Incident report analysis

Summary	Recently, a DoS attack has affected the organization. During this attack, ICMP packets flooded the network, through an unconfigured firewall. This allowed a DDoS attack to overwhelm the organization's systems and cause business operations to stop for two hours.
Identify	An unconfigured firewall led to a DDoS attack that allowed a malicious actor to overload the servers with ICMP packets.
Protect	New implementations include new firewall rules to limit ICMP packet rates, source IP address verifications to check for spoofed IP addresses, and network monitoring for anomalies. An IDS/IPS system is also to be implemented to help filter out ICMP traffic with suspicious characteristics.
Detect	An intrusion system as well as new firewall logging implementations will be used to detect unauthorized access to confidential and sensitive data. SIEM tools will also be extremely helpful in monitoring logs for suspicious activity.
Respond	The incident management team has blocked incoming ICMP packets, stopped all non-critical network services offline, and restoring critical network services. Management was made fully aware of the incident and the steps taken afterward.
Recover	Any data lost was recovered from the most recent backup stored the previous night. Staff was informed of this essential reset to the systems and that any recent changes to customer information would have to be re-entered.

Reflections/Notes: Vulnerability scans and security audits should occur a bit more frequently, and keeping software updated will help lower the likelihood of something like this catching the team off guard and help keep business operations up and running.