Incident report analysis

Summary	Recently our network services stopped working for 2 hours as a result of a DDoS attack. The incident management team found out the actor sent a flood of ICMP packets resulting in normal network traffic not being hable of reach network results. The team stopped all non-critical network services so it could be restored.
Identify	A malicious actor sent a flood of ICMP packets resulting in normal network traffic not being hable of reach network results.
Protect	The team implemented a new firewall rule as well as source ip address verification on the new firewall and an IDS/IPS system to filter out ICMP suspicious traffic.
Detect	To detect new abnormal traffic the team implemented a network monitor software and a source ip address verification on the new firewall to prevent ICMP packets flooding.
Respond	The team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. For future events the team should inform the upper management team in order for the clients to get notified about the status of the web site availability as well as the legal authorities if needed. The team will also proceed to isolate affected systems to prevent further escalation to the network and use the newly implemented monitor software to detect the traffic before it affects our systems.
Recover	The newly updated firewall will help in the future preventing the ICMP flood attacks but also the network non-critical services in case of the attack should

	be shutdown to prevent internal network traffic. When the situation is resolved the services should be brought online by order of importance.

Reflections/Notes:

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 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.