Incident report analysis

Summary	The organization's network services became unresponsive, and workers were unable to access and use the network resources they needed to perform their normal work. We are convinced that this anomaly was caused by a Distributed Denial of Service (DDoS) attack, in which the organization's servers were overwhelmed with more requests than they were able to process, thus denying service to legitimate network users.
Identify	The specific variant of this attack was an ICMP flood, in which the targeted servers are oversaturated with ICMP (Internet Control Message Protocol) packets. ICMP is commonly used as a quick way to troubleshoot network connectivity and latency by issuing a "ping". The server attempted to respond to all these messages, but with all the bandwidth used up by the attack, it was unable to process legitimate internal traffic.
Protect	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Detect	A malicious actor had sent a flood of ICMP pings to the company's network through an unconfigured firewall. This was the vulnerability that was exploited and will need to be fixed to prevent incidents of this nature in the future.
Respond	The security team took the following measures to deal with this kind of attack in the future: - A new firewall rule to limit the rate of incoming ICMP packets. - Verification of the source IP address in the firewall to check for spoofed IP addresses in incoming ICMP packets.

	- The implementation and use of event management tools to monitor the network and detect anomalous traffic patterns. - An IDS/IPS (Intrusion Detection/Protection System) to filter some ICMP traffic based on suspicious characteristics.
Recover	As mentioned above, part of the recovery strategy included (initially) blocking all ICMP packets to give the server a chance to recover its normal rate of operation. After the incident was contained, the firewall, which up to that point lacked proper configuration, was upgraded to limit the rate of incoming ICMP packets.

Reflections/Notes: