Incident report analysis

Project Description:

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	Organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. The security team has found that the malicious actor has sent the flood of ICMP pings into the company's network. This allowed the malicious actor to overwhelm the network through a distributed denial of service (DDoS) attack. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	A malicious actor used an ICMP flood attack to the company's internal network. The internal network was affected and all network resources had to be restored.

Protect	The security team has implemented a new firewall rule to limit the rate of the incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The security team has added a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and a network monitoring software to detect abnormal traffic patterns.
Respond	For future events, The cybersecurity team will analyze the network logs for abnormal activity. The team will also immediately restore any critical systems, networks and services that were affected by the incident. The team will separate the affected systems to stop any more problems with the network.
Recover	To recover from an ICMP flood DDoS attack, network services need to be brought back to normal. In the future, ICMP flood attacks can be blocked at the firewall. First, non-important network services should be turned off to lower internal traffic. Then, the important services should be brought back online first. Once the ICMP flood stops, all the non-important services can be turned on again.

Reflections/Notes: