Interview Questions:

Network Security:

Question 1:

1. Restate the Problem

The problem is that your firewall is not blocking SSH connections, it is allowing the connection to come through, which would allow a remote user to access your machines.

2. Provide a Concrete Example Scenario

A prime example of this is when I was tasked with an activity in my Cyber Security bootcamp through Berkeley extension, I created a security group that allowed ssh connections from my local machine. This helped me connect to the Jump-Box that i created, the difference though is that i was not allowing SSH connections from anywhere but my local machine. All my VMs in this project followed the same inbound rule BUT the main difference is that I used my Jump- Box to manage which IP could SSH in my virtual network and in this case it was only me. The problem with denying all SSH connections in a virtual network is that it makes it difficult to get to these machines and make changes. If you have configured a machine to deny all inbound SSH connections you will receive a connection refused message, It either can do this because the SSH client is not installed or it might be that you have set a inbound rule that might be blocking said connection.

3. Explain the Solution Requirements

If I was put in the place that one of my Project VMs was accepting SSH connections, i would assume that the source of the error was one of the inbound security rules that i put into place was A: Was non existent or B: has not been configured properly C: it has been configured properly but the priority of the rule is conflicting with another security rule. If any of these problems were happening, I would check my AZURE VMs to see where the problem has occurred, this would most likely be in my inbound rules, I would then either make/edit a rule to make sure that SSH connections are either being blocked/limited depending on which machine we are working with. After this step I would got to my shell and test to see if i can SSH directly into the VM i set the rule on, if i configured the rule correctly if would either accept/deny my connection, in your case it would show as connection denied.

4. Explain the Solution Details

So specifically how to do this would be first to check firstly if our security group has been configured correctly, this is where we would add inbound/outbound security rules. Next we look in our inbound security rules list since a SSH connection would be an incoming connection. So click on inbound security rules and see if SSH connections have been allowed. If it is showing as denying SSH connections you should be fine. Another thing to note is that when you are setting up your VMs with AZURE, in the VM configuration page there is a checkbox that specifies if we should accept SSH connections on that VM, if that box is checked then that VM WILL allow SSH connections. I would also check my VMs. I would do this by going to my VMs page and again, checking the inbound security rules. If there is a rule that is allowing SSH connections i would click on it and scroll to the bottom where it was an ALLOW/DENY checkmark, I would then mark this a DENY which basically would deny any SSH connections. After I have checked and implemented these changes I would then open my shell and try SSH into the target machine using this command ssh -i {keypath} user@ip.

5. Identify Advantages/Disadvantages of the Solution

​

-Doing this would help to make your network safer but that being said there are multiple ways that an attacker might be able to gain unauthorized access to a network. Blocking an SSH connection is a great way to prevent a potential attacker from gaining remote access to a network. Other great ways to ensure that your network isn't going to be compromised is making sure you have strong security policies put into place beforehand ie. password policy. One thing we also did in the development of our ELK stack project was setting up firebeat and metricbeat, both of these were used to see incoming connections to our VMs, there are also many ways of monitoring these including SNORT.

Question 2:

1. Restate the Problem

-The problem is that you are running HTTP over port 80 which goes against your compliance guidelines that stipulates that all traffic should be done through encryption in motion. The easiest way to manage and solve this would be to run HTTPS which is encrypted, this would only allow encrypted traffic over your network.

2. Provide a Concrete Example Scenario

-During our project in creating an ELK stack all of our servers were running HTTP on port 80, the reason we allowed this is that we were running our servers over a private network so we weren't getting traffic from a public domain. In a controlled network on a private domain it is easy to control and monitor incoming traffic on our machines but if i was a large scale company it would make more sense to block all unencrypted traffic being that it could be malicious, you would also have more traffic from the internet which could open a slew of malicious activity. In a real deployment I would block HTTP over port 80 and rather use HTTPS over port 443 which is encrypted. In a bigger company with more sensitive data I would definitely want to encrypt the data that is being sent. In my personal ELK stack I would configure my Web-servers to only allow HTTPS traffic through the load balancer, that would ensure that all traffic that is coming through would be encrypted.

3. Explain the Solution Requirements

-Running HTTP on port 80 on a server is a potential problem because that data that you are sending won't be encrypted, this could lead to a data breach of sensitive information if we choose to send data to/form this server through a middle man attack. The easiest way to solve this problem is by changing the traffic from HTTP over port 80 to HTTPS over port 443 which is encrypted. This would be a safer way of transferring files over our network, although not completely safe it would make our server slightly safer. It solves the problem by encrypting our unencrypted traffic.

4. Explain the Solution Details

-I would go into the security group and VMs inbound rules and make sure to block HTTP over port 80 and I would allow HTTPS over port 443, this would block HTTP traffic and allow HTTPS traffic which is secure. I would also implement Kibana in my deployment to monitor any traffic in my network. I would obtain certifications to ensure that traffic is secure, I would generate a CSR to embed your public key to ensure a safe connection. I would implement monitoring software that would monitor all traffic going through our firewall to ensure that malicious traffic is being blocked. These tools would harden the deployment by being preventative opposed to reactive, this would help monitor that safe traffic would be maintained between the internet and servers.

5. Identify Advantages and Disadvantages of the Solution

- Will your solution break clients that used to communicate with the server over port `80`?

- Do you have to do any work to keep this solution running longterm? Or can you simply "set it and forget it?”

​

-My solution would break clients that used connections over port 80 being that we would be blocking all HTTP requests. The work that would have to be done is that these existing clients would have to switch from HTTP to HTTPS, this also as mentioned before has to do with our compliance guidelines and these clients wouldn't be an exception. It only ensures safer data transmission.