

Portfolio piece #2. Use the NIST cybersecurity frameworks to respond.

Summary

On April 15, 2025, a multimedia company experienced a Distributed Denial of Service (DDoS) attack that overwhelmed its network with ICMP traffic, taking internal services offline for around two hours. The attack took advantage of a firewall that hadn't been properly configured, allowing too much ICMP traffic through. The issue was resolved by blocking ICMP traffic, turning off non-critical services, and restoring essential systems. Since the incident, the company has improved its firewall rules, added ICMP filtering, and implemented better monitoring tools.

Identify

Attack Type: DDoS using ICMP flood

Source: External attacker exploiting an unconfigured firewall

Impacted Systems: Entire internal network — all services temporarily disrupted

Vulnerabilities: Firewall misconfiguration, no traffic limits, no monitoring tools

Security Gaps: ICMP not filtered, IP sources not verified, weak threat detection

Protect

Configure firewalls to block or limit ICMP and other unnecessary traffic

Add IP source verification to catch spoofed packets

Use Multi-Factor Authentication (MFA) for remote admin access

Perform regular firewall checks and updates

Train staff on basic network security practices

Detect

Use tools like Wireshark, NetFlow, or Zeek to detect unusual ICMP activity

Install IDS/IPS systems to identify and react to threats

Enable firewall logs and use SIEM tools for real-time alerts

Set traffic baselines to spot abnormal behavior

Monitor login and device activity to flag suspicious access

Respond

Blocked all ICMP traffic and isolated affected parts of the network

Shut down unnecessary services to free up network resources

Ran a forensic analysis of the attack

Documented what happened and how it was handled

Updated the response plan based on lessons learned

Notified stakeholders and clients as needed

Recover

Restored services in stages, starting with the most critical

Verified systems weren't tampered with during the attack

Applied firewall updates and confirmed proper setup

Reviewed and revised the disaster recovery plan

Planned follow-up audits and penetration tests

Reflections/Notes

This attack highlighted serious gaps in the company's firewall setup and monitoring. By applying the NIST Cybersecurity Framework, the company is now better equipped to catch and handle similar threats going forward.