Interview

1. Restate the problem

In order to restrict access to the VMs in your network, we need to deploy firewalls. Firewalls provide protection against outside cyberattacks by shielding the network from malicious traffic. A set of rules must be created to allow or deny traffic and access in the network. In case of an event where the firewall in place allows SSH connections when it is not supposed to, it can cause severe consequences like unauthorized access leading to breach of secure data.

2. Provide a Concrete Example Scenario

During the project on automated ELK server deployment which we had done during the cybersecurity bootcamp, we had set up a network with 4 VMs connected to another VM which was configured as a jump box. Only the jump box VM could be accessed from the Internet using SSH. The other VMs are accessed through the jump box using SSH. If we try to access a VM that does not accept SSH connections, our access will be denied since the security rules do not permit the access.

3. Explain the Solution Requirements

Only the jump box can connect using SSH to the other VMs while the VMs cannot to each using SSH. In case the VMs connect to each other using SSH, it would mean that the firewall rules are not configured to block the access or if the rules are already in place, it could be a security attack. Further, we would need to review the existing firewalls rules. To verify whether the rules are functional, we would conduct SSH login attempts on all the VMs.

4. Explain the Solution Details

On Azure UI, we can check the settings for the network security groups which lists down the currently set security rules in the network – destination ports, source, and destination. We can attempt SSH logins on all VMs from different IP addresses and between the VMs. We can test the connection for SSH for each VM to check if firewall allows/blocks the connection.

5. Identify Advantages/Disadvantages of the Solution

Since we have created an inbound security rule that Jump box can be only accessed from my personal IP address and other VMs can only be accessed through the jump box, I believe the solution guarantees that the Project 1 network is now "immune" to all unauthorized access.

With the help of Wireshark and Kibana, we can monitor the VMs to detect any suspicious authentication attempts.