Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	The multimedia company experienced a Distributed Denial of Service (DDoS) attack, causing a significant disruption to its internal network for a duration of two hours. The attack targeted the company's network services, rendering them unresponsive due to an influx of Internet Control Message Protocol (ICMP) packets. Normal internal network traffic was halted, resulting in the inability to access any network resources.
Identify	Regular audits of internal networks, systems, devices, and access privileges were not conducted, leading to the vulnerability in the unconfigured firewall All critical network resources needed to be secured and restored to a functioning state due to ICMP Flood Attack
Protect	The team implemented ● A new firewall rule to limit the rate of incoming ICMP packets ● Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets ● Network monitoring software to detect abnormal traffic patterns ● An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

Detect	To detect new unauthorized access attacks in the future, the team added n IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics and implemented network monitoring software to detect abnormal traffic patterns.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. 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: