Incident report analysis

Summary	Our organization recently experienced a Distributed Denial-of-Service (DDoS) attack originating from external sources, specifically flooding the network with ICMP packets. This targeted our internal network infrastructure, overwhelming resources and causing a complete outage where normal internal traffic could not access any network resources or services. The impact was a two-hour service disruption affecting all internal operations. The Incident Management Team responded by blocking incoming ICMP packets at the perimeter, taking all non-critical network services offline to conserve resources, and subsequently restoring critical network services, resolving the incident.
Identify	After investigating we found that the vulnerability in our network was an unconfigured firewall. Which allowed the malicious attacker to overwhelm the company's network through a DDoS attack. This resulted in complete disruption of internal services for two hours, halting web/graphic design workflows, social media campaigns, and client communications.
Protect	The team implemented a new rule to the firewall to limit the number of incoming ICMP requests to prevent the server from being flooded again. Implemented network monitoring software to flag abnormal traffic patterns. IDS/IPS deployment to block suspicious ICMP characteristics.
Detect	Used source IP address verification for anti-spoofing checks on all

	inbound ICMP traffic
Respond	During the attack, the team immediately blocked all incoming ICMP packets to halt the flood, took non-critical services offline to preserve bandwidth, and restored critical operations within two hours; post-incident, we implemented new firewall rules (rate limits/anti-spoofing) and deployed an IDS/IPS.
Recover	To restore operations immediately, we need verified backups of active client design projects and hardened configurations for firewalls; our recovery processes include prioritizing critical systems validating network stability for 1 hour before reactivating non essential services followed by client notifications via backup channels (email/SMS) regarding delayed deliverables, root-cause analysis of the firewall misconfiguration within 48 hours, and quarterly DDoS simulation drills to refine resilience.

Reflections/Notes: