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 organization experienced a DDoS attack, which.....
Identify	A DDoS attack which took the network services down so network resources and other network-related features couldn't be used.
Protect	New firewall rules are in place, and IDS and IPS systems have been installed, which will help protect against future attacks.
Detect	The IDS/IPS system and the network monitoring software will help detect future attacks.
Respond	The incident management team blocked incoming ICMP packets, stopped all non-critical network services offline. This will help in the future.
Recover	The organization recovered by restoring critical network services. Of course, this helped the network to come back on. This will help in the future.

Reflections/Notes: