In this project I created an incident report using the knowledge I have gained about networks throughout the Google Cybersecurity Certificates “Network Security” course to analyze a network incident within a fictional scenario. I analyzed the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF).

Multimedia Company DDOS Attack

Incident Report Analysis

Summary	Recently our organization experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, network services 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.
Identify	The cybersecurity team found in an investigation that a malicious actor 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	The cybersecurity team has implemented new network hardening practices to prevent future attacks: A new firewall rule to limit the rate of incoming ICMP packets,, Network monitoring software to detect abnormal traffic patterns, and a IPS system to filter out some ICMP traffic based on suspicious characteristics

Detect	To detect new unauthorized access attacks in the future, the team will use an intrusion detection system (IDS) to monitor all incoming traffic from the internet. The team also configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
Respond	For future security incidents, the cybersecurity team will isolate compromised systems to prevent further network disruption. They will prioritize the restoration of any critical systems and services impacted by the event. The team will also conduct a thorough analysis of network logs to identify any suspicious or abnormal activity. Additionally, all incidents will be promptly reported to senior management and, when necessary, to relevant legal authorities.
Recover	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: