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 faced a security issue when all network services suddenly became unresponsive. The cybersecurity team discovered it was due to a flood of incoming ICMP packets, known as a distributed denial of service (DDoS) attack. To mitigate the attack, they blocked it and temporarily halted non-critical network services, prioritizing the restoration of critical ones.
Identify	A malicious individual or group launched an ICMP flood attack against the company, causing widespread disruption across the internal network. It became crucial to safeguard and restore all critical network resources to ensure normal functioning.
Protect	The cybersecurity team enforced a new firewall rule to control the influx of incoming ICMP packets and deployed an IDS/IPS system to filter potentially suspicious ICMP traffic based on identifiable traits.
Detect	The cybersecurity team set up source IP address verification on the firewall to detect forged IP addresses in incoming ICMP packets and installed network monitoring software to identify unusual traffic patterns.
Respond	In future security events, the cybersecurity team plans to isolate affected systems to contain potential network disruptions. They'll prioritize restoring any critical systems impacted. Afterward, they'll analyze network logs for signs of suspicious activity and report incidents to upper management and relevant legal authorities, if necessary.
Recover	To recover from an ICMP flooding DDoS attack, restoring normal access to network services is crucial. For future protection, the firewall can block external ICMP floods. Then, halting non-critical services minimizes internal network congestion. Prioritizing, critical services are restored first. Once the ICMP flood subsides, gradually bring back

	non-critical systems and services online.

Reflections/Notes: