NIST Framework Scenario/Report

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.

NIST Framework Report

Summary	The multimedia company experienced a two-hour network outage after being targeted by a distributed denial-of-service (DDoS) attack. During the incident, the attacker flooded the company's network with ICMP ping packets, which overwhelmed resources and prevented normal internal traffic from accessing network services. Investigation revealed that the traffic entered through an unconfigured firewall, allowing the malicious actor to exploit this weakness and disrupt operations.
Type of Attack	The organization experienced an ICMP flood DDoS attack that disrupted network operations for approximately two hours. The attack flooded and overwhelmed the company's internal network resources. Because of the excessive traffic, normal internal network traffic was unable to access critical network services during the incident. The systems most impacted included the company's internal servers, network infrastructure devices (firewalls and routers), and workstations that rely on those services for connectivity.
Identify	Our organization will regularly conduct vulnerability and configuration audits of firewalls, routers, and switches to ensure no unconfigured or default rules are left exposed. An updated asset inventory will be maintained to track all internal systems and devices. Access privileges will be reviewed consistently to enforce the principle of least privilege, and penetration testing and risk assessments will be performed to identify potential weaknesses, including those related to ICMP traffic handling.
Protect	To protect internal assets, the company will implement strict firewall policies that block or limit unnecessary ICMP traffic. New firewall rules will include rate limiting to prevent network flooding, and IP source verification will be configured to reduce spoofing attempts. Employees will receive regular training on incident response and

	security awareness so that IT personnel can quickly recognize denial-of-service activity. In addition, all network security policies will be documented and enforced, including change management procedures for firewall rule updates.
Detect	The organization will deploy network monitoring software capable of identifying abnormal traffic patterns, such as spikes in ICMP requests. Firewall, IDS/IPS, and server logs will be centralized and analyzed to improve visibility across the network. Automated alerts will be configured to notify the security team if incoming ICMP traffic exceeds established thresholds. The effectiveness of these detection tools will also be tested regularly through simulated attack exercises.
Respond	To improve response capabilities, the organization will develop and test a DDoS response playbook so that all staff members understand the escalation process during an incident. The IDS/IPS system will be configured to automatically filter malicious ICMP traffic in real time. Clear communication channels will be established to notify both technical staff and management when an incident occurs. After each attack, the security team will conduct a post-incident analysis to refine firewall rules, IDS/IPS signatures, and monitoring thresholds.
Recover	The company will prioritize restoring critical network services first, followed by non-critical services, to minimize downtime. After recovery, all systems will be validated to confirm they were not altered or compromised during the attack. Business continuity and disaster recovery plans will be updated to reflect lessons learned from each incident. A post-recovery review will also be conducted with management to discuss improvements and consider additional resilience measures, such as leveraging third-party DDoS mitigation services.