**Incident Report Analysis**

## **Scenario**

****

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.

| **Summary** | The company experienced a security event when all network services suddenly stopped responding. The cybersecurity team found the disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services so that critical network services could be restored. | | |
| --- | --- | --- | --- |
| Identify | Malicious actors targeted the company with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be secured and restored to a working state. | | |
| Protect | The cybersecurity team needs to implement a new firewall rule that limits the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics recognized from their digital signatures. | | |
| Detect | The cybersecurity team will configure source IP address verification on the firewall to detect and block spoofed IP addresses in incoming ICMP traffic. They will also implement a Security Information and Event Management (SIEM) solution to monitor and analyze network traffic through real-time log analysis. | | |
| Respond | For future security incidents, the cybersecurity team carries out network segmentation and isolates affected systems to contain the disruption. They work on restoring critical systems and services impacted by the event. The team reviews network logs from the Security Information and Event Management (SIEM) tool to detect any suspicious or unusual activity. All incidents are reported to upper management and relevant legal authorities when necessary. | | |
| Recover | To recover from a DDoS attack caused by ICMP flooding, network services must be restored to normal functioning. In the future, external ICMP flood attacks can be blocked at the firewall to prevent recurrence. During the recovery process, stopping all non-critical network services reduces internal network traffic and minimizes the attack surface, allowing for easier containment and management. Critical network services should be restored first. Once the ICMP packet flood subsides, all non-critical systems and services can be brought back online. | | |