Incident report analysis

Summary	The organization recently faced a DDoS attack. The attack was carried out by overwhelming the network by flooding ICMP packets. The malicious actor carried out the attack by sending malicious ICMP packets to the organization's network through an unconfigured firewall. The incident management team responded by blocking all incoming ICMP packets and shutting non-critical network services and restoring critical network services. The network security team addressed the incident by reconfiguring the firewall to filter abnormal ICMP traffic and also look out for ICMP packets coming from a spoofed IP address.
Identify	The organization faced a Distributed Denial of Service (DDoS) attack. The attack affected the organization's network services, bringing them to a halt for 2 hours and deprived the normal internal network traffic of any network resource.
Protect	In order to prevent similar types of attacks happening in future the organization’s firewalls must be reconfigured to detect malicious ICMP traffic.Source IP address verification must also be implemented to prevent malicious ICMP packets arriving from a spoofed IP address.
Detect	To prevent any similar attacks in future robust firewall configurations must be kept in place paired with strong network monitoring capabilities to filter out legitimate traffic from malicious traffic. IDS/IPS must be implemented to monitor for any malicious traffic and network monitoring software to detect abnormal traffic patterns.

Respond	To ensure the availability of the business operations in case of any similar future incident, the organization's internal network must be segmented to isolate and contain such incident and not bring the entire network down.
Recover	

Reflections/Notes: