Incident report analysis

Summary	The organization faced a Distributed Denial of Service (DDoS) attack that disrupted network services for two hours. The attack involved a surge of ICMP pings bypassing an unconfigured firewall, causing the network to become overwhelmed. In response, the cybersecurity team introduced enhanced security measures to prevent future incidents.
Identify	The attack was a DDoS attack utilizing ICMP packets, which disrupted the internal network for two hours. The organization's firewall was unconfigured, likely making it easier for malicious actors to execute the attack.
Protect	The network security team has added a new firewall rule to limit the rate of incoming ICMP packets, addressing the cause of the outage. They have also enhanced the firewall configuration to verify source IP addresses, helping to prevent spoofed IP addresses in incoming ICMP packets. Additionally, an Intrusion Detection/Prevention System (IDS/IPS) has been implemented to monitor and filter suspicious network activity.
Detect	To detect and prevent future attacks, the organization will utilize firewall logging tools and an IDS to monitor all incoming network traffic from external IP addresses. Additionally, the organization should consider implementing a Security Information and Event Management (SIEM) tool for real-time monitoring and alerts.
Respond	The network security team has updated firewall and security rules to detect and mitigate ICMP floods and similar request flood attacks. The affected firewall has been reconfigured with robust security settings, aligning with the baseline configuration. All security personnel have been informed about the cause, response, and outcome of the attack. Upper management has been

	briefed on the incident and will coordinate with content teams to notify customers about the outage. Additionally, management will work with law enforcement and other relevant organizations as mandated by local regulations.
Recover	The affected server has been reset to its baseline configuration and is now fully operational. All data and assets impacted by the incident have been restored from the most recent backup. The network security team's configuration updates should now block future ICMP flood attacks at the firewall. Next, non-critical network services should be identified and paused to minimize internal traffic. Critical network services should be prioritized for restoration. Once the ICMP packet flood subsides, non-critical services can be brought back online.

Reflections/Notes: