Incident report analysis

Summary	A security incident just occurred at the company, where all the network services stopped responding for 2 hours. The cybersecurity team investigated, and found out that this disruption was caused due to a DDoS attack. The attack involved sending a flood of ICMP packets to the network through an unconfigured firewall. Then the company's incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services
Identify	During the incident, it was discovered by the incident management team that the malicious actor used the current firewall's configuration to send a flood of ICMP packets. Due to this, the entire internal network was affected and critical network services required to be restored to the functioning state.
Protect	In order to protect the internal network from future similar attacks, the network security team implemented: 1. A new firewall rule to limit the rate of incoming ICMP packets. 2. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	In order to detect similar security incidents in future, the network security team has implemented: 1. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets 2. Network monitoring software to detect abnormal traffic patterns
Respond	In this security event the attackers were able to disrupt all the internal network systems. Therefore, in future the cybersecurity team will try to contain the attack so it

	does not disrupt the entire network. The team will then prioritise restoring all the affected critical network services. Then the team should use the network logs to check for any other abnormal activities. Then report the incident and actions taken to deal with the incident to the management.
Recover	In-order to recover from ICMP flooding DDoS attack, the access to the network services must be restored to a normal functioning state. Due to the implementation of a new firewall control that limits the ICMP packets, in future, the firewall can be used to block all the incoming ICMP packets to the network. Then the affected critical services should be restored before other services are restored.
Govern	Upon discovery of the incident, CSIRT and CISO were immediately informed by the cybersecurity team. CSIRT responded by blocking incoming ICMP packets and contained the incident. Simultaneously, the cyber security team started investigating the incident.

Reflections/Notes: Conducting regular red team exercises which involves testing the firewall would allow the organisation to determine if the firewall requires configuration update.