Incident report analysis

Summary	A Distributed Denial of Service (DDoS) attack occurred targeting our internal network. The attacker used a flood of ICMP packets to overwhelm the system through an unconfigured firewall. As a result, all internal network services were inaccessible for approximately two hours. The issue was resolved by blocking ICMP packets and restoring critical services.
Identify	• **Attack Type:** ICMP Flood – a form of DDoS. • **Vulnerability:** Unconfigured firewall allowed external ICMP traffic. • **Systems Affected:** Entire internal network – no services were accessible during the incident.
Protect	**List protective measures taken :** • **Apply firewall rules to restrict ICMP packet rate.** • **Enable source IP verification to block spoofed IPs.** • **Conduct regular vulnerability scans and firewall audits.** • **Establish network segmentation to isolate internal systems.** • **Train staff on cybersecurity awareness.**
Detect	• Install **Network Monitoring Software** (e.g., Wireshark, Zeek).

	• Deploy **IDS/IPS systems** (like Snort, Suricata) to detect abnormal ICMP traffic. • Enable **SIEM tools** (e.g., Splunk, ELK) for log aggregation and anomaly detection. • Monitor for **unusual bandwidth usage** or spikes.

Respond	• Set up an **Incident Response Plan (IRP)**.
	• Regular **tabletop exercises** with IR team.
	• Maintain a **runbook** for immediate response steps:
	  ○ Identify and block malicious traffic.
	  ○ Notify internal teams.
	  ○ Isolate affected systems.
	  ○ Log all details for forensics.

Recover	• Restore critical systems and services with **backups**. • Patch firewall vulnerabilities. • Document incident in a **Post-Incident Review Report**. • Update policies based on lessons learned. • Revalidate network integrity using **health checks**.

Reflections/Notes: