Incident report analysis (multimedia company)

Summary	This morning, a multimedia company experienced what is believed to be a DDoS attack. The attack brought havoc to the internal systems of the organisation, an overwhelming amount of ICMP packets were discovered by the security analyst. The traffic was ongoing for almost 2 hours. As a result of this, the internal network could not access network resources and the system stopped responding. The team have taken decisive action by blocking all ICMP packets in the network, all non critical services were stopped, allowing only critical services to run. At this moment the team is working hard to rectify the issues. It is believed the malicious actors found a vulnerability in the firewall in which they exploited.

Identify	The incident response team reviewed the organisations systems, devices and access policies to see if there are any gaps in security. The team found out that a malicious actor managed to gain access to the network through an unconfigured firewall. After gaining access, they released an overwhelming amount of ICMP packers. Further inspection reveals, the attacker compromised the system for 2 hours, internal network devices couldn't access network resources. The organisation plans to prioritize this vulnerability by implementing new firewalls rules to limit the rate of ICMP packets, source IP address verification to prevent spoofed IP addresses, network monitoring software to detect abnormal traffic patterns and IDS/IPS to filter out some ICMP packets based on suspicious characteristics. The teams will communicate these findings and mitigation strategies to the stakeholders. The team will continue to monitor and review the risk management strategy.
Protect	The Team has implemented few systems and policies in place to safeguard the network, these are; A new firewall rule to limit the rate of incoming ICMP packets, Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, Network monitoring software to detect abnormal traffic patterns and An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To ensure the same incident doesn't happen again, the team has implemented intrusion detection system/ intrusion prevention system to stop suspicious activities, new firewall rules to block unwanted ICMP packets and network monitoring software to detect unusual network characteristics
Respond	The incident response team responded by blocking unwanted ICMP packets, stopping all non-critical services and only allowing critical services to run. The team carried out a full investigation to understand the source of the attack and have implemented further security measures to patch the vulnerability.

Recover	The incident response team has restored normal operation by implementing various systems such as new firewall rules and network monitoring software to ensure the network is safe and reliant to future attacks