Incident report analysis

Summary	Our company faced a Distributed Denial of Service (DDoS) attack, which lasted for approximately two hours. Due to a flood of incoming ICMP packets, our organization's network services stopped responding, hindering regular network traffic operations. It resulted in interruption of critical business operations like web design services, graphic design, and social media marketing solutions that are being provided to clients. This incident occurred due to an unconfigured firewall, which allowed the attacker to take advantage of this activity and flood the company's network with ICMP packets unchecked using spoofed IP addresses.The incident was then mitigated by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The type of attack was Distributed Denial of Service (DDoS) attack, carried out by flooding the company's network system with ICMP packets. Targeted systems included internal network devices and critical network services used for business operation. The vulnerability that caused exploitation was a misconfigured firewall mainly due to lack of ICMP packets filtering and source IP address verification. The estimated impact was 2 hours of network downtime, loss of business productivity and possible reputational harm.
Protect	To secure the organization's network and prevent further risk immediate actions were taken such as configuration of firewall's rule to limit ICMP traffic and verify source IP address. Network monitoring system as well as an IDS/IPS system to filter out suspicious ICMP traffic were also installed.
Detect	In order to detect similar threats in future, continuous network monitoring tools will be used to identify unusual traffic patterns like spikes in ICMP packets. An

	Intrusion Detection/Prevention System (IDS/IPS) will be deployed to flag and block suspicious ICMP as well as other abnormal packets.
Respond	If a security event happens in the future, the cybersecurity team will immediately isolate the affected systems to stop the problem from spreading then, making sure that the systems and services are backed up and running. After that, they will review network logs for anything unusual or suspicious. They will also make sure to report the incident to upper management and legal authorities, if needed.
Recover	To recover from a DDoS attack caused by ICMP flooding, the main priority is to restore network services to normal operations. In the future, external ICMP flood attacks can be mitigated by blocking them at the firewall. During recovery, all non-essential network services should be temporarily shut down to minimize internal network traffic. Critical services should be restored first. Once the flood of ICMP packets has stopped, non-critical systems and services can be gradually brought back online.

Reflections/Notes: The incident highlighted the importance of proper firewall configurations and an IDS/IPS system to filter out some ICMP traffic. Implementing additional protective measures and conducting staff training will be crucial to strengthening our defense against future DDoS attacks and similar threats.