

Incident report analysis

Completed by Chidubem Onochie-Onyetenu

Summary	The company experienced a security event in which all network services suddenly stopped responding for two hours. The cybersecurity team found that the disruption was caused by a distributed denial of service (DDoS) attack: a flood of incoming Internet Control Message Protocol (ICMP) packets sent through an unconfigured firewall. The incident management team responded by blocking the incoming ICMP packets and taking all non-critical network services offline so that critical network services could be restored.
Identify	A malicious actor or actors targeted the company with an ICMP flood attack, taking advantage of an unconfigured firewall. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state.
Protect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets, and an intrusion detection and prevention system (IDS/IPS) to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team configured source Internet Protocol (IP) address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, and implemented network monitoring software to detect abnormal traffic patterns.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network and attempt to restore any critical systems and services that were disrupted. The team will then

	analyze network logs to check for suspicious and abnormal activity, and report all incidents to upper management and, where applicable, the appropriate legal authorities.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services must be restored to normal functioning. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic, and critical network services should be restored first. Finally, once the flood of ICMP packets has timed out, all non-critical network systems and services can be brought back online.