Incident report analysis

Summary	The organization experienced a **Denial of Service (DoS) attack** that disrupted internal network operations for approximately **two hours**. The attack was caused by a flood of **ICMP packets** originating from a malicious external source. Due to an **unconfigured firewall**, the excessive ICMP traffic overwhelmed network resources, causing critical services to become unresponsive. As a result, internal users were unable to access network systems and services during the incident window. The incident response team mitigated the attack by **blocking incoming ICMP traffic**, temporarily **disabling non-critical services**, and prioritizing the **restoration of critical systems**. After the incident, the cybersecurity team investigated the root cause and implemented new technical controls, including ICMP rate limiting, source IP verification, network monitoring software, and an IDS/IPS solution.
Identify	The cybersecurity team conducted a review of affected systems and network configurations to identify the root cause and impact of the incident. ● **Type of attack:** Denial of Service (DoS) via ICMP flood ● **Attack vector:** External network traffic exploiting an unconfigured firewall ● **Affected systems:** ○ Internal network infrastructure ○ Network services relied upon by employees ● **Business impact:**

	○ Two hours of operational downtime ○ Temporary loss of access to internal network resources ● **Identified vulnerability:** ○ Lack of firewall rules governing ICMP traffic ○ Absence of traffic rate limiting and spoofed IP validation This analysis revealed gaps in firewall configuration and network traffic monitoring that allowed the attack to succeed.
Protect	To better safeguard organizational assets and reduce the risk of future DoS attacks, the following protective measures should be implemented or strengthened: ● Configure strict firewall rules to limit and control ICMP traffic by default ● Enforce rate limiting on all inbound network traffic, not just ICMP ● Implement source IP address verification to prevent spoofed packets ● Establish secure baseline firewall configurations and conduct regular configuration audits ● Develop and document network security policies defining acceptable traffic types ● Provide security awareness training for IT staff on DoS prevention and firewall hardening These measures reduce the organization's attack surface and prevent misconfigurations from being exploited.
Detect	To improve early detection of abnormal or malicious network activity, the organization should strengthen monitoring and detection capabilities: ● Deploy **network monitoring software** to identify abnormal traffic spikes

	● Use **IDS/IPS systems** to detect suspicious packet characteristics and patterns ● Enable **firewall and router logging** for ICMP and high-volume traffic events ● Implement **alerting thresholds** to notify security teams of unusual traffic behavior ● Regularly review logs to distinguish between authorized and unauthorized traffic Improved detection allows security teams to identify DoS attacks early and respond before services are fully disrupted.
Respond	For future cybersecurity incidents, the organization should follow a structured response plan: ● **Containment:** ○ Immediately block malicious traffic at the firewall ○ Isolate affected network segments if necessary ● **Neutralization:** ○ Apply rate limiting and filtering rules ○ Disable unnecessary services during active attacks ● **Analysis:** ○ Review traffic logs, IDS alerts, and firewall records ○ Identify attack patterns and sources ● **Communication:** ○ Notify internal IT teams and management ○ Provide updates to affected employees as needed ● **Improvements:** ○ Update incident response playbooks ○ Conduct post-incident reviews to refine response procedures

	A documented response plan ensures faster, more consistent handling of future incidents.
Recover	To restore normal operations and improve recovery capabilities, the following steps should be taken: ● Restore all **network services** to normal operational status ● Verify **network stability and performance** after mitigation ● Confirm that firewall, IDS/IPS, and monitoring tools are functioning correctly ● Review and update **backup and recovery procedures** for network configurations ● Communicate system restoration status to internal stakeholders Recovery efforts should focus not only on restoring services but also on validating that vulnerabilities have been addressed to prevent recurrence.

Reflections/Notes:This incident highlights the importance of **proactive network hardening, continuous monitoring, and structured incident response planning**. Applying the NIST CSF enabled the organization to analyze the incident systematically and integrate lessons learned into a broader cybersecurity strategy.