**Roy Sanderfer Homework 13 submission**

**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

My firewall is supposed to block SSH connections, however I see that some connections are coming through.

1. Provide a Concrete Example Scenario
   * In Project 1, did you allow SSH traffic to all of the VMs on your network?

No, I allowed SSH from my Jump Box to Web-1,2 and,3, but not to my Elk Stack Server.

* + Which VMs did accept SSH connections?

Web\_1, 2, and 3 all accept SSH connections

* + What happens if you try to connect to a VM that does not accept SSH connections?

You get an SSH connection refused error.

* + Why?

Because the request to connect to the server is routed to the SSH host, but the host does not accept the request, so you get a connection refused error.

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?

If the source of the SSH was from outside of the network, I would say there is a firewall inbound policy error. If the source of the SSH was from inside the network I would not be concerned because that is allowed.

* + Which general configurations would you double-check?

I would check the inbound configurations.

* + What actions would you take to test that your new configurations are effective?

I would try to SSH into the machine from a source outside of the network.

1. Explain the Solution Details
   * Which specific panes in the Azure UI would you look at to investigate the problem?

I would start in the NSG pane and then take a look at the inbound policies.

* + Which specific configurations and controls would you check?

The inbound policies.

* + What would you look for, specifically?

I would look for policies pertaining to inbound SSH traffic and any inconsistencies with them.

* + How would you attempt to connect to your VMs to test that your fix is effective?

I would attempt to connect with a machine outside of the network.

1. Identify Advantages/Disadvantages of the Solution
   * Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access?

The solution I implemented is good and will make the network immune to all unauthorized access until another event takes place. When that happens I will re-evaluate and make the network safe until the next event happens and then we do it all over again.

* + What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?​

There are a couple of things that come to mind that I could do. I could add an IDS, which is Intrusion Detection System. This type of system helps analyze the quantity and types of attacks. I can use this information to implement more effective controls. Also, an intrusiondetection system can also help identify bugs or problems with my network device configurations. I could also implement an ACL, or Access Control List. Access Control Lists are network traffic filters that can control incoming or outgoing traffic. ACL’s work on a set of rules that define how to forward or block a packet at the router’s interface. An ACL is the same as a Stateless Firewall, which only restricts, blocks, or allows the packets that are flowing from source to destination. When you define an ACL on a routing device for a specific interface, all the traffic flowing through will be compared with the ACL statement which will either block it or allow it. The criteria for defining the ACL rules could be the source, the destination, a specific protocol, or more information. ACLs are common in routers or firewalls, but they can also configure them in any device that runs in the network, from hosts, network devices, servers, etc.