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, providing web design, graphic design, and social media marketing solutions, faced a DDoS attack resulting in a compromise of its internal network for a two-hour duration. The attack involved a flood of ICMP packets, causing a disruption in network services and hindering normal internal traffic access to network resources.
Identify	The incident management team subsequent cybersecurity investigation revealed that a malicious actor exploited a vulnerability in an unconfigured firewall, allowing them to inundate the network with ICMP pings and execute a distributed denial of service (DDoS) attack.
Protect	The team has implemented a new firewall rule to limit the rate of incoming ICMP packets and source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Detect	The team implemented a Network monitoring software to detect abnormal traffic patterns and an IDS/IPS system was applied to filter out some ICMP traffic based on suspicious characteristics
Respond	The incident management team responded by blocking incoming ICMP packets and taking non-critical network services offline. Following the incident, the

	company should utilize the newly implemented firewall rules to limit the rate of incoming ICMP packets during DDoS attacks.
Recover	The team should regularly back up critical data and systems to minimize data loss and expedite recovery and implement automated recovery processes where possible to streamline restoration efforts.

Reflections/Notes: