Incident report analysis

Summary	The organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources.
Identify	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Protect	To address this security event, the network security team implemented: • 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 • An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	To detect similar security events in the future, the team will use the newly implemented network monitoring software and the IDS/IPS system to monitor suspicious activity coming from the internet, such as possible IP spoofing.
Respond	The team will receive appropriate training on the use of the previously mentioned software, and follow the playbook instruction on how to deal with an active cybersecurity threat.
Recover	To recover from this kind of attack, access to network services need to be

	restored to the last functioning state. Once the flood of ICMP packets have timed out, all network systems and services can be brought back online. No crucial data should have been compromised from this kind of attack.

Reflections/Notes: