#### **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 - **Our company utilizes a virtual network and cloud storage. When using a virtual network you must ensure that your firewall blocks SSH connections - to prevent backdoor entrance from hackers. Last week our security officer reported that our firewall is allowing SSH connections.**

Provide a Concrete Example Scenario

* + In Project 1, did you allow SSH traffic to all of the VMs on your network? **SSH traffic was only allowed to the JumpBox**
  + Which VMs did accept SSH connections? **Web 1 and Web 2 did not accept SSH or public connections.**
  + What happens if you try to connect to a VM that does not accept SSH connections? Why? The user will get a “Connection Refused” error code. This means that; **1. SSH is not running, 2. The port is blocked by a firewall or 3. try a different port.**

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? **1. I set a public I.P. address for the virtual machine or two I did not configure my Security Network Group properly.**
   * Which general configurations would you double-check? **I would check to see if my I.P. address was public or private. I would also check to see which ports were open.**
   * What actions would you take to test that your new configurations are effective? **After I fixed the error I would attempt to SSH into my VM’s from another network. I would run a network scan (ping, nmap) as well.**
2. Explain the Solution Details
   * Which specific panes in the Azure UI would you look at to investigate the problem? **SSH, SSH from JumpBox and port 5601**
   * Which specific configurations and controls would you check?**Inbound Security Rules**
   * What would you look for, specifically? **Which ports are open in addition to checking load balancer**
   * How would you attempt to connect to your VMs to test that your fix is effective? I would attempt to SSH into my JumpBox and open a container
3. Identify Advantages/Disadvantages of the Solution
   * Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access? **NO**
   * What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?​ I would install metricbeat to monitor logs, data and CPU usage.