Incident report analysis

Task:

In this activity, you will create an incident report using the knowledge you've gained about networks throughout this course to analyze a network incident. You will analyze the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF).

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.

Summary	The company faced a security issue when all network services suddenly stopped working. The cybersecurity team discovered that a distributed denial-of-service (DDoS) attack caused the disruption by flooding the network with ICMP packets. The team responded by blocking the attack and shutting down non-critical network services to restore critical ones.
Identify	A malicious actor launched an ICMP flood attack against the company, affecting the entire internal network. Critical network resources had to be secured and restored to working order.
Protect	The cybersecurity team set up a new firewall rule to limit the number of incoming ICMP packets and added an IDS/IPS system to filter out ICMP traffic with suspicious traits.
Detect	The cybersecurity team created a firewall rule to limit incoming ICMP packets and installed an IDS/IPS system to block suspicious ICMP traffic.
Respond	In future security events, the cybersecurity team will isolate affected systems to stop further network disruptions. They will work on restoring critical systems

	and services affected by the event. Afterward, they will review network logs for any suspicious or unusual activity and report incidents to upper management and legal authorities, if needed.
Recover	To recover from a DDoS attack using ICMP flooding, network services need to be returned to normal. In the future, external ICMP floods can be blocked at the firewall. Non-critical services should be shut down to reduce internal traffic, and then critical services should be restored first. Once the ICMP flood ends, non-critical systems and services can be brought back online.

Reflections/Notes: The cybersecurity team took swift action to mitigate the impact of the DDoS attack by blocking the flood of ICMP packets and prioritizing the restoration of critical services. Moving forward, the team plans to enhance protection with firewall rules and IDS/IPS systems while refining recovery processes to ensure a quicker return to normal operations. This proactive approach will help safeguard the network against similar attacks in the future.