Jaime Brown

9/27/2021

Cyber Security

**Activity File: Interview Questions**

**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

**Run the ssh client, in verbose mode $ ssh -vvv user@host. Next on the server check the auth.log for any errors $ sudo tail -f/var/log/auth.log. when you go to debugging. If you have access to the server run the sshd server to debug mode on another port to fix issues.**

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?

**I did show SSH traffic in all the VM’s on the network, from checking the website I have at least 2 ssh, if I try to connect a VM that isn’t connected to the SSH I would get an error that it’s not attached to one.**

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?

**Depending on the inbound or outbound correction, if it is connected which it is there is no error given, if I lost the connection to the SSH I would test the connection or troubleshoot the connectivity issue.**

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 start by selecting diagnose and solve problems function from the Azure website, from there select the category that best describe the issue of the app by using the keywords from the homepage.** **You want to run a custom script, or a custom script extension to help you configure workloads, make sure your VM’s are up and running, you will then deploy and manage the configurations.** **You are checking to make sure there are no pool or node errors. Log back into your portal, open up the dashboard and you will want to select the VM, once your there look for the backup Items tile and select the Azure VM and from there you can view the list of protected Virtual Machines and the statuses and when they were last restored time.**

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?​

**If going off the details above, you would not have any issues nor problems. If at any time however there is an issue you would want to re-run the above configuration and troubleshoot any and all issues. The Advantages/Disadvantages less hardware, its eco-friendly, recovery time is quicker, system upgrades, thin clients and software licensing made easy. VM’s you can use your IP address, or you can purchase a VPN and will be provided with another IP address to use other than your own.**