Incident report analysis using 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.

Summary	The organisation's network suddenly stopped responding due to a DDoS attack which compromised the internal network for 2 hours until it was resolved. The disruption to the internal network was caused by an incoming flood of ICMP packets. Blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services were performed by the incident management team. The root cause was an unconfigured firewall which was exploited by the threat actor who sent a flood of ICMP pings into the company's network, resulting in a DDoS attack.
Identify	The threat actor executed an ICMP flood attack which affected the entire internal network for 2 hours. All critical network resources had to be secured and restored back to a functioning state.
Protect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets. They also implemented an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team implemented Network monitoring software to detect abnormal traffic patterns. Source IP address verification was configured on the firewall to validate IP addresses on the incoming ICMP packets.
Respond	For future cyber security events, the cyber security team will isolate affected systems to contain the breach and minimise the attack's surface area. They will attempt to restore all critical resources that were affected by the event. Then the team will analyse logs and traffic from their SIEM, IPS and IDS to find any suspicious and abnormal activity. Senior management will become aware of this incident as well as legal authorities if needed.
Recover	To recover from ICMP flooding DDoS attack, the team needs to restore the network services back to a functioning state. The external ICMP flood attacks

	can be blocked by the newly configured firewall. Then all non-critical network resources and activity will be suspended to reduce internal network congestion and traffic. Once the ICMP packets have timed out, the non-critical network resources and activity can be restored.