**Review the scenario below. Then complete the step-by-step instructions.**

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

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.

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

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company’s network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them here:

* **Identify** security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
* **Protect** internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
* **Detect** potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
* **Respond** to contain, neutralize, and analyze security incidents; implement improvements to the security process.
* **Recover** affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.

**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | During the attack, the organization’s network was overwhelmed by a flood of ICMP packets, causing network services to stop responding for 2 hours. The incident management team blocked incoming ICMP packets, took non-critical services offline, and restored critical ones. The cybersecurity team discovered that a malicious actor exploited an unconfigured firewall to launch a DDoS attack with ICMP pings. |
| Identify | The incident management team audited the systems, devices, and access policies involved in the attack to pinpoint security gaps. The team found that a malicious actor exploited an unconfigured firewall to launch a DDoS attack with ICMP pings known as an ICMP flood attack. Upon initial review, we only had a disruption in service for about 2 hours. This affected the whole organization because it knocked off connection to our internal network and could not access network resources needing critical network resources to be restored. |
| Protect | The network security team implemented an update to the firewall by adding a new rule to limit the rate of ICMP packets and source IP verification. Additionally, the team is implementing proactive technology such as network monitoring software and install an IDS/IPS system. |
| Detect | To detect new attacks in the future, the team has added network monitoring software to detect and alert the team for any abnormal traffic patterns. The team also installed IDS/IPS systems to filter out ICMP traffic based on suspicious characteristics and alert the team when ICMP traffic is filtered out. |
| Respond | The incident management team promptly blocked incoming ICMP packets, deactivated non-critical services, and restored essential ones. We performed comprehensive firewall maintenance and implemented new rules to limit ICMP packet rates and verify source IPs, mitigating future DDoS attack risks. Upper management has been briefed on the incident and will notify appropriate legal authorities if needed. |
| Recover | The team updating the configuration of the firewall to stop incoming ICMP packets, allowed us to start the process of recovering the servers. Then deactivating non-critical services allows for the team to focus on getting critical services back online. Lastly, once the flood of ICMP packets have ended, non-critical services can be brought online. |

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