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 afternoon we saw a really compromising attack, we could see that our company of multimedia was attacked by threat actors by flooding all the network with ICMP packets, in other words we saw a DoS attack, at first it was a really common day, but with the pass of the time we started to being attacked by the packets. This ICMP flooding attack crashed the server for two hours until the IT team could solve it.
Protect	After this attack and the help of everyone on the team we could make new strategies to stop this type of attack. First we have to focus on network's company, because it was the weakest part of this attack, specially on some protocols related to ICMP, the pings are really important on this part, because it was the cause of the attack and also it could be the solution of this problem, for example you can send "pings of death" to destroy the system, but you can start trying to communicate with other systems with the same "ping".
Detect	We start looking that the services were not responding and then we start looking at the pings to other computers to learn what was happening with the communication.

Respond	To respond to these attacks we could make a lot of strategies, first we can do a patch system to develop new actualizations and make it harder for the threat actor to hack the system. On the other hand we can block the ICMP at the firewall to stop the flood and try to repair it, also we could make new IP verification to all the users and detect abnormal communication on the network.
Recover	On the end we try to stop the services some minutes to try to solve this problem from the root (which take us 2 hours) and make it stronger for the private data of the users.

Reflections/Notes: The hardest part of this was trying to give a view of the recovery of the organization. At the end everything was a little bit strange, because we didn't have a lot of information about the incident so we had to suppose some things.