Incident report analysis

APPLYING NIST CSF TO IMPROVE NETWORK SECURITY.

Summary	The summary of this event is about a multimedia company that experienced a Distributed Denial of Service (DDoS) attack specifically utilizing an ICMP flood, which caused two hours of network downtime whereby both internal and external users were unable to access critical resources. It was caused by an unconfigured firewall that allowed malicious ICMP packets to overwhelm the network. The mitigation steps taken were blocking incoming ICMP packets , stopping all non-critical network services and then restoring critical services to stabilize the network.
Identify	The attack identified in this incident was the Distributed Denial of Service(DDoS) attack, specifically an ICMP flood attack (Ping flood) where the attacker sends an overwhelming number of ICMP packets to saturate the target processing capacity. The system affected was the network infrastructure that impacted the internal network rendering critical and non-critical network services inaccessible The firewall was also exploited as the entry point of the attack.
Protect	To protect the organization, various systems or procedures need to be updated or changed to further secure the organization's assets which are; ● **Firewall Configuration and Management:** The organization should ensure that the firewall is configured to block unnecessary

	ICMP, regularly review and update firewall rules to adapt to evolving threats and conduct a full audit of firewall configurations ensuring that no other vulnerabilities exist. ● **Network Security:** tools like SIEN can be used to monitor and analyze logs for signs of attack, organizations should also implement the use of Intrusion Detection and Prevention Systems(IDS and IPS) to detect, prevent and block unusual traffic patterns. ● **Incident Response Plan Update:** Organizations should include protocols in handling DDos attack incase they come across any incident like that again. ● **Patch Management:** organizations should ensure that they regularly update all network hardware to the latest firmware patch known vulnerabilities. ● **Employee Training and Awareness:** organizations should employ expertise or world class security specialists to train staff on identifying signs of network issues.
Detect	Considering ways the organization can monitor and analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Below are some strategies: ● **Network Traffic Monitoring:** tools like Wiresharks or Solarwinds should be implemented to continuously monitor traffic patterns and detect unusual spikes. The organization should also utilize NetFlow to analyze and distinguish between legitimate and anomalous traffic. ● **Application Monitoring:** Web applications firewalls should be

	deployed to protect from malicious requests such as SQL injections or cross site scripting. ● **User Activity Tracking:** Implementation of IAM solutions like Azure AD to track users access. ● **Endpoint Monitoring:** using tools like Crowdstrike to monitor endpoint activity and to detect unusual behavior on endpoints
Respond	Containing the cybersecurity incidents and the devices affected, isolating the device affected, implementing access restrictions and engaging in incident response tools should be an immediate action. Moving on to neutralizing the incidents, the root cause should be identified, mitigation of the exploited should follow. Also removing the malware is necessary and then data can be restored. Network traffic data, logs and alert, endpoint activity should be involved in analyzing the incident after all these the recovery and improvement process can come through.
Recover	This stage is all about recovering from the incident, getting information needed for immediate recovery like the incident scope and impact, root cause analysis. Moreover also including the processes involved to help recover from the incident and the preventive enhancement for future recovery. Finally the recovery improvement recommendations.