Incident report analysis

Summary	The multimedia company experienced a Distributed Denial of Service (DDoS) attack that disrupted its internal network for two hours. The attack flooded the network with ICMP packets, rendering normal internal traffic inaccessible. Upon investigation, it was found that a malicious actor exploited an unconfigured firewall, allowing the DDoS attack to overwhelm the network.
Identify	The DDoS attack affected the network systems for the company causing the entire internal network to be inaccessible. All critical network resources needed to be restored.
Protect	In response, the company's cybersecurity team implemented various measures, including rate-limiting incoming ICMP packets, source IP address verification, network monitoring, and an IDS/IPS system to filter suspicious ICMP traffic.
Detect	To better detect these kinds of attacks in the future, the company should deploy network monitoring software with intrusion detection capabilities to identify abnormal traffic patterns, potential DDoS attacks, and IP spoofing.
Respond	To improve network security, the company plans to focus on regular audits, policy implementation, monitoring capabilities, incident response, and recovery strategies. These actions aim to strengthen the organization's network security and mitigate the risk of future cybersecurity incidents.
Recover	The cybersecurity team implemented necessary updates to the security processes and network infrastructure to prevent similar DDoS attacks. In the future, external ICMP floods can be blocked by a firewall, and all non-critical network services should be stopped to reduce the amount of traffic. Then, critical network resources should be restored, once the attack has stopped, all network services should be brought back online.

Reflections/Notes: