Domain: Network Security

Question 1: Faulty Firewall

Suppose you have a firewall that's supposed to block SSH connections, but instead lets them through. How would you debug it?

Response:
A firewall is used to control traffic going into a network or a host by comparing the characteristics of the incoming traffic against a predefined set of rules. It may look at the IP, the ports involved and the type of protocol being used eg ICMP, HTTP, etc. In this scenario, the firewall was expected to block SSH traffic but instead is allowing it through.

In our first project in Cybersecurity Bootcamp, we had a similar requirement for a set of VMs to be accessible by SSH over port 22 only by a single machine referred to as a Jump Box. Any other machines that try to connect would encounter timeouts when trying to login. We setup a network security group to act as a firewall which had rules to only allow SSH using port 22 if the IP of the machine matches the one used by the Jump Box.

If we encountered a scenario in this setup where the VMs are accepting SSH connections from other clients, the first thing we would check i the network security group rules. Is there are a defined rule that is supposed to limit SSH connections? If the rule exists, we would check the setting for the rule if it has the correct IP and port for the Jump Box and the IP and port settings for the Web VMs. We would also double check if there are any rules that conflict or override eg higher priority over the rule which limits the SSH connection.

Once any updates or corrections are made to the configuration, we will test this by having the Jump Box make a proper SSH connection to the Web VMs. Aside from this, we would also test the scenario where a machine other than the Jump Box would attempt to SSH to the web VMs. If the Jump Box can make an SSH connection and other machines are blocked, then the firewall/network security group would be working as expected.