Incident report analysis

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.

Summary	A DDoS attack occurred, targeting the company's internal network by flooding it with ICMP packets. The internal network became unresponsive for approximately two hours, disrupting all services. The attack exploited an unconfigured firewall that allowed the malicious traffic to pass through. The security team responded quickly, blocking ICMP packets and restoring essential services. The root cause was identified, and preventive measures were implemented.
Identify	The unconfigured firewall allowed a flood of ICMP traffic, leading to a network

	outage. Affected systems included internal servers and business-critical network services. A security audit revealed the firewall did not have rules to limit or inspect ICMP traffic, making it a major vulnerability.
Protect	New firewall rules were implemented to limit ICMP traffic and verify source IP addresses. Security policies were updated to enforce regular configuration audits. Awareness training for IT personnel on firewall configuration and DDoS threats was initiated. An IDS/IPS system was added to better filter traffic in real time.
Detect	Network monitoring tools were installed to identify unusual traffic spikes. An IDS/IPS was configured to detect ICMP-based threats and alert the security team. Logs and alerts are now continuously reviewed for suspicious patterns in traffic.
Respond	The cybersecurity team blocked incoming ICMP traffic and shut down non-essential services. Critical services were restored first to reduce business impact. Post-incident analysis was conducted and shared with stakeholders. Incident response protocols were updated to include DDoS-specific actions.
Recover	Systems were restored after two hours of downtime. Data was not compromised, but services were temporarily inaccessible. Recovery procedures were reviewed and reinforced. The team documented lessons learned and integrated improvements into recovery planning.

Reflections/Notes:

- This incident highlights the importance of proactive firewall configuration.
- The organization must invest in continuous monitoring and regular security audits.
- A documented incident response plan and staff readiness significantly reduced downtime.
- Incorporating CSF functions ensures the company is more resilient to future attacks.