP traffic patterns and possible DDoS activity. |
| Respond | During the attack, our organization’s incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline and restoring critical network services. Upon investigating security events, the network security team implemented a new firewall to limit the rate of incoming traffic, 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, and an IDS and IPS system to filter out some ICMP based on suspicious characteristics. |
| Recover | The team will recover all deleted data by restoring the database from the previous night. All staff have been informed that any customer information entered or changed after the incident would not be recorded on the backup. They will need to re-enter the information into the database once it has been restored from last night’s backup. |

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