## Activity File 4: 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.

1. Select one domain and one question.
   * Questions are provided for each domain. Choose one to answer from your chosen domain. ​
2. 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

*Firewall can be faulty due to misconfiguration and this causes over 95% of the firewall breaches. A faulty firewall means that firewall has incorrect configurations sue to lack of research. Configuring a firewall requires precise planning and an accurate workflow – only an expert would know where to start. Yet, all too often, the person responsible for firewall configuration doesn’t select the appropriate settings from the access control list.*

*Human error is usually to blame for misconfigurations, and you don’t have to look far to understand why. For example, in network device configuration, ‘eq’ (‘equal to’) allows access to a single, specified port – whereas ‘neq’ (‘not equal to’) allow access to any other service. The typo of a single ‘n’ can reverse an entire traffic path from being incredibly niche to incredibly broad!*

1. Provide a Concrete Example Scenario
   * In Project 1, did you allow SSH traffic to all of the VMs on your network?
   * The ssh traffic was allowed to all.
   * Which VMs did accept SSH connections?
   * *All VMs accepted 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?

*The source of error is firewall misconfiguration to accept ssh connections.*

* + Which general configurations would you double-check?

*The firewall zones and IP addresses were not protected, therefore will need to be architect and reconfigured.*

*When using firewall, the internal IP addresses should be used for all internal networks. The NAT must therefore be configured to allow internal devices to communicate on the internet whenever necessary.*

*The next setting is establishing a network firewall zone and assign them to the firewall sub interfaced. As you build out your network infrastructure, switches that support virtual LANs (VLANs) should be used to maintain level-2 separation between the networks.*

* + What actions would you take to test that your new configurations are effective?

1. Explain the Solution Details
   * Which specific panes in the Azure UI would you look at to investigate the problem?

The panes include subnet, then click on AzureFirewall of choice.

* + Which specific configurations and controls would you check?

The configurations include defining NAT rules, network rule collection and Application rule collections. The priority would be set to 1000 and action is set to allow. The IP address name is set to Allow

* + What would you look for, specifically?

The general process to create a network rule collection that allows DNS resolution traffic. In this case, let's imagine we want to use Google's public DNS servers, 8.8.8.8 and 8.8.4.4.

*Name: workload-network-rule-collection*

*Priority: 1000*

*Action: Allow*

*IP Addresses name: allow-dns-goog*

*Protocol: UDP, TCP*

*Source Addresses: 10.30.2.0/24 (again, this is our workload subnet network ID)*

*Destination Addresses: 8.8.8.8,8.8.4.4 (you can input multiple values by separating them with a comma)*

*Destination Ports: 53*

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

*The Azure diagnostic tools can be used in testing connectivity.*

1. Identify Advantages/Disadvantages of the Solution
   * Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access?

*The new solution guarantees immunity to the network, after test, there is no unauthorized ssh access.*

* + What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?​

*The controls were monitored through Azure Active Directory Privileged Identity Management (PIM)*

**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

*When there is any open ports, it means that the port may be open for use, therefore the action is to close the port.*

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?
   * *The following ports were left open for HTTP (443) HTTP (80) and SSH (22). In case of configuring any port, you must first open necessary ports using Azure Management console.*
   * In a real deployment, which specific machine would you configure differently? How, and why?
   * *Database server can be configured differently. This is important since there is additional need to protect data.*
2. Explain the Solution Requirements
   * Why is running HTTP on port 80 a potential problem?
   * *There are many attacks that take place in port 80, the attacks range from several web clients such as SQL Injections, cross-site requests and buffer overruns. Most attackers therefore use these ports to attack a server, therefore, the ports should remain closed.*
   * How would you reconfigure a server to serve HTTP traffic safely?
   * *Loging through ssh can be moved higher so that the hackers find it difficult to attack the server. It can also be harder for the attacker to locate the attack surface for ssh service.*
   * How does this solution fix the problem?
   * *The solution helps in making it harder for the attacker to launch a successful attack on a server.*
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?
   * *The solution will block the clients that use port 80, such as SQL injection.*
   * Do you have to do any work to keep this solution running long-term? Or can you simply "set it and forget it?”
   * *The solution can be set once but there is also chance to constantly review the allocation of active ports.*

#### Domain: Cloud Security

**Question 1: Cloud Access Control**

How would you control access to a cloud network?

1. Restate the Problem

*It is important to have an access control so that only authorized virtual devices are allowed access to devices. There is also need to have control on the virtual network and subnet provisioning and also IP addressing. Therefore, to prevent attacks, it is important to segment the subnets and use the private IP addresses that are available*.

1. Provide a Concrete Example Scenario
   * In Project 1, did you deploy an on-premises or cloud network?
   * *The project was deployed on cloud*
   * Did you have to configure access controls to this network?
   * *Yes, the allow rules were denied in broad range of IP addresses, including 0.0.0.0.0 to 255.255.255.255.*
   * What kinds of access controls did you configure, and why were they necessary?
   * *What access control was done using RBAC. It allowed a single user to manage machines and virtual networks. It also allows users to manage all resource groups that include virtual machines websites and subnets.*
   * How do these details relate to the interview question?
   * *Access control is important in managing resources in cloud platform.*
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?
     + *The access control approach in the VM include allowing one user to manage SQL databases, allow one user to manage the resources in resource groups such as virtual machines and websites. An application was used in accessing all resources in a resource group.*
     + Local firewalls (ufw, etc.) on each VM?
     + Every virtual machine had firewall nstalled to filter traffic.
     + Protocol allow/deny lists?
     + The following range of IP’s were allowed in the network

| **IP V4 ranges** | **IP V6 ranges** |
| --- | --- |
| 13.107.6.0/24 | 2620:1ec:4::/48 |
| 13.107.9.0/24 | 2620:1ec:a92::/48 |
| 13.107.42.0/24 | 2620:1ec:21::/48 |
| 13.107.43.0/24 | 2620:1ec:22::/48 |

* + What did each access control achieve, and why was this restriction necessary for the project?
  + *Each of the access control achieved restricted access to the data and ensured that there is no unauthorized access to information.*

1. Explain the Solution Details
   * Which rules do you set for each NSG in the network?
   * *The domain \*.dev.azure.com were left to allow. The URLs that support signing and licensing connections are also set to allow. They include login.live.com, go.microsoft.com, app.vssps.dev.azure.com.*
   * How does access to the jump box work?
   * *The access to jump-box prevents working on the main server, so that if there are errors that can be made are done on the jump-box but not on the server. Only final commits are reflected on the live server. They are therefore secure environments that are not used for non-administrative purposes.*
   * How does access from the jump box to the web servers work?
   * *The connection from the jump-box to the server uses telnet/ssh services and this is done via authentication using the standard username or password.*
2. Identify Advantages/Disadvantages of the Solution
   * Does your solution scale?
   * *The use of jump-box can be scaled to manage many VMs.*
   * Is there a better solution than a jump box?
   * *There are many solutions that can be a better alternative to jump-box, an example to wrike that gives a better bird’s view of the progress of the administrator’s efforts.*
   * What are the disadvantages of implementing a VPN that kept you from doing it this time?
   * *There are countries where the use of VPN is prohibited, VPN also might have Private Network. This means that people might create a performance problem in the process. Mot connections through VPN is also slower than when using apps like jump-box. There are VPN’s that also monitor data, making them even more vulnerable to attacks.*
   * What are the advantages of a VPN?
   * *VPN is important in hiding private information, it can hide private data such as web browsers from accessing connections. There are some secure VPNs that provide military grade 256 data encryption. VPN can be used in avoiding bandwidth throttling and even having allowing down the connection speed.*
   * When is it appropriate to use a VPN?
   * *VPN can be used in accessing blocked services such as Netflix.*

**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

*A corporate VPN offers organizations the opportunity to provide their employees access to a secure end-to-end encrypted connection to cloud resources on a company network. A corporate VPN encryption provides a secure network connection to the employee’s devices, no matter where employees are working.*

*Transform your organization’s remote corporate access with our seamless, secure and highly scalable Corporate VPN. Perimeter 81’s innovative and easy-to-use solution provides businesses the ability to manage and protect their private cloud resources from critical attacks on their network.*

1. Provide a Concrete Example Scenario
   * In Project 1, which VMs did you have on the network?
   * *In project 1, there are two VMs used in the network.*
   * Which tools did you use to control access to and from the network?
   * *In Azure, there are virtual network, Azure Private Network Link and creating NSG having a security configuration. Another security tool is a jump-box.*
   * If you didn't use a VPN, what did you use?
   * *When there is no VPN a jump-box is used.*
   * What disadvantage(s) did your non-VPN solution have?
   * *Jump-box are free and secure. They are also easy to use.*
   * What advantage(s) did your non-VPN solution have?
   * *From the security side, the jump box becomes a target, and in theory, would be easier to compromise than a true firewall. Even if a software firewall was running on the jump box system, I'm sure someone would knock that approach.*
2. Explain the Solution Requirements
   * Would a VPN meet the access control requirements you had for Project 1?
   * The corporate VPN would provide all security requirements required in section 1.
   * How would a VPN protect the network just as well, or better, than your current solution?
   * *A VPN is better than a jump-box because they cannot be easily be compromised.*
3. Explain the Solution Details
   * Which Azure tools would you use to implement a VPN to your Project 1 network?
   * *There are two tools, Azure VPN with perimeter 81, Azure security is more effective with our cloud solution, which enables monitoring across all your resources, protecting even your most inconsequential data.*
   * How would you onboard users to the new VPN system?
   * *Azure VPN Gateway connects your on-premises networks to Azure through Site-to-Site VPNs in a similar way that you set up and connect to a remote branch office. The connectivity is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).*
4. Identify Advantages and Disadvantages of the Solution
   * In Project 1, would a VPN have been an appropriate access control solution?
   * *There are countries where the use of VPN is prohibited, VPN also might have Private Network. This means that people might create a performance problem in the process. Mot connections through VPN is also slower than when using apps like jump-box. There are VPN’s that also monitor data, making them even more vulnerable to attacks.*
   * Under what circumstances is a VPN a good solution?
   * *VPN is important in hiding private information, it can hide private data such as web browsers from accessing connections. There are some secure VPNs that provide military grade 256 data encryption. VPN can be used in avoiding bandwidth throttling and even having allowing down the connection speed.*
   * When, if ever, is a VPN "overkill"?
   * *VPN can be used in accessing blocked services such as Netflix.*

**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

*Containers offer a logical packaging mechanism in which applications can be abstracted from the environment in which they actually run. This decoupling allows container-based applications to be deployed easily and consistently, regardless of whether the target environment is a private data center, the public cloud, or even a developer’s personal laptop. Containerization provides a clean separation of concerns, as developers focus on their application logic and dependencies, while IT operations teams can focus on deployment and management without bothering with application details such as specific software versions and configurations specific to the app.*

1. Provide a Concrete Example Scenario
   * In Project 1, when did you use containers?
   * *A container is a readymade software environment that has the application code and its dependency's preloaded within an image. ... The container engine allows each application (container) to run on top of the host operating system but remain isolated from each other*
   * What did you use containers for?
   * *Save costs by lifting and shifting your existing applications to containers, and build micro services applications to deliver value to your users faster. Use end-to-end developer and CI/CD tools to develop, update, and deploy your containerized applications*
2. Explain the Solution Requirements
   * Why was this an appropriate use for containers?
   * *Azure Container Instances enables exposing your container groups directly to the internet with an IP address and a fully qualified domain name (FQDN). When you create a container instance, you can specify a custom DNS name label so your application is reachable at customlabel.azureregion.azurecontainer.io.*
   * What security benefits did you expect from using containers?
   * *Azure Container Instances also supports executing a command in a running container by providing an interactive shell to help with application development and troubleshooting. Access takes places over HTTPS, using TLS to secure client connections.*
3. Explain the Solution Details
   * In Project 1, how did you configure VMs to be able to run containers?
   * *Azure Container Instances enables deployment of container instances into an Azure virtual network. When deployed into a subnet within your virtual network, container instances can communicate securely with other resources in the virtual network, including those that are on premises (through VPN gateway or ExpressRoute).*
   * How did you select and install the correct container?
   * How did you verify that it was running correctly?
4. Identify Advantages/Disadvantages of the Solution
   * How would you have achieved the same thing without containers?
   * *There are no alternatives to containers*
   * What are the advantages to doing it without containers?
   * *Containers need special skills to implement.*
   * What are the disadvantages?
   * It becomes difficult to manage resources without use of containers.

**Question 4: Cloud Infrastructure as Code**

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

1. Restate the Problem

*Infrastructure as code is the process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.*

1. Provide a Concrete Example Scenario
   * In Project 1, when did you use infrastructure as code (IaC)?
   * Cloud computing is far from being a panacea, though. While it allows you to set up your infrastructure needs quickly—thus solving severe problems such as high availability and scalability—it does nothing to solve the inconsistency issues. When you have more than one person performing the configurations, you’re bound to get discrepancies.
   * What tool did you use?
   * *IaC tools can vary as far as the specifics of how they work, but we can generally divide them into two main types: the ones that follow the imperative approach, and the ones who follow the declarative approach.*
   * What did you use it to do?
   * *The first significant benefit IaC provides is speed. Infrastructure as code enables you to quickly set up your complete infrastructure by running a script. You can do that for every environment, from development to production, passing through staging, QA, and more. IaC can make the entire software development lifecycle more efficient.*
2. Explain the Solution Requirements
   * Were there any alternatives to IaC?
   * *Configuration orchestration tools, which include Terraform and AWS CloudFormation, are designed to automate the deployment of servers and other infrastructure.*
   * *Configuration management tools like Chef, Puppet, and the others on this list help configure the software and systems on this infrastructure that has already been provisioned*
   * What benefits does IaC have over alternative approaches?
   * ***Consistency****: Manual processes result in mistakes, period. Humans are fallible. Our memories fault us. Communication is hard, and we are in general pretty bad at it. As you’ve read, manual infrastructure management will result in discrepancies, no matter how hard you try.*
   * *Accountability: This one is quick and easy. Since you can version IaC configuration files like any source code file, you have full traceability of the changes each configuration suffered. No more guessing games about who did what and when*
3. Explain the Solution Details
   * In Project 1, which specific configurations did your IaC set up?
   * *Azure Resource Manager allows you to define the infrastructure and dependencies for your app in templates, organize dependent resources into groups that can be deployed or deleted in a single action, control access to resources through user permissions, and more.*
   * How did you run and test these configurations?
   * *NixOS also makes it very easy to rollback to a prior configuration, since new configuration files don’t overwrite old ones. NixOS can therefore be used to view the current IaC configurations.*
4. Identify Advantages/Disadvantages of the Solution
   * Are there any disadvantages to using IaC over the "traditional" approach?
   * **More Efficiency During the Whole Software Development Cycle:**
   * *By employing infrastructure as code, you can deploy your infrastructure architectures in many stages. That makes the whole software development lif cycle more efficient, raising the team’s productivity to new levels.*
   * *You could have programmers using IaC to create and launch sandbox environments, allowing them to develop in isolation safely. The same would be true for QA professionals, who can have perfect copies of the production environments in which to run their tests. Finally, when it’s deployment time, you can push both infrastructure and code to production in one step*.

#### 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

*A security Alert is determined using Azure platform using the alert system. The alert can be grouped in terms of their severity. The system can make alert on long events, long search queries and tests for website availability. The alerts can be grouped as follows; New showing that the issue has been detected, acknowledged means that the alert is being worked on and closed means that the issue has been addressed.*

1. Provide a Concrete Example Scenario
   * Describe the network you built for Project 1. Identify the VMs on the network and what they do.
   * *The network build has one VM for monitoring network traffic.*
   * Which VMs should be publicly accessible?
   * *Only non-administrative VMs should be publicly available.*
   * Which VMs should not be publicly accessible?
   * *The VM used in administrative use should not be accessible to the public.*
2. 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?
   * *The alerts include system overload*,
   * Why should these VMs be associated with these alerts?
   * *The alerts are important in monitoring attacks online.*
3. Explain the Solution Details
   * Which tool in Project 1 would you use to set such an alert?
   * *The create rule tool was used in making the alerts in the Virtual Machine.*
   * What would the alert rule be? For example, would the alert fire upon a failed SSH attempt or a ping request?
   * *The alerts that can be set include Azure billing alerts. There should be no alert for ssh connections.*
4. Identify Advantages and Disadvantages
   * Are there any malicious circumstances that the alert(s) discussed above do not address?
   * *There may be failure when there is system overload, in this case the alerts may not work.*

**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

*System logs provide a glimpse of what happens within the system. Many logs are intended to facilitate system debugging. When the system become slow, the operator is unlikely to find it difficult to find what they are looking for, this is because most operates The other log challenge is that messages from multiple sources may interleave at runtime. When this happens, the message id cannot help in resolving the problem since the thread can be used in for other independent tasks. When it comes to static interleaving, it can be more challenging because different modules are written by different developers hence a similar log message may be integrated differently.*

*Logging also means there is internal synchronization of information and this may means that multithreaded system may be affected by changing their threads. For a large system, logging may require release operation, and this may lock an object so that a lock contention may be prohibited.*

1. Provide a Concrete Example Scenario
   * In Project 1, when did you deal with log data?
   * *The log data dealt with is application logs information.*
   * What kind(s) of data did you investigate?
   * *The data investigated is the application logs within the server.*
   * How much data were you dealing with?
   * *The log query returned values greater than 100, hence attracting attention of the logging data.*
   * What were you looking for?
   * *I was looking for anomalies from SQL queries log.*
2. Explain the Solution Requirements
   * What information did you need to find what you were looking for?
   * *I needed logs from an external query, therefore I had to query logs from*
   * What does an analyst need to analyze large amounts of log data to find this information?
   * *The analyst can use log systems such as* ***Logstash*** *that has capability of ingesting data from multiple sources and select the filtered data and sends to the analyst.*
   * In Project 1, what tools did you use to analyze log data?
   * *The log data was organized using ELK, where docker images are used to compose graphs. Logs can also be found from supervisor.*
3. 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?
   * *Logtash was used in developing graphs of logs. The specific chat is utc\_time\_per hour, other charts include log request vs time. The application requests can be grouped depending on the time it takes and the resources used by the reques.*
4. Identify Advantages and Disadvantages of the Solution
   * What kinds of data did you not inspect during Project 1?
   * *The resource use was not analyzed during project one. There are many other parameters that were not analysed such as the content of the logs and the threat level of individual logs could not be enumerated.*
   * Would having access to this additional data have changed your process or conclusions? If so, how?
   * *The access of additional data would have changes the types of threats suspected to be in the system.*

**Question 3: Escalating Security Events**

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

1. Restate the Problem

*A security Alert is determined using Azure platform using the alert system. The alert can be grouped in terms of their severity. The system can make alert on long events, long search queries and tests for website availability. The alerts can be grouped as follows; New showing that the issue has been detected, acknowledged means that the alert is being worked on and closed means that the issue has been addressed.*

1. Provide a Concrete Example Scenario
   * What kinds of events and alerts did you encounter in Project 1?
   * *The events that receive alerts include large % of CPU usage, Server response time and large result count out of a log query.*
   * Which of these events was most interesting or suspicious?
   * The most suspicious alerts are the server response time that can signal man-in-the middle attack or denial of service. Another important one is large result from query exceeding 100, this may signal spam or DDOS attack.
   * Why was the event suspicious? What led you to investigate it?
2. Explain the Solution Requirements
   * What do you need to figure out in order to determine if this event is worth escalating?
   * *Alert management is important in considering the which one is worth your attention. The alerts can be managed through the use of alert rules. The rules can be sorted based on the resource groups.*
3. Explain the Solution Details
   * How did you use Kibana to find this information?
   * *Using elastic search, custom query can be used to manage alerts especially setting up an alert when a document matches a rule’s query. Kibana is also important when defining and running queries, for example when feidl value is set to 10, and the source ip is 10, then an alert is generated for every source of IP. The screenshots for defining rules has been attached with the document.*
4. Identify Advantages and Disadvantages of the Solution
   * How confident are you in your conclusion?
   * *The rules can have advanced configuration, where reference URLs and false positives could be defined. There are also tags that were to be added, again the author and License are also important when managing alerts.*
   * What additional data would be useful to determine if your conclusions are correct?
   * *An additional data that can be added to the alerts include timestamp override, rule name override and building block.*