Incident report analysis

Instructions

Summary	The organization experienced a sudden stop in network services due to DDoS ICMP flood attack, which were admitted through an unconfigured firewall. The security team responded by adding ICMP rate limiting, source IP verification, traffic monitoring, and an IDS/IPS to filter suspicious ICMP traffic.
Identify	Assets affected were the internal network services, where the main exploited vulnerability was an unconfigured firewall that allowed unrestricted ICMP traffic which compromised the internal network for two hours.
Protect	The team implemented firewall rate-limiting for ICMP packets & IDS/IPS to analyze and block suspicious ICMP traffic.
Detect	The team implemented source IP verification to check for spoofing, as well as the implementation of network monitoring tools to detect anomalies.
Respond	The cybersecurity team will contain and neutralise the attack by isolating affected systems. They will then analyze the incident by reviewing network logs for suspicious activity and report their findings to senior management and relevant stakeholders.
Recover	External ICMP flood traffic should be blocked at the firewall to prevent recurrence. Recovery should prioritise restoring critical services first, therefore non-critical services should be shut down temporarily to reduce internal network traffic. Once the ICMP flood subsides, all remaining non-critical systems and services can be safely brought back online.