Incident Scenario – ICMP DDoS Attack on Internal Network

Organization:

A medium-sized multimedia company specializing in web design, content marketing, and client hosting services.

Scenario:

On a Wednesday morning, employees began reporting issues accessing internal services:
- Internal email was unresponsive
- Shared drives were inaccessible
- Network printers failed to respond

The IT helpdesk escalated the issue, and the security team launched an investigation. Over the course of the next two hours, multiple systems remained offline or extremely slow. Network monitoring logs revealed an unusual spike in ICMP traffic, specifically a high volume of Echo Request packets.

Upon further analysis, the team confirmed the company was experiencing a Distributed Denial of Service (DDoS) attack — specifically an ICMP Flood. It appeared that the attack was originating from multiple spoofed IP addresses, taking advantage of unconfigured or outdated firewall rules.

Summary:

This incident prompted a full review of the organization's network hardening posture, and the security team responded using the NIST Cybersecurity Framework.