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?**

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

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

You can test these connections by first making sure that your jump box can connect to the designated web machines, after that try to connect to the web machine with a different workstation. Because the work station does not have the ssh key or the same ip as the jumpbox it should not connect to the web machines.

In the event that the web machine does allow the other workstation to connect via ssh you would have to troubleshoot the situation. I would start by checking my network security groups, in my groups I would make sure that all my rules are set correctly. After that I would verify that I have the ssh key set correctly. After checking and correcting any errors that may have been found. Verify your repair.

While this will make your network more secure, malicious actors might find another way to exploit a network, we can use monitoring to help watch traffic on our networks. You 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 you the ability to aggregate logs from all your systems and applications, analyze these logs, and create visualizations for application and infrastructure monitoring, faster troubleshooting, security analytics.

Question 2: Unsecured Web Server

Suppose you find a server running HTTP on port 80, despite compliance guidelines requiring encryption in motion. What do you do?

1. **Restate the Problem**

2. **Provide a Concrete Example Scenario**

    - **In Project 1, did you have servers running HTTP on port 80? If so, why was it permissible to do so?**

    - **In a real deployment, which specific machine would you configure differently? How, and why?**

3. **Explain the Solution Requirements**

    - **Why is running HTTP on port 80 a potential problem?**
    - **How would you reconfigure a server to serve HTTP traffic safely?**
    - **How does this solution fix the problem?**
4. **Explain the Solution Details**

    - **Which tools and technologies would you use to implement this solution in Project 1?**
    - **How, specifically, would you use these tools to harden your deployment?**
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?”**