**Interview Activity**

**Chosen Domain: Cloud Security**

**Question 1: Cloud Access Control**

How would you control access to a cloud network?

1. Restate the Problem
    - **How would I regulate specific areas in a cloud network to special sets of rules?**

2. Provide a Concrete Example Scenario

    - In Project 1, did you deploy an on-premises or cloud network?
        - **Cloud network**
    - Did you have to configure access controls to this network?
        - **Yes**
    - What kinds of access controls did you configure, and why were they necessary?
        - **The access controls I configured was allowing ssh to port 22 from the Red Team virtual network by creating a security group and designating an inbound security rule.**
        - **This was necessary in order to gain access to ELK through port 22.**
    - How do these details relate to the interview question?
        - **These details relate to the interview question by demonstrating how access controls can aid an individual to protect their cloud-based framework by only allowing authorized users to work with classified files.**
3. Explain the Solution Requirements

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

        - **NSGs were placed around the ELK VNet and VMs while the firewalls were positioned around the VMS. TCP protocols were also part of the security rules.**
    - What did each access control achieve, and why was this restriction necessary for the project?
        - **NSGs were used to create rules that allowed or denied inbound network traffic which was necessary in order to specify where the port, source, destination, and protocols needed to be.**
        - **Local firewalls were used to eliminate any unwanted network communications.**
        - **The TCP was used to verify the data traveling from the two**

**endpoints from jump box to DVWAs**

4. Explain the Solution Details

    - Which rules do you set for each NSG in the network?
        - **Inbound traffic was set to the load balancers by setting the source IP and the destination to the virtual network. The protocol was TCP while the port was 80.**
    - How does access to the jump box work?
        - **Access to the jump box works by setting the personal IP to the source IP address and the destination to virtual networks. The port was set to 22 and protocol to any.**
    - How does access from the jump box to the web servers work?
        - **By allowing the internal ssh from the jumpbox by setting the source IP address to the destination to the virtual network. The port was 501 and protocol was set to any.**
5. Identify Advantages/Disadvantages of the Solution

    - Does your solution scale?
        - **Yes, the solution scales**.
    - Is there a better solution than a jump box?
        - **Although Jump box is good it also allows it to be exposed to organizations causing a lot of risks. By switching to a network traffic with zero trust security allows for better security.**
    - What are the disadvantages of implementing a VPN that kept you from doing it this time?
        - **The disadvantages is that it requires an in-depth understanding of public network security issues and proper deployment options while availability depends on factors widely outside of their control**
    - What are the advantages of a VPN?
        - **Advantages are that the VPN protects private data and gives remote and international locations better service quality**
    - When is it appropriate to use a VPN?
        - **It is appropriate to use a VPN when protecting data to make sure it can be accessed securely through various devices.**

**Question 2: Corporate VPN**

What are the advantages and disadvantages of using a corporate VPN, and under what circumstances is using one appropriate?

1. Restate the Problem
    - **What would be the pros and cons of using a corporate VPN and what**

**conditions are needed when using one?**

2. Provide a Concrete Example Scenario

    - In Project 1, which VMs did you have on the network?
        - **The VMs on the network were the Jumbox Provisioner, Web-1, Web-2, and ELKVM.**
    - Which tools did you use to control access to and from the network? **The Network Security group is what was used to control access to and from the network.**
    - If you didn't use a VPN, what did you use?
        - **I would use the Network Security group.**
    - What disadvantage(s) did your non-VPN solution have?
        - **The disadvantages would be that the network would have more of a chance of being easily compromised.**
    - What advantage(s) did your non-VPN solution have?

3. Explain the Solution Requirements

    - Would a VPN meet the access control requirements you had for Project 1?
        - **Yes because it allows a direct connection between the RedTeam-VNet and the ELK-VNet.**
    - How would a VPN protect the network just as well, or better, than your current solution?
        - **The VPN allows for an extra layer of security**

4. Explain the Solution Details

    - Which Azure tools would you use to implement a VPN to your Project 1 network?
    - **The tools I would use would be the Virtual Network tool followed by creating a Local Network Gateway and Gateway Subnet**
    - How would you onboard users to the new VPN system?

5. Identify Advantages and Disadvantages of the Solution

    - In Project 1, would a VPN have been an appropriate access control solution?
        - **Yes, a VPN would be appropriate.**

    - Under what circumstances is a VPN a good solution?
        - **A VPN is a good solution due to it being able to allow remote employees access to a company’s resources and being able to create a Tunnel across less secure networks that only authorized users can access.**

    - When, if ever, is a VPN "overkill"?
        - **It would be considered “overkill” when being used together with**

**another VPN or software application**

**Question 3: Containers**

When is it appropriate to use containers in cloud deployments, and what are the security benefits of doing so?

1. Restate the Problem

   **When can you use containers in cloud environments and how can you keep the network secure**

2. Provide a Concrete Example Scenario

   - In Project 1, when did you use containers?
     - **By starting and attaching the ansible container from the JumpBox provisioner and adding ELK to the group of host web servers within the ansible host file.**
   - What did you use containers for?
     - **The containers were used to configure the ELK VM.**

3. Explain the Solution Requirements

   - Why was this an appropriate use for containers?
     - **This was an appropriate use for containers because it's a lot faster and uses only a fraction of the memory when in comparison to a VM.**
   - What security benefits did you expect from using containers?
     - **The security benefits from using the containers is that there is no interaction between the containers allowing a decrease in security risks**.

4. Explain the Solution Details

   - In Project 1, how did you configure VMs to be able to run containers?

     - **I configured the VMs by adding their web servers to the container host files and then created a playbook that permitted them to run containers.**
   - How did you select and install the correct container?
     - **I was able to select and install the correct container by running the YAML file**
   - How did you verify that it was running correctly?
     - **I verified it by running the ansible playbook with the specific VM**

5. Identify Advantages/Disadvantages of the Solution

- How would you have achieved the same thing without containers?
  - **You could only use Virtual Machines**
- What are the advantages to doing it without containers?
  - **With VMs it is better with guest compatibility due to it being able to run any operating system**
- What are the disadvantages?
  - **The disadvantages are that it requires more memory, CPU, and storage.**

**Question 4: Cloud Infrastructure as Code**

What are the security benefits of defining cloud infrastructure as code?

1. Restate the Problem
   **What are the security advantages of presenting cloud infrastructure as code?**
2. Provide a Concrete Example Scenario
   - In Project 1, when did you use infrastructure as code (IaC)?
     - **I used it to create a playbook file**
   - What tool did you use?
     - **Docker**
   - What did you use it to do?
     - **Configure ELK**
3. Explain the Solution Requirements
   - Were there any alternatives to IaC?
     - **Yes, Service provisioning**
   - What benefits does IaC have over alternative approaches?
     - **It allows you to program your infrastructure**
4. Explain the Solution Details
   - In Project 1, which specific configurations did your IaC set up?

**- name: Config ELK with Docker**

**hosts: elk**

**become: true**

**tasks:**

**- name: Install docker.io**

```
apt:

update_cache: yes
name: docker.io

state: present

- name: Install pip3

apt:

force_apt_get: yes

name: python3-pip

state: present

- name: Install Docker Python Module

pip:

name: docker

state: present

- name: Download and launch a Docker web container

docker_container:

name: elk

image: sebp/elk:761

state: started

restart_policy: always

published_ports:

- 5601:5601

- 9200:9200

- 5044:5044
```

**- name: Configure elk VM to use more memory**

**sysctl:**

**name: vm.max_map_count**
**value: "262144"**

**state: present**

- How did you run and test these configurations?
  - **By running the playing ansible-playbook elk-playbook.yml**

5. Identify Advantages/Disadvantages of the Solution

- Are there any disadvantages to using IaC over the "traditional" approach?
  - **Bad configurations can be replicated on all servers**
  - **Requires you to choose the right tools **very specific**