Incident report analysis

Summary	The multimedia company recently experienced a DDoS attack. It was found that a malicious attacker used ICMP packets to flood the server. The team responded by blocking incoming ICMP packets. This was caused by a firewall misconfiguration that allowed malicious attacker to overwhelm company's network
Identify	There was an DDos attack that overwhelmed the organization's network. It was due to a misconfigured firewall
Protect	**The Firewall was updated and properly configure to receive the just enough ICMP and block unnecessary one and IDP/IPS was used to filter out suspicious behaviours**
Detect	The use of packet log analyzer to detect malicious actor actions
Respond	**All the incoming ICMP packets were stopped immediately to prevent critical service from halting**
Recover	Use backups to store the operation to normal

Reflections/Notes: From the activity I learned how to use NIST CSF to write an incident response. It taught me valuable information for each action that should be undertaken. However, my incident response can still be improved by learning more appropriate action for each stage.