#### **Domain: Network Security**

**Question 1: Faulty Firewall**

Blocking SSH connections is the proper way to harden the security of your server. There are no ways of brute forcing the SSH key, when you compare to passwords which can easily be cracked using brute force, especially a weak one.

It is good practice to make sure no one can gain access to your machines unless you want them to.

In Project 1 of my cybersecurity bootcamp, we created something similar.

We created a Network with VMs that has a firewall which is called Network Security Groups. We set NSG rules that allow or block SSH connections.

In the Network, all the VMs accept SSH connections, but the connections are limited to certain IP addresses and groups. If you try to SSH to the VMs that don't accept SSH connection you will not be able to connect.

This is due to the fact that there may be NSG rules that are blocking/Denying SSH connections. The other reason, maybe only TCP connections are enabled for SSH in security group rules.

If we configured a firewall that's supposed to block SSH connections, but one of the VM accepted SSH connections, the problem may be in the NSG rules.

The first thing you should do is to go to your Azure network and check the configuration/implementation of your security rules.

After checking the configuration and making sure everything is how you want it to be, then try to SSH to the VM and see if you can establish a connection.

If you are still getting a connection, then you should navigate to your Azure resource panel and click on the VM that you need to investigate. Then click on the Network tab and inspect the NSG rules that are created if they meet the requirements. Make sure the NSG rule which Block/Deny SSH connection has a higher priority than all other rules. Check the source and make sure the value is not “Any”, any allows incoming traffic from anywhere. Once everything is checked, go back to your terminal and try to SSH to your VM. You shouldn’t be able to connect.

The VM's have been configured with SSH key access only, which is the most secure way to configure remote access, and this will guarantee there are no unauthorized connections to the VM.

To make sure you identify suspicious attempts it is best to implement security for internal traffic by using network security groups or Azure firewall, establish a private network access to azure services by associating an NSG with the subnet and restrict rules to your configured resources. You can also protect applications and services from external network attacks. Finally make sure anti-malware software and signatures are updated.