Incident report analysis

Summary	Our company experienced a DDoS attack in which a flood of ICMP pings exploited an unconfigured firewall, overwhelming the network and disrupting services for two hours. The cybersecurity team resolved the incident by blocking ICMP traffic and temporarily disabling non-critical services. To prevent future occurrences, they implemented a series of improvements, including firewall updates, source IP verification, network monitoring, and an IDS/IPS system.
Identify	The team determined that the unconfigured firewall allowed a flood of ICMP packets, enabling the DDoS attack. The malicious actor exploited the lack of rate-limiting and source verification, overwhelming the network. The team identified which internal systems were impacted to prioritize restoration efforts. The team noted the unconfigured firewall and absence of detection tools as primary gaps in the network's security.
Protect	Implemented rate-limiting on incoming ICMP packets to prevent similar floods, configured the firewall to verify source IP addresses to block spoofed packets, installed and configured an Intrusion Detection and Prevention System to filter and block suspicious ICMP traffic, enhanced internal security policies to include regular reviews of firewall configurations and rule updates.
Detect	Set up software to track and analyze traffic patterns, enabling early detection of anomalies like DDoS attacks. Programmed the IDS/IPS to recognize and flag unusual ICMP traffic characteristics. Configured automated alerts to notify the team of potential attacks, ensuring a faster response time.

	Analyzed historical data to refine detection mechanisms and establish baseline traffic patterns for comparison.
Respond	As an immediate measure, halted all ICMP packets at the firewall to stop the attack. Temporarily disabled non-essential services to focus on restoring primary operations. Worked in coordination with the incident response team to contain and neutralize the attack. Recorded all actions taken during the response phase to improve future procedures and training.
Recover	Reconfigured and restarted essential systems once the attack was mitigated. Addressed the exploited vulnerability by updating firewall settings and rules. Integrated network monitoring tools and IDS/IPS systems to detect and mitigate threats proactively. Communicated findings across the team and leadership to strengthen organizational awareness and future readiness.

Reflections/Notes: