**Network security**

\*\*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

According to compliance guidelines servers should not be running on port 80, this port should not be open. When you are running http off of port 80 you are violating the encryption in motion compliance guideline.

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?

The specific jump box server does allow HTTP to port 80- it allowed ssh to port 80 only from my IP address for testing purposes. It allows port 80 since this is a test server not being utilized in a real environment.

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

Since this is a test deployment running port 80 http to my home IP is allowable. But in a real deployment port 80 would not be open and instead would only allow filtered access for http.

3. Explain the Solution Requirements

- Why is running HTTP on port `80` a potential problem?

This is a well known port and therefore a thread when allowing unfiltered http web traffic to run through it.

- How would you reconfigure a server to serve HTTP traffic safely?

You could allow web traffic through port 80 but only allow filtered access within the inner data servers- not just open the port up for any kind of traffic. And for example a commercial website would allow port 80 traffic but have a firewall and a DMZ zone in between the website application and the inner data servers of the actual company.

- 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?

The network security group to create inbound and outbound rules to accommodate the filtering process.

- 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`?

No, because within the inbound and outbound rules it will be specified that they can still access the Jump-box via port 80.

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

Yes a system admin will have to modify the permissions and allow new users to be able to communicate with the server via port 80. With the Jump box and this specific solution you have to specify with users and IP addresses are allowed to do this. All other incoming traffic will be blocked within this specific Jump box project solution.

**#### Domain: Cloud Security**

**\*\*Question 1: Cloud Access Control\***\*

How would you control access to a cloud network?

1. Restate the Problem

It is one of the most important security tools an organization can have: controlling access to a cloud network. There are specific resources that let’s say the Sale’s Team has access to- we wouldn’t want them accessing the same resources that network engineers have access to. There’s a minimum necessary standard within healthcare that I think clearly defines this limitation. We want the Sale’s team to access everything essential to their workflow, and easily, but not have their access go beyond that.

2. Provide a Concrete Example Scenario

During a project within my cybersecurity bootcamp we created a test microsoft azure cloud environment just like this. We deployed multiple VMs within a virtual network in Azure- the only people who could access these were the instructors and the students. An organization would do something similar with their network engineers accessing this environment and no one else.

- In Project 1, did you deploy an on-premises or cloud network? I deployed a cloud network with ansible containers.

- Did you have to configure access controls to this network?

Yes these were apart of our network security groups.

- What kinds of access controls did you configure, and why were they necessary?

We deployed a rule that allowed only access via my personal IP to the Elk server.

- How do these details relate to the interview question?

The first step was to configure the network security for the Elk stack covering the whole subnet. All IP address traffic was blocked except for my own. This specific NSG only would allow traffic from one specific VM called the Jump box. You would then configure any other NSGs needed inside this specific subnet. I implemented SSH key access to avoid the threat of brute force password attacks.

3. Explain the Solution Requirements

- In Project 1, what kinds of access controls did you have to implement? Consider:

- NSGs around the VNet? Around the VMs?

NSGs around vnet- Elk-horn-nsg and Read\_Team\_nsg

- Local firewalls (ufw, etc.) on each VM?

Each VM had a UFW firewall wall around each of them, no complicated firewalls were assembled outside of this

- Protocol allow/deny lists?

Allow- allowing my IP address, TCP traffic, out of port 5601 destination IP elk private IP 10.1.0.4

Allow- allowing any source to SSH via port 22 with any destination. TCP traffic

Red\_Team\_nsg

Allow- IP address for source for Jumpbox private IP 10.0.0.4, TCP traffic, via port 122, allowing ssh connection via the jump box VM from the outside

Allow- my internal vnet IP address access via port 80, Any kind of traffic, port 80 traffic from the internet to internal vnet.

Allow- SSH from my IP address to jump box vm via any kind of traffic.

- What did each access control achieve, and why was this restriction necessary for the project?

SSH connections to port 80 were only allowed through the jump box through my internal IP address. No other access was necessary to complete testing procedures, so it was closed off to other IP and traffic. More restrictive access controls would’ve been implemented if this cloud network server was going to allow more outside traffic.

4. Explain the Solution Details

- Which rules do you set for each NSG in the network?

Ssh to port 22 for testing, allowing my IP 70.57.4.170 destination IP 10.1.0.4 destination port ranges 5601 allowing TCP traffic.

- How does access to the jump box work?

User who’s IP address is allowed to ssh, via port 80, using a public key that is input into the virtual machine’s specs. As long as the user inputs the correct public IP address of jumpbox into the command line along with the public key they will be allowed to access the server.

- How does access from the jump box to the web servers work?

Once the users are inside the jump box they can then ssh freely into the ansible containers using the private IP addresses, starting the containers and then attaching themselves to the containers. Once inside the containers they are able to ssh into the Elk-server used to run elk stack monitoring system.

5. Identify Advantages/Disadvantages of the Solution

- Does your solution scale?

For testing purposes this specific solution would be perfect if there was a small amount of users and an admin could easily add them so they can gain access. The shortcomings could come from a larger organization trying to use this- if too many users are trying to be provisioned to use this solution the administrative cost could be too high to maintain. When an update comes around only a single system needs this update.

- Is there a better solution than a jump box?

Another solution would be to establish an internal UFW firewall, this security system could handle much more capacity and more user’s could be provisioned to use the system. Another DMZ type security layer could be implemented instead of the jump box to handle larger numbers of users.

- What are the disadvantages of implementing a VPN that kept you from doing it this time?

VPNs aren’t supported on all devices at the moment, so implementing one on a large scale when they aren’t compatible with the Linux VMs we are using wouldn’t make sense. VPNs also have the potential to slow down your connection speed significantly and take up extra bandwidth on the network it is connecting to.

- What are the advantages of a VPN?

It can bypass firewalls set up by applications, you can go anywhere and still access all of the websites you need to. VPNs create a secure browsing experience that can potentially directly connect you to the internal network that is on prem.

- When is it appropriate to use a VPN?

When Linux VMs are not being used, Windows, MacOs and Android Os are much better equipped and compatible with VPNs (also annoyingly enough Chromebooks cannot use VPNs very well). When you need a solution that can handle a large amount of users that needs to be directly connected to their organization's network securely through tunneling.

**#### Domain: Logging and Monitoring**

**\*\*Question 1: Setting Alerts in a New Monitoring System\*\***

How do you determine which alerts to set in a new monitoring system?

Note: In Project 1, you did not set up any alerts. However, you still have enough experience to answer this question.

1. Restate the Problem

2. Provide a Concrete Example Scenario

- Describe the network you built for Project 1. Identify the VMs on the network and what they do.

The first VM we created is the Jump box Provisioner, this serves as a starting point and the only VM that allows outside access via port 80. A user is able to ssh with the public key into the jump box- this serves as a starting point to access the other VMs. They will also needs their IP address allowed via inbound security rules within the network security group for the jump box. Once the user is inside the jump box they are able to ssh via private IP to all the additional VMs- these are Web one, two and three. To connect to the specific Elk server that runs the Elk- stack system the user would need to connect, start, attach and then connect and ssh into the ansible container. From this specific container they are able to ssh via the private IP address of the Elk server into the elk environment.

- Which VMs should be publicly accessible?

Jump-Box-Provisioner

- Which VMs should not be publicly accessible?

Elk container, Web-1, Web-2, Web-3

3. Explain the Solution Requirements

- Consider the VMs that should not be publicly accessible from the internet. Which alert(s) should these VMs fire and when?

Log monitoring, whenever a user gets into the server via ssh, traffic monitoring the internal interface, any suspicious traffic attempting to get into these internal servers that are not recognized.

- Why should these VMs be associated with these alerts?

Since the only VM that is accessible from the outside is the Jump-box, all other traffic and logging data needs to be monitored so only specific users are accessing these sensitive servers. Security analysts needs to know who is accessing each VM at all times and if there is unnecessary access it needs to be looked into and researched.

4. Explain the Solution Details

- Which tool in Project 1 would you use to set such an alert?

Alert rules

- What would the alert rule be? For example, would the alert fire upon a failed SSH attempt or a ping request?

An alert would fire when anyone tries to ssh into any other VM except for the Jump-box. An alert would also fire if there was a failed ssh attempt into the Jump-box. Ping alerts would be utilized when someone is trying to contact any other inside VM besides the jump box- since those are internal no successful pings should happen for those VMs. All ping attempts needs to fire an alert and recorded.

5. Identify Advantages and Disadvantages

- Are there any malicious circumstances that the alert(s) discussed above do not address?

If this is an inside security threat from a user who has the public key and they are a verified user- these alerts would not prove to be useful. If they usually access the jump box and other VMs on a daily basis this activity would not seem abnormal- but their intentions might be malicious.