Activity File: Interview Questions

Domain: Network Security

1. Restate the Problem

It is important in the company network to close all unnecessary ports in firewall. To avoid hackers outside to access all network resources, data and other sensitive materials. Some companies are not closing some unnecessary ports on their firewalls and lead to network breach.

1. Provide a Concrete Example Scenario

In my project 1 of my Cybersecurity boot camp, I build my cloud firewall in Azure and only allow SSH traffic from my home public IP to my jump box-provision machine. My jump box has access to my 3 VM servers that has only private IP address and cannot access via public IP. I allow port 80 from my cloud firewall to access my public IP home network, so that I can access my DVWA website and Kibana. Just in real scenario, company should only allow needed ports and close the ports that is not needed so that to avoid network breaches. Although there is a lot of way hacker can access network company, but this is first step to protect network.

1. Explain the Solution Requirements

After I build my network Security Group (NSG) I configure to allow only SSH and HTTP traffics. My NSG allow inbound access to my jump box. Then I configured my NSG within the subnet to allowed connection only between the jump box and other local IP address.

1. Identify Advantages and Disadvantages

This solution is work with my project because only SSH and HTTP traffic allow my firewall. Firewall is one of the network security appliances that once it runs you never touch it unless there is a problem. It is hard to maintain all the ports in firewall because some applications required some certain ports need to be open to allow to access internal or outside company networks.

1. Explain the Solution Details.

To SSH to my jump box and access my DVWA website Kibana, I create inbound rules to allow SSH to my jump box provision via my public home IP, allow HTTP traffic via my home public IP, allow my load balancer where my 2 web servers connected to balance the load on both servers, I allow the traffic via my home public IP, allow my jump box to my virtual network to access my 3 internal VM server via SSH. For my Kibana server I build a separate NSG and create inbound rules to allow my Kibana webserver to my home public IP.