Incident report analysis

Summary	The organization encountered a security incident characterized by an abrupt cessation of network services. Upon investigation, our cybersecurity experts identified the disruption as a result of a distributed denial of service (DDoS) attack, initiated through an inundation of incoming ICMP packets. In response, our team swiftly mitigated the attack by implementing countermeasures, which included halting all non-essential network services to prioritize the restoration of critical network functionality.
Identify	The company fell victim to a malicious individual or group who executed an ICMP flood attack, causing widespread disruption across the internal network. As a result, the cybersecurity team had to prioritize the safeguarding and recovery of all critical network assets to ensure their return to operational status.
Protect	The cybersecurity team proactively fortified the network defenses by introducing a novel firewall rule that restricts the rate of incoming ICMP packets and deployed an Intrusion Detection System/Intrusion Prevention System (IDS/IPS) to scrutinize and filter out ICMP traffic displaying suspicious attributes.
Detect	The cybersecurity team bolstered security measures by configuring source IP address validation on the firewall to scrutinize incoming ICMP packets for any signs of spoofed IP addresses. Additionally, they deployed network monitoring software to actively identify and flag abnormal traffic patterns within the network.
Respond	In anticipation of future security incidents, the cybersecurity team has devised a comprehensive strategy. Their approach involves isolating impacted systems to curtail any potential network-wide disruptions. Subsequently, the team will endeavor to reinstate critical systems and services that may have been affected during the incident. Following this, a meticulous examination of network logs will be conducted to uncover any traces of suspicious or abnormal activity. Additionally, all incidents will be diligently reported to senior management and, if deemed necessary, to the relevant legal authorities.
Recover	In the aftermath of a DDoS attack orchestrated through ICMP flooding, the paramount objective is to reinstate network services to their standard operational state. To proactively safeguard against potential future external ICMP flood attacks, the cybersecurity strategy involves fortifying the firewall's capabilities to thwart such threats. When confronted with a DDoS incident, the recovery plan unfolds methodically: first, the temporary cessation of all

	non-critical network services mitigates internal network congestion. Subsequently, critical network services are prioritized for restoration as the initial phase of recovery. Finally, once the deluge of ICMP packets has naturally timed out, the gradual reactivation of non-critical network systems and services takes place. This systematic approach not only facilitates swift recovery but also bolsters defenses against future ICMP flood attacks, all while minimizing the disruption to essential network operations.

Reflections/Notes: