Incident report analysis

Summary	Our security team noticed our internal network suddenly stopped to respond. After investigating our system we found that a DDOS attack had happened. A bad threat actor had compromised our internal network for two hours before protecting our system from this attack.
Identify	The security team found a malicious actor had sent a flood of ICMP pings into our internal network through an unconfigured firewall. The misconfiguration of firewall allows threat actors to overwhelm our network through a Distributed Denial of Service (DDOS) attack.
Protect	The security team implemented a new firewall rule to limit the number of incoming ICMP packets. Implemented source ip address verification on the firewall to check for spoofed ip address on incoming ICMP packets.
Detect	The security team Implemented a network monitoring tool (e.g. SIEM tools) to monitor and identify anomalies and abnormal traffic patterns into the network. Implemented IDS/IPS network security tools to detect and block some ICMP traffic based on suspicious characteristics.
Respond	The incident management team blocked incoming ICMP packets and blocked all non-critical network services offline.
Recover	Restoring critical services and back the system to normal operation again.

Reflections/Notes: