Incident Report Analysis

Summary

A DDoS attack using ICMP packets disrupted the organization's network for two hours. The attack exploited an unconfigured firewall, allowing a flood of ICMP traffic to overwhelm internal services. Critical services were restored after blocking ICMP packets and implementing emergency responses.

Identify

- Conduct regular audits of firewalls, open ports, and access controls
- Maintain updated asset inventory and network diagrams
- Review user access privileges to apply the principle of least privilege
- Evaluate third-party services for potential vulnerabilities

Protect

- Apply firewall rules to limit or block unnecessary ICMP traffic
- Implement rate-limiting and source IP validation on the firewall
- Provide staff training on recognizing and reporting DDoS indicators
- Disable unused network services and secure protocol configurations
- Ensure timely patching of systems and network appliances

Detect

- Deploy network monitoring tools to track traffic volume and patterns
- Use IDS/IPS to detect and flag unusual ICMP or DDoS-related behavior
- Set up automated alerts for traffic anomalies and protocol misuse
- Regularly review logs for early indicators of malicious activity

Respond

- Follow a defined DDoS response plan to contain and mitigate attacks
- Temporarily disable non-critical services to preserve network stability
- Update firewall and IPS configurations based on attack analysis

- Document the event and communicate actions to relevant teams

Recover

- Restore critical services and gradually bring non-critical systems online
- Reapply saved firewall and network configurations if altered
- Conduct a post-incident review to strengthen future defenses
- Update the business continuity plan with lessons learned

Reflections/Notes:

This incident highlights the importance of proactive firewall configuration, real-time traffic monitoring, and a clear incident response strategy. Regular reviews of security policies and technical safeguards are critical to defending against similar threats.