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	There has been an attack to which a threat actor used a DDoS attack and was able to penetrate the system and flooded it with ICMP.
Identify	There has been an attack in which a threat actor used a DDoS attack and flooded the server with ICMP that were oversized. This could be that they had found an employee IP address and used an IP attack method known as smurf attack where the attacker impersonated an authorized user and sent data packets that are oversized more than 64KBT. In this case we had multiple DoS attacks known as DDoS.
Protect	After identifying the cause of the breach First we blocked all traffic in our network, and all these different IP's sending DDoS attacks wouldn;t be able to keep doing so. Second We are strengthening our security by going through our firewalls rules and regulations by checking what ports we allow and disallow. Checking on how how our reverse proxy protocols is responding to the request of different IP trying to access our network, in this case NGFWs are great for they reject IP address that are even familiar with it but trying to have access from a different location or out of a segment that the IP usually is requesting data from. Passed the firewall our IDs and IPs are responding properly.

Detect	Through our SIEM tools we have detected that the attacker used multiple computers not only was it a DDos attack but a botnet. For the IP spoofing they might've used a brute force technique which they might've used to gain access to our data by impersonating an authorized user. Another possible vulnerability would be the smurf attack, when they gain access to an authorized user IP and impersonate them.
Respond	We have put in place next generation firewalls (NGFWs) and we have also established policies and regulation on ports, our reverse proxy corresponds correctly with who gets access to our network, IDSand IPS are working properly helping prevent any intrusion that might be able to go through our firewalls. Segmentation of network in place for we have established a demilitarized zone and control zone for all different branches in the organization each one with their own segments.
Recover	Daily production is up and running, we are working on ways to prevent a similar or any other vulnerability. For this we are doing a lot of pen tests in the VM and checking the SIEM tool to keep up with our daily log event.

Reflections/Notes: