**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 question below from each of the following domains:
   * Network security
   * Cloud security
   * Logging and monitoring
2. Write a 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?

1. Restate the Problem
   1. How would debug a firewall that was designed to block SSH connections, but in reality lets them through. I would check first all traffic rules established, I would also see what connections have been established for all of the vms.

Make sure each section of your response answers the questions laid out below. ​

1. Provide a Concrete Example Scenario
   * In Project 1, did you allow SSH traffic to all of the VMs on your network?
   * A.) No
   * Which VMs did accept SSH connections?
   * A.) Jumpbox
   * What happens if you try to connect to a VM that does not accept SSH connections? Why?
   * A.) It doesn’t work, the pathway isn’t built. Or there is a rule that is blocking traffic
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?
   * A.) the rules put in place during the building of that VM are sound, that a either the peering was made sound, but some how the others were build incorrectly. Or the Ip addresses for the other VMs are incorrect.
   * Which general configurations would you double-check?
   * A.) peerings
   * What actions would you take to test that your new configurations are effective?
   * A.) Allowable access through which ports, and priorities of rules
3. Explain the Solution Details
   * Which specific panes in the Azure UI would you look at to investigate the problem?
   * A.) Virtual Networks, NSG’s possibly the Load balancers then Access Control (IAM),
   * Which specific configurations and controls would you check?
   * A.) Peerings, Resource groups, Inbound Security rules
   * What would you look for, specifically?
   * A.) Containers, Source Ips, Destination, Protocol, settings,
   * How would you attempt to connect to your VMs to test that your fix is effective?
   * A.) Rebuild the VM if need be, from the ground up, so as to solidify the standard of the network and the transfer of data.
4. Identify Advantages/Disadvantages of the Solution
   * Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access?
   * A.) no
   * What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?​
   * A.) Incoming traffic rules and adjustments rules made for access to the network

**Domain: Cloud Security**

**Question 1: Cloud Access Control**

How would you control access to a cloud network?

1. Restate the Problem

A.)I would control access to a cloud network with IAM, Identity and access Management. This would focus on policies and practices both physical and electronic. Put emphasis on monitoring unauthorized internal and external access, internal misuse, internal or external modification and outside verifiable threats. Stay ahead of the curve on vulnerabilities of the network and areas of opportunity

1. Provide a Concrete Example Scenario
   * In Project 1, did you deploy an on-premises or cloud network?
   * A.) Cloud Network
   * Did you have to configure access controls to this network?
   * A.) Yes, ansible
   * What kinds of access controls did you configure, and why were they necessary?
   * A.) Limited Remote access, mandating that my IP be key in accessing the network.
   * How do these details relate to the interview question?
   * A.) Shows the different options for developing a computer and a network,. Understanding the difference between on-site physical equipment and cloud services plays a huge role in how the network will take shape. It also plays a huge role in cost efficiency.
2. 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?
     + A.) I created two network security groups for this project Red\_team3NSG and the main one ElkProject1VM-nsg
     + Local firewalls (ufw, etc.) on each VM?
     + A.) the NSG along with the Red-Team3\_LoaD\_Balancer
     + Protocol allow/deny lists?
     + A.) VM must use the same SSH keys as your WebVM's and then added my public IP address to the whitelist
   * What did each access control achieve, and why was this restriction necessary for the project?
   * A.) SSh keys allow for a single access to the VMS. The NSG’s that allows for limited TCP traffic over port 5601
3. Explain the Solution Details
   * Which rules do you set for each NSG in the network?
   * A.) Added my public IP to the whitelist, we created an incoming rule for the security group that allows TCP traffic over port 5601 from my Public IP.
   * How does access to the jump box work?
   * A.) Command ssh -i <private key path> [azadmin@52.183.92.55](mailto:azadmin@52.183.92.55)
   * How does access from the jump box to the web servers work?
   * A.) the IP address is confirmed and the port access is allowed
4. Identify Advantages/Disadvantages of the Solution
   * Does your solution scale?
   * A.) no, it’s time consuming, But rebuilding the VM to possibly rebuilding the entire network is the most logical way of solving any ills and making sure that the the issue does not persist.
   * Is there a better solution than a jump box?
   * A.) Not for this project. although a VPN would imo be more secure
   * What are the disadvantages of implementing a VPN that kept you from doing it this time?
   * A.) Cost, and the idea that it’s not applicable for the size of this project.
   * What are the advantages of a VPN?
   * A.) Security, shuts down almost any spying of your network, creates an understood pathway that keeps the company functional.
   * When is it appropriate to use a VPN?
   * A.) Any time the money makes sense for such an application. If the size of the company and the traffic along the VPN adds up then make the VPN a prior

**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. One of the advantages of using a corporate VPN, is the security. The pathways are established, basically you won’t have to deal with some of the GEO-restrictions and the idea of someone spying on you is little to none. The VPN also give you access to the web with secure links, and flow of date can be legitimately faster if everything is done right, meaning you have the right tech to run the VPN. The main disadvantages of a corporate VPN is that is a real chance that speeds can slow down due to encryption, distance and if you are dealing with a wide variety of tech that may not match up. Cost is also a potential disadvantage.
3. Provide a Concrete Example Scenario
   * In Project 1, which VMs did you have on the network?
   * A.) [ElkProject1VM](https://portal.azure.com/#@Tsolidsolgmail.onmicrosoft.com/resource/subscriptions/fe48d39c-5238-4380-9646-eadbf10ab02b/resourceGroups/Red-Team3/providers/Microsoft.Compute/virtualMachines/ElkProject1VM), [JuMpBox-Pro](https://portal.azure.com/#@Tsolidsolgmail.onmicrosoft.com/resource/subscriptions/fe48d39c-5238-4380-9646-eadbf10ab02b/resourceGroups/Red-Team3/providers/Microsoft.Compute/virtualMachines/JuMpBox-Pro), [Web-1](https://portal.azure.com/#@Tsolidsolgmail.onmicrosoft.com/resource/subscriptions/fe48d39c-5238-4380-9646-eadbf10ab02b/resourceGroups/Red-Team3/providers/Microsoft.Compute/virtualMachines/Web-1), [Web-2](https://portal.azure.com/#@Tsolidsolgmail.onmicrosoft.com/resource/subscriptions/fe48d39c-5238-4380-9646-eadbf10ab02b/resourceGroups/Red-Team3/providers/Microsoft.Compute/virtualMachines/Web-2)
   * Which tools did you use to control access to and from the network?
   * A.) Red\_team3NSG and ElkProject1VM-nsg and Ansible container, SSH keys, Rules
   * If you didn't use a VPN, what did you use?
   * A.) Red-Team3\_LoaD\_Balancer
   * What disadvantage(s) did your non-VPN solution have?
   * A.) The flow of traffic between the VMs, was slower and bit more time consuming.
   * What advantage(s) did your non-VPN solution have?
   * A.) Security was stronger in my opinion,
4. Explain the Solution Requirements
   * Would a VPN meet the access control requirements you had for Project 1?
   * A.) Possibly with the The VM had to use the same SSH Keys as the WebVM’s.
   * How would a VPN protect the network just as well, or better, than your current solution?
   * A.) VPN’s by nature create a secure tunnel for date to process through, VPN’s scramble all of the traffic in this tunnel with encryption. Which limits if not completely negates all outside monitoring. A VPN can and will encrypts all of the connections.
5. Explain the Solution Details
   * Which Azure tools would you use to implement a VPN to your Project 1 network?
   * A.) Ansible Containers, SSH
   * How would you onboard users to the new VPN system?
   * A.) Jump-box
6. Identify Advantages and Disadvantages of the Solution
   * In Project 1, would a VPN have been an appropriate access control solution?
   * A.) I believe that a VPN could work
   * Under what circumstances is a VPN a good solution?
   * A.) level of traffic and amount of users, kind of the same thing.
   * When, if ever, is a VPN "overkill"?
   * A.) Smaller companies, with limited need for access to the outside interent.

**Domain: Logging and Monitoring**

**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. “What are the challenges of collecting huge amounts of log data? How do security analysts deal with them.. The issue/challenges with collecting huge amounts of log date, is storage and processing. Does it make sense to store all of that date?
3. Provide a Concrete Example Scenario
   * In Project 1, when did you deal with log data?
   * A.) first instance would be with the creation of the VMs, deciding how much storage capacity and processing capabilities to give the machines and deciding if it was cost effective. Understanding what to anticipate for on a daily basis, and then preparing for the worst.
   * What kind(s) of data did you investigate?
   * A.) Log Nominal, ratio data. Followed by and mainly or Processing and storage
   * How much data were you dealing with?
   * A.) terabytes
   * What were you looking for?
   * A.)
4. Explain the Solution Requirements
   * What information did you need to find what you were looking for?
   * A.) IP address, Command line,
   * What does an analyst need to analyze large amounts of log data to find this information?
   * A.)Proper equipment, Servers, firewalls Event log archiving/ analyzer , Flexible Log parser,
   * In Project 1, what tools did you use to analyze log data?
   * A.) Git bash, Ansible, Azure
5. 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?
   * A.)Yes, helped me to Organized the data and the systems, allows
6. Identify Advantages and Disadvantages of the Solution
   * What kinds of data did you not inspect during Project 1?
   * A.) Physical options for Cloud replacement.
   * Would having access to this additional data have changed your process or conclusions? If so, how?
   * A.) possible, if I would have had access to more security options, this could have changed the project.