Scenario

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. 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.

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.

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**
- **Network monitoring software to detect abnormal traffic patterns**
- **An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics**

Incident report analysis

Summary	The organization experienced a network service ICMP flooding which required the organization to bring down all non critical network service. The organization was able to return network service back to normal operations and will implement steps to further secure their companies network.
Identify	After the organization recently experienced a distributed denial of service attack by a flood of ICMP pings, the team discovered that the primary compromise was an unconfigured firewall. The malicious attacker was able to overwhelm the server and bring down its operations temporarily.
Protect	The team has addressed this security event by implementing a rate limit on incoming ICMP pings, source IP address verification through the firewall to prevent IP Spoofing, network monitoring software to detect abnormal network traffic, and an IDS/IPS to detect or prevent ICMP traffic based on specific characteristics.
Detect	To improve and prevent future DDoS attacks the team will ensure that all firewalls are configured and unused ports disabled, as well as using network monitoring tools to observe abnormal activities.
Respond	For future security events the team will isolate the affected system to prevent disruption of services. The team will also analyze network logs to ensure abnormal network behavior is occurring on the network. Finally the team should report all incidents to upper management to follow through on next steps or action plan.
Recover	To recover from ICMP flooding DDoS attack all system functionality must be brought back to normal operations. All noncritical network operation on the network should be stopped to reduce network traffic. Next, all critical network services should be restored first. Once the ICMP flood packets have timed out,

	return all non critical service online.

Reflections/Notes: