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	Our company suffered a DDOS attack through an unconfigured firewall which led to the security team having to take all non-critical areas of the network down until the incident was dealt with.
Identify	This was a DDOS attack using ICMP packets through an unconfigured firewall to overload the network and in response all non-critical infrastructure was taken offline.
Protect	In order to protect us from future attacks we implemented a new firewall rule to detect for a high level of ICMP packets as well as any packets that may be using IP spoofing. New network monitoring software was installed as well as an IDS/IPS system to filter out any unwanted traffic that makes it through.
Detect	The installation of new network monitoring software as well as the new IDS/IPS will increase the likelihood of detecting this event in the future.
Respond	If any device on the network is compromised the team must isolate the incident from the rest of the network. If it is too late and the incident has spread, all non-critical network infrastructure must be taken offline. We have implemented rules to help ensure that this event will be detected and a repeat not possible due to our strengthened firewall rules that account for the ICMP

	DDOS attacks.
Recover	Bring back online all non-critical network infrastructure. Validate the integrity of critical and non-critical network areas.

Reflections/Notes: