Incident report analysis

Summary	The organization experienced a Distributed Denial of Service (DDoS) attack using ICMP packet floods, which overwhelmed the internal network and caused a complete outage for two hours. The attacker exploited a misconfigured firewall that allowed ICMP packets from any source IP. As a result, normal business operations were halted. The incident was mitigated by blocking ICMP traffic, stopping non-critical services, and implementing additional firewall and monitoring rules.
Identify	The type of attack was a Distributed Denial of Service (DDoS) via ICMP flood. The attack exploited a misconfigured firewall that allowed excessive inbound ICMP packets. This attack impacted all internal systems by halting communication, blocking access to shared resources, and disabling normal network traffic. The estimated business impact includes 2 hours of downtime, potential data loss from interrupted sessions, and reduced customer trust.
Protect	To prevent similar incidents in the future, firewall configurations must be reviewed regularly to ensure unnecessary protocols like ICMP are blocked unless explicitly needed. Limit incoming ICMP packet rate. Enforce secure firewall baseline configurations. Train staff on firewall management best practices. Policies should also be updated to ensure periodic security audits are performed and that default configurations are never left unchanged in production environments.
Detect	Use network monitoring software (such as Wireshark, Zeek, or Suricata) to observe traffic behavior and set alerts for unusual spikes, especially related to ICMP. Implement a centralized SIEM solution to aggregate and analyze logs. Intrusion Detection and Prevention Systems (IDS/IPS) can help identify patterns of DDoS activity. Continuous monitoring of firewall logs will enable real-time detection of flooding behavior or spoofed IPs.

Respond	In the event of a DDoS or similar attack, the organization should: - Immediately block offending traffic at the firewall or router level - Use IP spoofing filters and rate-limiting - Stop non-critical services to prioritize essential operations - Notify stakeholders and log all incident details - Perform forensic analysis to understand the attack vector Post-incident review should result in improved firewall rules, better documentation, and updated incident playbooks.
Recover	Recovery actions include restarting previously halted services, restoring access to internal resources, and validating firewall integrity. Network and server logs should be backed up and reviewed. Conduct a full system audit to confirm no residual malware or vulnerabilities. Ensure communication with clients and internal teams to provide transparency. Lessons learned should be used to improve future response and hardening protocols.

Reflections/Notes: Credential misuse and DDoS combined increased incident complexity & hardening firewall rules and user awareness training are now essential.