## Activity File 4: Interview Questions

#### 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. Read more about access control lists and how they work here.

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 comnnections

* + What happens if you try to connect to a VM that does not accept SSH connections? Why?

1. 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.*