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	
Identify	The incident management team audited the system in order to determine the gaps in the security. The team found that a malicious actor flooded the network through ICMP pings through an unconfigured firewall. This vulnerability allowed a DDoS attack.
Protect	The team has implemented these measures to safeguard the network: • 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 any incoming attacks and threats the team has implemented IDS (intrusion detection System) to monitor the incoming packets. SIEM tools are regularly used to monitor logs for any threats. Network Protocol analyzers are also used for sniffing any malicious packet.
Respond	The team responded by Blocking incoming ICMP packets and stopping all

	network communications, restoring critical network services.
Recover	The team restored all the network services after resolving the issue.

Reflections/Notes: