Scenario

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

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 experienced a Distributed Denial of Service (DDoS) attack using ICMP (Internet Control Message Protocol) packets. This attack flooded the network, overwhelming it and causing a disruption in normal network services for approximately two hours. The incident was exacerbated by firewall misconfigurations that allowed the attack to penetrate the network unchecked, leading to a critical downtime in network operations.
Identify	During the incident analysis, it was identified that the network disruption was caused by a DDoS attack utilizing ICMP packets. The investigation revealed that the firewall configurations were inadequate, which allowed the malicious ICMP flood to reach and impact internal network resources.
Protect	To enhance network security and prevent future attacks, several protective measures were implemented: • New Firewall Rules: A new rule was introduced to limit the rate of incoming ICMP packets, effectively mitigating the impact of ICMP flood attacks. • Source IP Address Verification: Source IP verification was enforced on the firewall to detect and block spoofed IP addresses associated with incoming ICMP packets, preventing potential spoofing attacks.
Detect	In response to the attack, the company bolstered its detection capabilities with:

	• Network Monitoring Software: Deployed to continuously monitor network traffic for abnormal patterns indicative of potential security threats. • IDS/IPS System: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) were implemented to filter ICMP traffic based on suspicious characteristics, enhancing the ability to detect and mitigate DDoS attacks in real-time.
Respond	The incident management team swiftly responded to the DDoS attack by: • Blocking Incoming ICMP Packets: Immediate action was taken to block incoming ICMP packets to halt the ongoing flood, preventing further network disruption. • Stopping Non-Critical Network Services: Non-critical network services were temporarily taken offline to prioritize critical operations and mitigate the impact of the attack. • Restoring Critical Network Services: Efforts were focused on restoring critical network services to normal operation, minimizing downtime and restoring business continuity.
Recover	Since the attack primarily caused a disruption in network services without data loss, the recovery phase involved: • Restoration of Normal Operations: Waiting for all network services to resume full functionality after implementing security measures and mitigating the impact of the DDoS attack. • Monitoring for Stability: Continuously monitoring the network post-incident to ensure stability and resilience against potential future attacks.

Reflections/Notes: