**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** | This morning our organization was hit by a DDoS attack which compromised the internal network for 2 hours. During the attack, your 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. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.  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. | | |
| --- | --- | --- | --- |
| Identify | The attacked affected the organization’s network services. Normal internal network traffic could not access any network resources due to an incoming flood of ICMP packets. 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 | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services  . 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 | A Network monitoring software is implemented to detect abnormal traffic patterns. | | |
| Respond | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. | | |
| Recover | The incident managment team implemented an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics and a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. Doing this will help the company avoid the same attack in the future. | | |

| Reflections/Notes: |
| --- |