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	A multimedia company's network services suddenly stopped responding due to an incoming flood of ICMP packets due to DDoS attack. The cybersecurity team investigated the security event and found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. The network security team implemented a new firewall rule, Source IP address verification on the firewall, Network monitoring software to detect abnormal traffic patterns,IDS/IPS system to filter out some ICMP traffic based on suspicious activities.
Identify	Network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. Critical network services need to be secured and restored.
Protect	The cybersecurity team investigated the security event and found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall.,IDS/IPS system to filter out some ICMP traffic based on suspicious activities.
Detect	Verified Source IP address on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented IDS/IPS system to filter out some ICMP traffic based on suspicious activities.

Respond	The cybersecurity team will isolate affected systems to prevent further disruption to the network, and the team will analyze network logs to check for suspicious activity.
Recover	Access to network services need to be restored, external ICMP flood attacks can be blocked at the firewall.Critical network services should be restored first.

Reflections/Notes: