Incident Report Analysis

Framework: NIST Cybersecurity Framework (CSF)

Incident Type: Distributed Denial of Service (DDoS) - ICMP Flood

Company Type: Multimedia (Web Design, Marketing)

Summary

Our internal network was compromised for two hours due to a DDoS attack involving a flood of ICMP packets. During the attack, employees reported failures with email, shared drives, and printing. The incident management team responded by blocking ICMP traffic and bringing critical services back online. An investigation revealed that the attacker exploited an unconfigured firewall, allowing overwhelming ICMP traffic into the network. Remediation steps included firewall rule updates, IP verification, monitoring enhancements, and IDS/IPS deployment.

Identify

The team discovered that outdated firewall rules and an unconfigured firewall allowed the ICMP flood attack. IP spoofing protections were not in place, and the network monitoring tool had not been updated, limiting its effectiveness. These vulnerabilities collectively allowed the attacker to disrupt internal services.

Protect

The following protections were implemented:
- Firewall rule to rate-limit ICMP packet intake
- Source IP verification to identify spoofed packets
- Updated and reconfigured network monitoring software
- IDS/IPS system to filter malicious ICMP traffic

Detect

To strengthen detection capabilities:
- IDS/IPS was deployed to flag suspicious ICMP patterns
- Firewall rules now detect and log excessive ICMP rates
- Network monitoring tools were updated for real-time anomaly detection
- IP spoofing detection now alerts security teams automatically

Respond

We trained the security team on patching and incident response protocols. A revised response playbook includes:

- Immediate ICMP filtering upon abnormal detection
- Isolation of affected systems
- Communication procedures for internal stakeholders
- Post-incident logging and analysis procedures

Recover

Full network operations were restored, and business services resumed. Critical systems were tested for stability. The firewall was reconfigured, and staff were briefed on the new security controls and post-incident recovery steps.

Prepared by: Charles J. Wasson