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 DDoS attack, causing a flood of ICMP packets to cause multiple network services to stop working. The Cybersecurity team responded by restoring critical network services, and shutting down non-critical services.
Identify	The company was targeted by a malicious actor with an ICMP flood attack that affected the internal network.
Protect	The cybersecurity team implemented a new firewall rule that will limit the rate of incoming ICMP packets and introduced an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team implemented source ip address verification on the firewall to actively check for any spoofed IP address on the incoming ICMP packets. Network monitoring software was added to detect abnormal traffic patterns.
Respond	Any affected systems will be isolated by the cybersecurity team in an attempt to restore disrupted critical systems. Afterwards, the networks will be analyzed to check for suspicious activity. Any incidents must be reported to upper management.

Recover	In order to recover, access to the network services must be restored back to normal. With these added changes, future external ICMP flood attacks should be blocked out by the newly added firewall rules. Critical services should always be restored first, after stopping any non-critical services.

Reflections/Notes: