Incident report analysis

Summary	Multimedia company experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. The security team found which caused the DDoS attack was due to incoming flood of ICMP packets, which essentially lead to failure to access network services and resources.
Identify	A malicious actor targeted the company and started a DDoS attack with ICMP flooding. This affected the internal network within the company and needs urgency to secure and restore the network resources affected.
Protect	The security took action by implementing a new firewall rule that limit the rate of incoming ICMP packets as well as an IDS/IPS system to filter out some traffic based on suspicious characteristics.
Detect	The security team has network monitoring software implemented to detect abnormal traffic patterns. As well source IP verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	Security team will attempt to restore any critical systems and services that were affected by the attack. For future attacks isolating the systems to prevent further disruption to the network. The security team will then analyze logs to check for suspicious and abnormal activity to get more clarity on the incident. Additionally the team will report back to management and appropriate legal authorities, if needed.
Recover	Network services need to be restored back to their normal functioning state with critical services as top priority. ICMP flooding can be prevented with firewalls in place. Review all non-critical network services and put them on hold to reduce network traffic. After all ICMP packets from the flood have been

	timed out, non-critical network services should be brought back online.

Reflections/Notes: The NIST CSF and its five core functions provide a framework of developing proactive plans and implementing responsive actions against cybersecurity threats. These functions are essential for establishing effective strategies within an organization. It is essential for an organization to process the capability to promptly rebound from incidents and mitigate risks to minimize potential harm.