Incident report analysis

Prepared By: Dhyanam

Role: Cyber Security Student (Learning)

Year:2026

Summary	Yesterday, the organization experienced a DoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the 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.
Identify	On investigating, the team 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 denial of service (DoS) attack.
Protect	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. • Regular firewall configuration reviews to prevent future misconfigurations.
Detect	To improve the detection capabilities, the security team has implemented following measure: • Network monitoring software to detect abnormal traffic patterns

	• An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Respond	The incident management team responded by blocking incoming ICMP packets and stopping all non-critical network services offline, and restoring critical network services. The team also documented all actions taken during the incident for post-incident analysis.
Recover	• Restored all non-critical services after confirming the network was stable. • Verified firewall configuration changes. • Monitored traffic post-incident to ensure no recurring attack.

Reflections/Notes:

- The incident highlighted the need for regular firewall audits.
- The response team acted quickly, minimizing the downtime.
- There is a need for better baseline traffic monitoring.
- This incident also showed the importance of documenting firewall configuration.