Incident report analysis

Summary	The company faced a security incident where all network services abruptly became unresponsive. Upon investigation, the cybersecurity team discovered that the disruption was due to a distributed denial of service (DDoS) attack involving a flood of incoming ICMP packets. To counter this, the team took action by blocking the attack and halting all non-essential network services to prioritize the restoration of critical ones.
Identify	The company's cybersecurity team investigated the security event and found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Protect	The network security team has implemented: ● A new firewall rule to limit the rate of incoming ICMP packets ● An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team configured Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and Network monitoring software to detect abnormal traffic patterns.
Respond	In preparation for future security events, the cybersecurity team plans to isolate affected systems to contain any potential disruptions to the network. They will prioritize the restoration of any critical systems and services that

	were impacted during the event. Subsequently, the team intends to scrutinize network logs for any signs of suspicious or abnormal activity. Furthermore, they will ensure that all incidents are promptly reported to upper management and, if necessary, to the relevant legal authorities.
Recover	Restoring normal functioning of network services after a DDoS attack via ICMP flooding requires a systematic approach. To mitigate future external ICMP flood attacks, the firewall should be configured to block such traffic. Priority should be given to restoring critical network services. Once the flood of ICMP packets has subsided, non-critical network systems and services can be gradually brought back online.

Reflections/Notes:

- Kushagra Gupta