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?

Make sure each section of your response answers the questions laid out below.

1. Restate the Problem: To find out why a firewall would allow any machine to SSh into it, you would have to check the inbound security rules under the network security group, double check the allowed IPs and update the IP addresses if they have changed overtime. another option would be using a time authenticator like Google authenticator to sync up with a VPN so IPs wouldnt have to be entered manually

2. Provide a Concrete Example Scenario: In class we set up a virtual network that has a network security group that would only allow our personal IP address to ssh into the docker machine after attaching a the SSH key to the inbound rule

In Project 1, did you allow SSH traffic to all of the VMs on your network? Yes, we used SSH keys to get rid of password vulnerabilities and prevent brute force attacks

Which VMs did accept SSH connections? jump-box-provisioner, web-1, web-2, and Elk NSG

What happens if you try to connect to a VM that does not accept SSH connections? Why? The connection would time out because it lacked the SSH key and could not connect. Also if there was a rule to have port 22 turned off. If a change needs to be made, port 22 could be opened briefly and after the change should closed to maintain secure machine and network.

3. Explain the Solution Requirements

If one of your Project 1 VMs accepted SSH connections, what would you assume the source of the error is? There could have been an incorrect setting during the inital setup of the inbound rules

Which general configurations would you double-check? The inbound security rules as well as the accept and deny list.

What actions would you take to test that your new configurations are effective? I would make sure that the machine can be SSH'd into after the key is saved into the inbound rules. It would make sense to perform a change and then verify that it is working properly. Including restarting the machine to make sure the changes took affect.

4. Explain the Solution Details

Which specific panes in the Azure UI would you look at to investigate the problem? Network security groups and inbound rules. Checking the resource groups to the find problems.

Which specific configurations and controls would you check? Checking ssh passwords under key-gen.

What would you look for, specifically? I would double check the the IP source of the machine that would SSH into the network security group as well as make sure the correct port is being utilized that was setup in the initial inbound security rule

How would you attempt to connect to your VMs to test that your fix is effective? Using Gitbash, I would attempt to make an SSH connection with the correct username and IP address for the external IP's. I would use Jump-box for an internal IP address. A port scan using nmap to see if port 22 is open. A Ping command to the machine to see if a connection can be established.

5. Identify Advantages/Disadvantages of the Solution

Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access? As long as an SSH key is utilized the chances of unauthorized access are greatly reduced and making sure the ports are closed. It may seem like the system would be secure enough to prevent from being hacked, but if possible, I would consult a penetration tester is see that the system is as secure as possible.

What monitoring controls might you add to ensure that you identify any suspicious authentication attempts? Utilizing Snort or Kibana can find suspicious activity. An external facing firewall out keep out unwanted traffic, such as an IDS or IPS. I would also set up and record any log activity that could keep a record of all system traffic in case an unusual activity accorded on the network.