



Incident report analysis - Nov 21, 2025.

Summary	<p>The multimedia company experienced a Distributed Denial of Service (DDoS) attack that compromised the internal network for two hours. The attack was executed via an incoming flood of ICMP packets which overwhelmed the network, causing all network services to suddenly stop responding and blocking access to internal resources. Investigation by the cybersecurity team identified the core vulnerability as an unconfigured firewall that allowed the malicious actor to launch the DDoS attack. The immediate response involved blocking the incoming ICMP packets, stopping all non-critical network services, and restoring critical services. To prevent recurrence, the team implemented a new firewall rule to limit ICMP packet rates, source IP address verification, network monitoring software, and an IDS/IPS system to filter suspicious ICMP traffic.</p>
Identify	<p>A malicious actor targeted the entire internal network with an ICMP flood. All critical network resources were affected and needed to be secured and restored. Future action must include regular audits of network systems, devices, and firewall configurations to proactively identify potential gaps in security.</p>
Protect	<p>To mitigate recurrence, the network security team implemented a new firewall rule to limit the rate of incoming ICMP packets. They also implemented an IDS/IPS system to filter suspicious ICMP traffic based on suspicious.</p>

	<p>SOME ICMP TRAFFIC BASED ON SUSPICIOUS characteristics. New policies and training must be established for system maintenance and firewall configuration review to prevent future unconfigured systems.</p>
Detect	The team configured source IP address verification on the firewall to check for spoofed IP addresses. They also implemented network monitoring software to detect abnormal traffic patterns. These tools allow the system to continuously monitor the network for security events and increase the speed and efficiency of detections.
Respond	For future security events, the cybersecurity team must have a plan to isolate affected systems to prevent further disruption (Mitigation). The team will analyze network logs to thoroughly check for suspicious activity (Analysis). All incidents will be reported to upper management and, if legally required, to appropriate authorities (Communications).
Recover	Access to network services needs to be restored to a normal functioning state. The recovery plan will prioritize restoring critical network services first, followed by non-critical network services once the ICMP flood traffic has timed out. The organization must establish clear communication procedures to keep end-users informed of service restoration updates.