Incident report analysis

Instructions

Summary	The multimedia company experienced a DDoS attack which resulted in the network being compromised for two hours. The incident was resolved by blocking incoming ICMP packets, halting non-critical network services, and restoring critical services. Investigation showed that a malicious actor initiated a flood of ICMP pings through an unconfigured firewall, causing a DDoS attack. Mitigation measures were implemented, including new firewall rules, source IP address verification, network monitoring software, and an IDS/IPS system.
Identify	The attack affected various hardware devices, operating systems, and software within the internal network. Business processes related to network services and communications were impacted by this attack. Authorized personnel requiring access to affected systems must be identified about the attack while the cybersecurity team investigates.
Protect	To protect against future attacks, access control measures were improved, including source IP address verification and access restriction. Data security measures were reviewed, and more protective technologies were considered for implementation.
Detect	Configured source IP address verification on the firewall to identify and block spoofed IP addresses used by attackers to disguise their origins. Deployed network monitoring software capable of identifying abnormal traffic patterns, enabling early detection and response to suspicious activities.
Respond	The cybersecurity team will implement isolation measures to contain affected systems and prevent further disruption to the network. Immediate efforts will focus on restoring critical systems and services that were impacted by the event. Following restoration, the team will conduct a thorough analysis of

	network logs to identify any suspicious or abnormal activity indicative of ongoing threats. Additionally, all security incidents will be reported to upper management and any relevant legal authorities, as necessary.
Recover	In the aftermath of a DDoS attack caused by ICMP flooding, the first objective is to restore network services to a normal functioning state. Implement proactive measures at the firewall to block external ICMP flood attacks, fortifying the network against similar incidents in the future. Temporarily halt all non-critical network services to help with internal network traffic and prioritize resource allocation for critical systems. Focus on restoring critical network services promptly to minimize operational disruptions and ensure essential functionalities are available to users. Once the flood of ICMP packets has subsided, systematically bring back online non-critical network systems and services in a phased approach to mitigate the risk of reoccurrence.

Reflections/Notes: The incident shows the importance of proactive cybersecurity measures, including regular audits, access control, and continuous monitoring. Implementing the NIST CSF framework can help organizations effectively manage cybersecurity risks and respond to security incidents promptly. Ongoing review and updates to security strategies are essential to staying ahead of evolving threats.