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 incident and integrate your analysis into a general security strategy:

- **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.

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	The company was subjected to a disruptive DDoS assault in which the internal network was compromised due to a flood of ICMP messages. The incident resulted in a two-hour network outage. The attack was countered by blocking incoming ICMP packets, suspending non-essential network services, and restoring important ones. An investigation revealed that the attack was enabled by an unconfigured firewall, prompting the deployment of several security measures such as rate limitation, source IP verification, network monitoring, and an IDS/IPS system to prevent such attacks in the future.
Identify	The company experienced a targeted ICMP flood attack orchestrated by malicious code, resulting in a widespread impact across the internal network. The immediate action needs to implement to safeguard all the affected assets.
Protect	The cybersecurity team executed a multifaceted approach to safeguard the network infrastructure. A new firewall rule was devised to curtail the rate of incoming ICMP packets, thereby mitigating the flood attacks impact. Additionally, an IDS/IPS was deployed to selectively filter out ICMP traffic exhibiting suspicious attributes the

	network’s resilience.
Detect	The cybersecurity team improved detection skills by acting proactively. At the firewall level, source IP address verification was put into effect, checking incoming ICMP packets for any signs of IP address spoofing. The purpose of this tactical improvement is to thwart potential spoof attacks from bad actors. Additionally, network monitoring software was carefully designed to detect abnormal traffic patterns and quickly spot anomalies that need further examination.
Respond	The cybersecurity team presented a thorough reaction strategy. In the case of an intrusion, quick containment will be used to isolate compromised systems and stop additional network interruption. Then, focused efforts will be made to fully restore the functionality of the affected vital systems and services. We will thoroughly examine network logs to find any signs of questionable or unusual activity so that we can take preventative action against potential attacks. As required by applicable regulations, all related incidents will be diligently reported to senior management and the appropriate legal authorities.
Recover	In order to restore regular network operations after a DDoS assault using ICMP flooding, the business has a recovery strategy in place. External ICMP flood attacks will be actively blocked by the firewall in order to stop them from happening again. Once internal network congestion has been reduced, a strategic plan involving the temporary termination of non-critical network services will be put into place. Following suit, important network services will be restored in a prioritized manner to make sure core functions quickly resume functioning. Following the termination of the ICMP packet flood period, non-critical network systems and services will be gradually reinstated, leading to a thorough restoration of the network ecosystem.

Reflections/Notes: