Incident report analysis.

Summary	Our organization experienced a Distributed Denial of Service (DDoS) attack that effectively compromised our internal network for a duration of two hours. The attack specifically targeted our network services by flooding them with ICMP packets, leading to an immediate cessation of service. This overwhelming traffic made it impossible for regular internal network activities to access any network resources. The issue was resolved after two hours of sustained efforts by our IT team to mitigate the attack and restore normal operations. Further investigation and security enhancements are currently underway to prevent future incidents
Identify	The company's cybersecurity team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. **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 detect new DDoS attacks in the future, the team will implement a new network monitoring software to detect abnormal traffic pattern and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline. For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report

	all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: