Incident report analysis

Summary	The organization experienced a security event where our network services suddenly stopped responding. This prevented our internal network traffic's normal communication processes. During our investigation the cybersecurity team discovered that an attacker sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the attacker to perform a successful distributed denial-of-service ICMP flood attack. The internal network was compromised for approximately two hours. The team temporarily shut down non-critical network services so that the critical ones could be restored.
Identify	It was discovered that an attacker was able to perform the DDoS ICMP flood attack by taking advantage of a vulnerable unconfigured firewall. The internal network was affected and unresponsive.
Protect	Our team has implemented rules to the unconfigured firewall to limit the amount of incoming ICMP packets. We have implemented source IP address verification to check for IP spoofing on incoming ICMP packets and network subnetting. We will also invest in an intrusion prevention system (IPS).
Detect	To detect suspicious and unauthorized activity in the future, we will implement an intrusion detection system (IDS) and a SIEM tool.
Respond	To respond to an incident similar to this in the future, the cybersecurity team should isolate and shut down affected systems. Then, they will restore any affected systems. Using the IDS and SIEM tool to look at logs and any suspicious activity to investigate the type of attack and where it originated. After, they will report to upper management to inform them of said incident.

Recover	To recover from a DDoS ICMP flood attack, the network has to be restored to its normal functions. Since the firewall is now configured to block external ICMP packets, there should be less of an attack surface. If needed, shut down non-critical network services. Allow the ICMP packets to reach the end of its TTL. Wait for critical network services to run at normal speeds. Then, bring back any previously shut down network services.

Reflections/Notes: Make sure that if any new firewall is introduced, that it does not remain unconfigured during its initial setup.