Incident report analysis

Summary	During the event, the organization's network services were inaccessible and has stopped responding due to an incoming flood of ICMP packets. The company's cybersecurity team has investigated the event and found that a malicious actor has sent the attack, sending ICMP pings into the company's network through an unconfigured firewall. This has impacted the organization's business operations, which includes web design services, graphic design and social media marketing solutions, inaccessible. The cybersecurity team has restored the network services by blocking any incoming ICMP packets, stopping all non-critical network services offline and restoring critical networks. In conjunction with network security team, they implemented the following: ● A new firewall rule to limit the rate of incoming ICMP packets ● Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets ● Network monitoring software to detect abnormal traffic patterns ● An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Identify	The incident management team has identified that the attacked occurred when a malicious actor had sent a flood of ICMP pings to an unconfigured firewall. This allowed the actor to exploit the network through a distributed denial of service (DDos) attack.

Protect	To safeguard the organization's assets, an immediate response strategy involves implementing port hardening by disabling all unused network ports, thereby reducing the risk of unauthorized access. Additionally, firewall policies should be updated and tightened to mitigate potential threats such as ICMP ping floods, which can be used in denial-of-service (DoS) attacks.
Detect	To monitor and respond to suspicious ICMP traffic from non-trusted IPs, a combination of IPS and NGFW is ideal. IDS can be layered in for visibility, while SIEM helps correlate and investigate incidents across the network.
Respond	As improvements to the security process, the team has implemented new firewall rule to limit the rate of incoming ICMP packets. Network monitoring software is also added to detect abnormal traffic patterns. An IDS/IPS system is also in place to filter out some ICMP traffic based on suspicious characteristics.
Recover	Recovery involves restoring to normal operations while ensuring the threat is fully contained. A document playbook should outline roles, steps and escalation process. Focus on restoring IT infrastructure and operations. A formal debrief to analyse root causes and improve defenses.

Reflections/Notes:

In conclusion, the organization deployed a firewall in the production environment without proper configuration or safeguards, which allowed a malicious actor to exploit the network through an ICMP flood attack. By fully implementing the recommended security measures, the organization can enhance its overall security posture and significantly lower the likelihood of similar incidents occurring in the future.