**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

I would first configure a firewall that’s supposed to block all SSH connections by identifying and configuring the specific inbound/outbound rules. Then, I would simply create a new rule by blocking Port 22 (SSH) via inbound communication. I would set that rule as a priority (Rule 100, 200, 300—some type of low number that the machine is able to take this rule into account as the first step).

1. Provide a Concrete Example Scenario
   * In Project 1, did you allow SSH traffic to all of the VMs on your network?
   * Which VMs did accept SSH connections?
   * What happens if you try to connect to a VM that does not accept SSH connections? Why?

For all of my VMs (Web-1, Web-2, Web-3 Elk-VM) I created an “Allow” rule to allow SSH traffic as a priority in order to access the server’s back end. If you try to connect to a VM that does not accept SSH connections, the connection will terminate and you will not be able to gain access to the VM.

1. Explain the Solution Requirements
   * If one of your Project 1 VMs accepted SSH connections, what would you assume the source of the error is?
   * Which general configurations would you double-check?
   * What actions would you take to test that your new configurations are effective?

One credible scenario is that the VM may not be started virtually in Microsoft Azure portal. The VMs need to be up and running in order to successfully SSH into them. I would double check the Networking Settings and verify the Inbound Port Rules. I would also check the Virtual Machines dashboard and check the status of the VM to determine if it is On/Running or Off/Deallocated. The action I would take is to go into Git Bash and attempt to ping the VM using its IP address to see if it’s accepting internet connectivity. Then, I would run the SSH command in Git Bash to see if I can successfully gain remote access into the VM.

1. Explain the Solution Details
   * Which specific panes in the Azure UI would you look at to investigate the problem?
   * Which specific configurations and controls would you check?
   * What would you look for, specifically?
   * How would you attempt to connect to your VMs to test that your fix is effective?

I would first go to the Virtual Machines UI open Networking and navigate to Inbound Port Rules. Then, I would check my Network Security Group (NSG), Virtual Network, and Resource Group to confirm that they are all consistently in the same region and under the same newly created network. I would also double check the Networking Inbound Port Rules priority of allowing SSH. Increase its priority before taking into account of any other configured rules.

1. Identify Advantages/Disadvantages of the Solution
   * Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access?
   * What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?​

My solution des not guarantee that the Project network is “immune” to all unauthorized access or malicious attacks. This is attributed to physical security and user/device security that needs to be addressed such as implementing Multi-factor Authentication (MFA), ensuring that my physical device and router are secure, making sure that my device has not been successfully fallen victim to any malicious software (ransomware, viruses, trojans, spyware, adware, etc) in order for an attacker to gain visibility into my physical network and being able to move laterally to my applications/software. Some additional monitoring controls that I would add to identify suspicious authentication attempts is to add monitoring/logging of user activity and Multi-factor Authentication (MFA). Tools I would also implement are Wireshark, Burpsuite, Snort to analyze packets of unknown/suspicious IP addresses and requests that are attempting to reach my network.