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	This was a DDoS attack, where the attacker was able to send out a multitude of of IMCP packets to disrupt the companys daily activities as a way to plug themselves into the system potentially.
Protect	I would recommend adding a command to the firewall to limit the amount of IMCP packets that are being pushed through to the companies servers, but leave just enough room to alert the team that a DDoS attack is trying to pry into the servers. I would also create a prompt that continuously backs up any current work being performed in an encrypted way straight to the cloud.
Detect	As I said in my response above we can leave an opening just large enough for the team to identify there is an attack trying to progress into our servers
Respond	The best way for us to respond and neutralize the next attack is to ensure we are in detection of it as it slowly trickles into our system by implementing a way for us to realize it sooner than wait for it to crash the entire system.
Recover	Implementing a command that backs up any work that happened within the last 5 mins before an attack will ensure that our workers can safely and securely access there work and continue working from where they left off

	without having to start over.

Reflections/Notes: