NIST CSF Incident Report Analysis

Summary	The organization in question experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the 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 team responded by blocking the attack and stopping all non-critical network services so that critical network services could be restored.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. The ICMP protocol was not blocked or rate-limited on the firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack, specifically what is known as an ICMP flood.
Protect	To work towards preventing similar security events in the future, the network security team implemented: 1. A new firewall rule to limit the rate of incoming ICMP packets. 2. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect similar attacks in the future, the network security team has implemented: 1. Source IP address verification on the firewall to check for spoofed IP

	addresses on incoming ICMP packets 2. Network monitoring software to detect abnormal traffic patterns
Respond	The incident management team responded by blocking incoming ICMP packets on the firewall and by suspending all non-critical network services. In the future, the team will isolate affected systems to prevent further spread of the attack. The team will also check network monitoring logs to investigate suspicious traffic.
Recover	Critical network services were restored. After restoration was validated and the flood of ICMP packets timed out, non-critical network services were resumed.