**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** | Earlier today, several employees reported being unable to access the company’s internal network. Upon reviewing the logs using the network analysis tool *tcpdump*, we identified multiple unauthorized IP addresses sending ICMP packets to our servers. Based on this activity, we believe a malicious actor carried out a Distributed Denial-of-Service (DDoS) attack. Services were unavailable for approximately two hours until the issue was resolved. |
| Identify | The incident response team conducted a thorough audit of all systems, devices, and access policies involved in the attack to identify any security gaps. The investigation revealed that the attacker exploited an unconfigured firewall to conduct the DDoS attack and send a flood of ICMP packets, overwhelming the network and causing the service disruption. |
| Protect | In response, the team implemented new security measures. These included configuring firewall rules to limit the rate of incoming ICMP packets and enabling source IP address verification to detect and block spoofed addresses in ICMP traffic. |
| Detect | To improve future threat detection, the team plans to deploy network monitoring tools capable of identifying abnormal traffic patterns. In addition, an intrusion detection and prevention system (IDS/IPS) will be implemented to analyze and filter ICMP traffic based on suspicious characteristics. |
| Respond | The team responded to the attack by blocking incoming ICMP packets and disabling all non-essential network services. Upper management has been informed of the incident, and they will notify customers regarding the two-hour downtime. |
| Recover | Critical network services were successfully restored, and all systems are now fully operational. |

|  |
| --- |
| Reflections/Notes: Make sure our firewalls meet our security standards and keep a close eye on network traffic to make sure we don’t have a similar incident in the future |