Incident report analysis

Summary	This organization recently 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 incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company’s cybersecurity team then 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.
Identify	Network services suddenly stopped responding due to an incoming flood of ICMP packets Normal internal network traffic could not access any network resources. This likely affected anyone requiring access to the company’s network services.
Protect	All users and employees requiring access (at differing levels) to the system were affected. The entire security team should be made aware of this attack, its cause, and mitigations. To address this security event, the network security team implemented:

	1. A new firewall rule to limit the rate of incoming ICMP packets 2. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets 3. Network monitoring software to detect abnormal traffic patterns 4. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	Existing security information and event management system (SIEM) and network monitoring tools should continue to be utilized to detect similar attacks in the future, and maintained at a regular cadence in order to ensure that they are configured correctly, and performing as expected.
Respond	Firewall, source IP, and ICMP traffic verification rules should be revisited regularly in order to mitigate this type of attack in the future. Training for the security team regarding the usage of these tools and their configuration should be updated and disseminated.
Recover	In this particular case it is unlikely that there was any loss of existing data. It is possible that legitimate traffic was blocked during the attack, and immediately following the security team's response to the attack. It is expected that user and client side retries should re-populated any traffic lost during this timeframe - it is recommended that these processes be revisited in order to ensure no loss of data in the event of a similar attack in the future.

Reflections/Notes: