ICMP DoS Attack Scenario (Training Simulation)

You are a cybersecurity analyst working for a multimedia company that provides web design, graphic design, and social media marketing services to small businesses. The organization experienced a Denial of Service (DoS) attack that disrupted the internal network for nearly two hours. During the incident, network services stopped responding due to a large volume of incoming ICMP packets. Normal internal traffic was unable to access network resources. The incident management team responded by blocking incoming ICMP traffic, stopping non-critical services, and restoring critical network operations. Following the response, the cybersecurity team investigated the incident and discovered that a malicious actor exploited an unconfigured firewall to flood the network with ICMP packets. This vulnerability allowed the attacker to overwhelm the network. To prevent future incidents, the security team implemented ICMP rate-limiting firewall rules, enabled source IP address verification to detect spoofed traffic, deployed network monitoring tools, and implemented an IDS/IPS to filter suspicious ICMP traffic. This scenario is part of the Google Cybersecurity Analyst Certificate and is intended for educational and portfolio purposes only.