Incident report analysis

Summary	In this scenario I am a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. The 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. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored.
Identify	A Malicious actor attacked the organization network with ICMP flood packets. Because of that, the internal network affected and had to be stopped.
Protect	A new firewall rule was implemented to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	Network monitoring software was implemented to detect abnormal traffic patterns, track authorized versus unauthorized users, and detect any unusual activity on user accounts.
Respond	For future incidents, it's important to isolate the problem to prevent further disruption to the network. One thing that can be done is analyse the log, making sure that the organization is running smoothly.
Recover	To recover from this type of attack in the future, external ICMP flood attacks should 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.