Incident report analysis

Summary	A distributed denial-of-service (DDoS) attack using a flood of ICMP packets overwhelmed the company's internal network for two hours, causing network services to become unresponsive. The attack exploited an unconfigured firewall vulnerability, allowing malicious ICMP traffic to flood the network. The incident was mitigated by blocking ICMP packets, taking non-critical services offline, and restoring critical services. Post-incident, firewall rules were updated, and monitoring and intrusion detection/prevention systems were implemented to prevent recurrence.
Identify	• Technology/Asset Management: The attack targeted the internal network infrastructure, specifically exploiting an unconfigured firewall that allowed unchecked ICMP traffic. Network devices, firewalls, and critical servers were affected as normal traffic was blocked by the flood. • Process/Business Environment: The attack disrupted web design, graphic design, and social media marketing services, impacting business operations and client deliverables. • People: Network administrators, cybersecurity team members, and incident response personnel require access to affected systems for mitigation and recovery.
Protect	• Access Control: Implemented firewall rules to limit ICMP packet rates and verify source IP addresses to block spoofed traffic. • Awareness/Training: The Cybersecurity team and relevant staff

	were informed about the attack vector and trained on new firewall configurations and monitoring tools. ● Data Security: No direct data breach was indicated, but network availability was compromised. ● Information Protection and Procedures: Updated firewall configuration policies and incident response procedures to address DDoS threats. ● Maintenance: Regular audits and firewall configuration reviews are scheduled to prevent similar vulnerabilities. ● Protective Technology: Deployed IDS/IPS systems to filter suspicious ICMP traffic and network monitoring software to detect abnormal traffic patterns early.
Detect	● Anomalies and Events: Network monitoring software was introduced to detect unusual ICMP traffic spikes indicative of DDoS attacks. ● Security Continuous Monitoring: Continuous monitoring of network traffic patterns to alert security staff of potential flooding or other anomalies. ● Detection Process: IDS/IPS systems are configured to identify and block suspicious ICMP packets based on traffic characteristics and source verification.
Respond	● Response Planning: Established action plans to immediately block malicious traffic, isolate affected network segments, and restore critical services. ● Communications: Incident response team coordinated internally

	and communicated status updates to management and affected users promptly. ● Analysis: Post-incident forensic analysis identified the root cause as an unconfigured firewall allowing ICMP floods. ● Mitigation: Blocking ICMP packets, taking non-critical services offline to reduce load, and applying firewall rules to limit traffic. ● Improvements: Implemented stricter firewall policies, source IP verification, and enhanced monitoring to improve response to future attacks.
Recover	● Recovery Planning: Restored normal network operations by removing blocks on legitimate traffic once the attack subsided and verifying system integrity. ● Improvements: Updated recovery procedures to include rapid deployment of firewall rules and monitoring alerts for faster mitigation. ● Communications: Communicated recovery status to stakeholders and ensured all systems were verified secure before resuming full services.

Reflections/Notes: This incident highlights the critical importance of properly configured firewalls and continuous network monitoring to defend against volumetric DDoS attacks. Applying the NIST CSF framework helped structure the response and remediation efforts, ensuring comprehensive coverage from risk identification to recovery. Ongoing training and policy updates are essential to maintain resilience against evolving threats.