Incident report analysis

Use the NIST Cybersecurity Framework to respond to a security incident

Summary	Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The company's cybersecurity team investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an ***unconfigured firewall***. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

Protect	To address this security event, the network security team implemented: ● A new firewall rule to limit the rate of incoming ICMP packets ● Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
Detect	To increase the speed and efficiency of detection the team will use an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics and a Network monitoring software to detect abnormal traffic patterns.
Respond	The team configured the firewall which was the exploited vulnerability used to launch the DDoS attack.
Recover	The internal network for two hours until it was resolved.

Reflections/Notes: It's important to do regular security audits in order to identify such vulnerabilities in the network. This event could have easily been prevented if the firewall was configured properly. For this, the security team needs to do regular security audits and keep the system updated and properly monitored.