#### **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

If your firewall is letting SSH connections through even though they should be blocked, there are a few steps to take.

1. Provide a Concrete Example Scenario

First you’ll want to ensure your security group has an inbound rule that is blocking all SSH connections except from your local machine and/or virtual machine (VM) IP address. For project one of my cybersecurity bootcamp we allowed SSH only from our Jumpbox VM in Azure. The remaining VMs were connected only to the Jumpbox without SSH access to limit exposure to the public and also allows us to do monitor and logging on a single device, the Jumpbox. If you try to connect via SSH from any other device you’ll receive a “connection refused” error because port 22 is blocked.

1. Explain the Solution Requirements

If you have inbound rules to accept SSH port 22 and are still having connectivity issues, try restarting your ssh by running sudo service ssh restart. If that doesn’t work, double check your credentials, that the firewall allows SSH, and that SSH is installed on your server. If you need to install SSH, run the command sudo apt install openssh-server.

1. Explain the Solution Details

To investigate the problem, take a look at your inbound security rules in your Azure security group. Check to see that your IP address is allowing port 22 TCP connections. If you’re using a local machine connected to a VM, ensure that you have an inbound rule to allow your local IP to connect via port 80 (HTTP).

1. Identify Advantages/Disadvantages of the Solution

It’s important to note that this does not make your system immune to unauthorized access. Attackers could spoof your IP address or find a backdoor or vulnerability elsewhere. You’ll want to set up continual monitoring tools and utilize tools such as wireshark to analyze packets moving in and out of the system. Ensure that all your software is updated to implement patches for vulnerabilities and train your employees.