## Activity File: Interview Questions

#### 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: **Since the firewall was supposed to block all connections, but instead is lets them through. The first step after identifying the problem is to stop all SSH traffic. Second, go to the network security group, click on the locations it has the problem, them go to inbound security rules and create a new rule restricting only access through a specific machine/network.**

2. Provide a Concrete Example Scenario

- In Project 1, did you allow SSH traffic to all of the VMs on your network? **No, the only SSH allowed was from the DevOps computer to the JumpBox. Once you were inside of docker of the specific machine you could SSH into all the machines in the network. Using a 2FA (Two-Factor Authentication).**

- Which VMs did accept SSH connections? **The only VM allowed to SSH into from outside of the network was the JumpBox.**

- What happens if you try to connect to a VM that does not accept SSH connections? Why? **It will get the response “request time out”. It won’t allow it. Because it was setup that way and you will need a 2FA (Two-Factor Authentication) to connect to the VM’s in the network.**

3. Explain the Solution Requirements

- If one of your Project 1 VMs accepted SSH connections, what would you assume the source of the error is? **First, I would look at the network security group to see if someone changed the rules in place. After I would assume that someone got the RSA private key from the JumpBox.**

- Which general configurations would you double-check? **The inbound security rules.**

- What actions would you take to test that your new configurations are effective? **After all the necessary steps to put the new configuration in place, I would try to connect on the network through a different computer to make sure it worked.**

4. Explain the Solution Details

- Which specific panes in the Azure UI would you look at to investigate the problem? **The activity log and the access control.**

- Which specific configurations and controls would you check? **SSH rules and check access.**

- What would you look for, specifically? **If any other IP address were added and look at the access control to see if anyone was allowed into the network.**

- How would you attempt to connect to your VMs to test that your fix is effective? **SSH into the JumpBox, get into the docker container with ansible, and SSH into every VM on the network to verify the connection is successful. To troubleshoot I would exit the network and try to connect from a different source of IP.**

5. Identify Advantages/Disadvantages of the Solution

- Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access? **Yes. The advantage of the solution specified guarantees that only DevOps has access through SSH into the network. Disadvantages would be a single point of failure; If the only network setup had any issues, it would make it impossible to connect.**

- What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?​ **A Snort Application and IDS (intrusion detection system) if possible. Advantages would be another layer of monitoring to secure the network and access. Disadvantages, would be slower delay on traffic and connection.**