**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** | Organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. |
| Identify | The company’s cybersecurity team then investigated the security event. They found that a malicious actor had 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) attack. |
| 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. And an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics |
| Detect | To detect future attacks, IP address verification on the firewall to detect spoof IP addresses from incoming ICMP packets and a network monitoring software was installed to detect abnormal traffic patterns from here on. |
| Respond | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| Recover | Critical network services was restored, with a new firewall rule limiting the rate of incoming ICMP packets and IDS/IPS system to filter out ICMP traffic based on suspicious characteristics, normal operations was restored after 2 hours. |

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