Incident report analysis

Summary	A multimedia company offering web design, graphic design, and social media marketing solutions fell victim to a Dedicated Denial of Service (DDoS) attack, which flooded the server with ICMP packets. This caused the network to be offline for 2 hours and in response, the incident management team blocked all ICMP packets and took non-critical network services offline. An investigation revealed that the attack exploited an unconfigured firewall, allowing a flood of ICMP pings to overwhelm the system. Following the attack, the network security team implemented several measures to prevent a recurrence, including limiting the rate of ICMP packets, spoofed IP checking, deploying network monitoring for traffic anomalies, and using an Intrusion Detection and Prevention System (IDS/IPS) to filter ICMP traffic.
Identify	The incident management team audited the systems involved in the attack to identify gaps in security. Maintain an updated inventory of all network assets, including firewall configurations and internal network resources. The team found out that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured wirewall.
Protect	The team can Implement stricter access control measures, including more granular firewall configurations, to prevent unauthorized traffic. Limit ICMP packet rates and configure firewall rules to automatically drop excessive packets. Also segregate the network into segments based on data and criticality, ensuring essential resources can remain operational even under an attack. Finally, educate employees and train them about DDoS attack patterns and best practices for dealing with situations.

Detect	For the future, the team will use an Intrusion Detection and Prevention System (IDS/IPS) to actively monitor and block suspicious or excessive ICMP packets. SIEM tools can also be utilized to monitor log data and send custom alerts on potential threats.
Respond	The team responded by blocking all incoming ICMP packets. Create a DDoS-specific playbook which features step-by-step guidelines for identifying, isolating, and mitigating DDoS traffic. Finally, communicate the incident to stakeholders and assure them about recovery efforts.
Recover	Following the attack, apply lessons learned to make feasible improvements in firewall configurations and monitoring solutions to better withstand future DDoS attacks. Document the incident, lessons, and insights to improve accountability.