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**

   Our firewall is supposed to block SSH connections, but instead it is letting connections through ssh.

2. 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?**

  In our project1 we had to set up a virtual network. Our network consisted of 3 web machines and a jump-box. During this exercise, we also had to set up inbound and outbound network security rules. We had to make one of them for SSH. We also had to set a rule that allowed the jump-box to ssh into the web machines through port 22. The way we did this is by only allowing the Jump-box's private IP to connect along with a ssh key.

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?**
- **Which general configurations would you double-check?**
- **What actions would you take to test that your new configurations are effective?**

  You can test connections by connecting the jump box to the selected web machines. We will also need to connect it to the web machine with a different workstation. Because the workstation does not have the ssh key or the same IP as the jump box. Therefore, it should not connect to the web machines.

4. 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?**

If the web machine allows the other workstation to connect via ssh, we would have to troubleshoot the situation. We need to start by checking the network security groups making sure all the rules are correct. We would confirm that the ssh keys are set correctly. After verifying and correcting any errors that are found, we would need to verify the repairs.

5. 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?**

While this can make your network more protected, malicious actors might find another way to manipulate the network. We have to monitor to help watch the traffic on the networks. We can use the ELK stack to help. The ELK stack is an acronym used to describe a stack that comprises three popular projects: Elasticsearch, Logstash, and Kibana. The ELK stack gives the ability to aggregate logs from all your systems and applications, analyze these logs, and create visualizations for application and infrastructure monitoring, faster troubleshooting, and security analytics.