Incident report analysis

13th February 2025

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.

Incident report analysis

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	A multimedia company experienced a DDoS attack that compromised systems for two hours. Network operations were at a halt due to an immense influx of ICMP packets. The internal network was affected, and traffic could not access any network resources. The incident team responded by blocking all incoming ICMP packets and stopping all non-critical network services offline. Investigations of the incident showed that a malicious actor sent floods of ICMP packets into the company's network through an unconfigured firewall. This vulnerability allowed the malicious actor to diminish the processing capabilities of the network through a Distributed Denial of Service Attack (DDoS).
Identify	The cybersecurity team investigations prove a malicious actor or group had sent several ICMP floods to the company's network through unconfigured firewalls. Upon initial review, this incident appears to be a Distributed Denial of Service (DDoS) attack. The entire internal network was affected.
Protect	The network security team implemented a new firewall rule to limit the rate of

	incoming ICMP packets, a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, network monitoring software to determine abnormal traffic patterns, and an IDS/IPS system to filter out traffic based on suspicious characteristics.
Detect	To detect ICMP floods in the future, the team would implement an IDS/IPS system in the organization's network to monitor all incoming traffic and alert any suspicious findings in the organization's network.
Respond	The security team responded by blocking all incoming ICMP packets using a firewall and stopping all non-critical network services offline.
Recover	The organization will return to normal operations by implementing network hardening techniques such as configuring a firewall to block unwanted traffic in the organization’s network.

Reflections/Notes: