Incident report analysis

Summary	The multimedia company recently experienced a Distributed Denial of Service (DDoS) attack, leading to a disruption of internal network services for two hours. This attack was executed through a flood of ICMP packets, overwhelming the company's network due to an unconfigured firewall that allowed unrestricted ICMP traffic. During the attack, normal network operations were halted, preventing internal traffic from accessing network resources. The incident management team responded by blocking incoming ICMP packets and stopping non-critical services to ensure critical network functionality. A subsequent investigation revealed that a malicious actor exploited the firewall vulnerability, initiating the DDoS attack by sending a high volume of ICMP pings into the network.
Identify	The security team identified this incident as a DDoS attack targeting network vulnerabilities, specifically through ICMP packet flooding. The affected systems included internal network services, essential for daily operations. The attack source exploited an unconfigured firewall, which allowed ICMP packets without restrictions, making the network susceptible to this type of attack. This incident highlights gaps in network configuration and a need for proactive vulnerability assessments to detect such weaknesses before they can be exploited.
Protect	To prevent future incidents, several protective measures should be prioritized, focusing on securing network traffic against unauthorized access. Implementing a firewall rule to restrict ICMP traffic will help limit potential DDoS attacks by only allowing necessary and legitimate ICMP packets to pass through, significantly reducing the risk of ICMP flooding. Additionally, an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) should be configured to filter and block suspicious ICMP traffic based on established

	patterns, further strengthening the network's defense against DDoS threats. Regular audits of firewall configurations, alongside the use of IDS/IPS filtering, will help maintain a robust, secure network environment that can better withstand similar attacks in the future.
Detect	Enhanced detection capabilities are essential for identifying potential threats early. Configuring source IP address verification on the firewall will help detect and block any spoofed IP addresses, making it more challenging for malicious actors to disguise the origin of an attack. Furthermore, implementing network monitoring software will enable the security team to quickly identify unusual patterns, such as unexpected spikes in ICMP traffic, which could signal an attack in progress. Regular monitoring and logging of network traffic not only aid in detecting anomalies in real time but also provide valuable data for incident investigation, enabling faster and more accurate response measures.
Respond	A response plan is crucial for containing and mitigating future cybersecurity incidents. In the event of a similar attack, the team should follow predefined procedures to contain the threat, such as isolating affected devices and blocking specific types of traffic to reduce the attack's impact. Neutralization procedures, including stopping non-critical network services and prioritizing critical functions, should be put in place. Analysis of the incident logs can help identify the attack's origin and behavior patterns, providing insights to strengthen future response strategies and improve overall security protocols.
Recover	After containing the incident, a structured recovery plan is essential to restore normal operations. Access to network services should be returned to a normal functioning state, with external ICMP flood attacks blocked at the firewall to prevent recurrence. Initially, all non-critical network services should be stopped to reduce internal traffic, while critical services are prioritized and restored first. Once the ICMP flood has timed out, non-critical network services can be gradually brought back online. A post-incident analysis should follow to assess any data loss or disruptions, with findings documented to refine recovery

	protocols and improve future response strategies.

Reflections/Notes: