Activity File: Interview Questions

- This first project covers a wide range of topics including cloud, network security, and logging and monitoring.
- When networking and talking to potential employers, you should be able to reference the work done on this project to answer specific interview questions or demonstrate your skills within a specific domain.
- You will choose a domain that you're interested in pursuing as a career and answer mock questions based on the suggested response format.

Instructions

1. Choose one of the following domains:

    - Network security
    - Cloud security
    - Logging and monitoring

    If you are unsure of which domain you want to focus on, that's okay. You can either choose the one you're most comfortable discussing, or complete the tasks in two or all three domains.

2. Select one domain and one question.

    - Questions are provided for each domain. Choose one to answer from your chosen domain.

3. Write a one-page response that answers the question using specific examples from your work on Project 1. Your response should flow and read like a presentation while keeping the general structure of the technical question response guidelines.

    You will submit this one-page response.

Reminder: Response Guidelines

As a reminder, good responses do the following. 1. Restate the problem. 2. Provide a concrete

example scenario. 3. Explain the solution requirements. 4. Explain the solution details. 5. Identify advantages and disadvantages of the solution. Including each of these components will ensure you prove your competency of subject matter and critical thinking.

Interview Questions by Domain

Below you will find a list of questions, grouped by specific domains. Select one question to answer.

For each question, where appropriate, we have provided you with specific prompts to consider as you structure each section of your response. Feel free to use these prompts or your own examples.

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?

Make sure each section of your response answers the questions laid out below. 1. Restate the Problem

1. Provide a Concrete Example Scenario
    - In Project 1, did you allow SSH traffic to all of the VMs on your network?
    - Which VMs did accept SSH connections?
    - What happens if you try to connect to a VM that does not accept SSH connections? Why?
2. Explain the Solution Requirements
    - If one of your Project 1 VMs accepted SSH connections, what would you assume the source of the error is?
    - Which general configurations would you double-check?
    - What actions would you take to test that your new configurations are effective?
3. Explain the Solution Details
    - Which specific panes in the Azure UI would you look at to investigate the problem?
    - Which specific configurations and controls would you check?
    - What would you look for, specifically?

- How would you attempt to connect to your VMs to test that your fix is effective?

4. Identify Advantages/Disadvantages of the Solution

    - Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access?

    - What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?

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

1. 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?

2. 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?

3. 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?

4. 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?”

Domain: Cloud Security

Question 1: Cloud Access Control

How would you control access to a cloud network?

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 1, did you deploy an on-premises or cloud network?
    - Did you have to configure access controls to this network?
    - What kinds of access controls did you configure, and why were they necessary?
    - How do these details relate to the interview question?
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?
        - Local firewalls (ufw, etc.) on each VM?
        - Protocol allow/deny lists?
    - What did each access control achieve, and why was this restriction necessary for the project?
4. Explain the Solution Details
    - Which rules do you set for each NSG in the network?
    - How does access to the jump box work?
    - How does access from the jump box to the web servers work?
5. Identify Advantages/Disadvantages of the Solution
    - Does your solution scale?
    - Is there a better solution than a jump box?
    - What are the disadvantages of implementing a VPN that kept you from doing it this time?
    - What are the advantages of a VPN?
    - When is it appropriate to use a VPN?

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

2. Provide a Concrete Example Scenario

    - In Project 1, which VMs did you have on the network?
    - Which tools did you use to control access to and from the network?
    - If you didn't use a VPN, what did you use?
    - What disadvantage(s) did your non-VPN solution have?
    - 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?
    - How would a VPN protect the network just as well, or better, than your current solution?

4. Explain the Solution Details

    - Which Azure tools would you use to implement a VPN to your Project 1 network?
    - 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?
    - Under what circumstances is a VPN a good solution?
    - When, if ever, is a VPN "overkill"?

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

2. Provide a Concrete Example Scenario

    - In Project 1, when did you use containers?
    - What did you use containers for?

3. Explain the Solution Requirements

    - Why was this an appropriate use for containers?
    - What security benefits did you expect from using containers?

4. Explain the Solution Details

    - In Project 1, how did you configure VMs to be able to run containers?
    - How did you select and install the correct container?
    - How did you verify that it was running correctly?

5. Identify Advantages/Disadvantages of the Solution

    - How would you have achieved the same thing without containers?
    - What are the advantages to doing it without containers?
    - What are the disadvantages?

Question 4: Cloud Infrastructure as Code

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

1. Restate the Problem

2. Provide a Concrete Example Scenario

    - In Project 1, when did you use infrastructure as code (IaC)?
    - What tool did you use?
    - What did you use it to do?

3. Explain the Solution Requirements

    - Were there any alternatives to IaC?
    - What benefits does IaC have over alternative approaches?

4. Explain the Solution Details

    - In Project 1, which specific configurations did your IaC set up?
    - How did you run and test these configurations?

5. Identify Advantages/Disadvantages of the Solution

    - Are there any disadvantages to using IaC over the "traditional" approach?

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.
    - Which VMs should be publicly accessible?
    - Which VMs should not be publicly accessible?
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?
    - Why should these VMs be associated with these alerts?
4. Explain the Solution Details
    - Which tool in Project 1 would you use to set such an alert?
    - What would the alert rule be? For example, would the alert fire upon a failed SSH attempt or a ping request?
5. Identify Advantages and Disadvantages
    - Are there any malicious circumstances that the alert(s) discussed above do not address?

Question 2: Challenges of Collecting Large Amounts of Log Data

What are the challenges of collecting huge amounts of log data? How do security analysts deal with them?

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 1, when did you deal with log data?
    - What kind(s) of data did you investigate?
    - How much data were you dealing with?

- What were you looking for?

3. Explain the Solution Requirements

    - What information did you need to find what you were looking for?
    - What does an analyst need to analyze large amounts of log data to find this information?
    - In Project 1, what tools did you use to analyze log data?

4. Explain the Solution Details

    - How did you use these tools to find the log data? E.g., which charts, graphs, etc. were useful for parsing the logs?

5. Identify Advantages and Disadvantages of the Solution

    - What kinds of data did you not inspect during Project 1?
    - Would having access to this additional data have changed your process or conclusions? If so, how?

Question 3: Escalating Security Events

How do you determine if a security event or alert is important enough for escalation?

1. Restate the Problem

2. Provide a Concrete Example Scenario

    - What kinds of events and alerts did you encounter in Project 1?
    - Which of these events was most interesting or suspicious?
    - Why was the event suspicious? What led you to investigate it?

3. Explain the Solution Requirements

    - What do you need to figure out in order to determine if this event is worth escalating?

4. Explain the Solution Details

    - How did you use Kibana to find this information?

5. Identify Advantages and Disadvantages of the Solution

    - How confident are you in your conclusion?
    - What additional data would be useful to determine if your conclusions are correct?
