**Interview Questions**

**Domain: Network Security**

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

* The firewall that is supposed to block the SSH connections is not working properly.

1. Provide a Concrete Example Scenario

* I did allow connections to all of the VMs on my network. All my VMs accepted SSH connections except for the Jump Box. If you try and connect to a VM that does not allow SSH connections, you would get an error or the connection would time out.

1. Explain the Solution Requirements

* I would assume the source of the error is a rule in the network security group configurations. I would double-check all of the network security group inbound rules. Actions I would take to try to test my new configuration are to attempt to SSH into the VMs from a source that is not allowed through the new rule.

1. Explain the Solution Details

* To investigate the problem I would look in the settings and networking pane inside of Azure. The specific configuration rules that I would check would are in the network security group and the IP address of the Jump Box. I would specifically look for rules that were set to allow SSH connections and make sure it just included my IP address, such as at the rule for denying all inbound traffic. I would check to make sure that the sections “any port, any protocol, any source and any destination” are to deny, to block all other traffic. I would attempt to connect to my VMs to test and make sure the everything is fixed by attempting an SSH connection from a source that should be denied.

1. Identify Advantages/Disadvantages of the Solution

* This does not guarantee that the network is now “immune” to all unauthorized access. If the VMs are not patched consistently then more vulnerabilities could potentially arise. Monitoring controls that I would add to ensure and identify any authentication attempts are installing the Filebeat container into the Web 1 & Web 1 VMs will allow me to configure alerts and see any attempts, this data will be sent to logstash for me to monitor.

**Domain: Cloud Security**

When is it appropriate to use containers in cloud deployments, and what are the security benefits of doing so?

1. Restate the Problem

* Using containers in cloud deployment has many security benefits.

1. Provide a Concrete Example Scenario

* I used the ansible container to install Filebeat, Metricbeat and Elk into the project VM’s. The containers I used were Filebeat to monitor auth.logs and Metricbeat to monitor the operating system, CPU and memory usage. The Elk container was to run Elk. The ansible container allows us to deploy all programs to the VM’s at one time.

1. Explain the Solution Requirements

* This was an appropriate use for the containers because it saves time and installs all programs at one time and to have some version control. The security benefits I expected from using containers were allowing for better patch management for the VMs.

1. Explain the Solution Details

* I configured the VMs by installing docker to be able to run. I installed the correct container by going to the docker repo and find the specific containers that I wanted. I can verify that it is running correctly by running the command sudo docker ps -a

1. Identify Advantages/Disadvantages of the Solution

* I could have achieved the same thing without containers, but I would have to manually install Metricbeat and Filebeat and then SSH into the container. The advantage of doing this with a container is that you do not have to rely on a script to install all the programs. This can take time to try and figure out any errors that arise from running the scripts. The disadvantages would be having to do this manually, which can take a lot of time and take time away from other important tasks.

**Domain: Logging and Monitoring**

How do you determine which alerts to set in a new monitoring system?

1. Restate the Problem

* Determine which alerts to set in a new monitoring system

1. Provide a Concrete Example Scenario

* There are 4 VMs on my network, Web 1 and Web 2 VMs are the webservers. The Elk is the SIEMS and montiors logs. Jump Box allows us to use ansible and reduce the attack surface on our machines in our network. The VMs that should be publickaly accessable are Web 1 and Web 2 and one VMs that should not be puoblicaly accessable are the Elk and Jump Box.

1. Explain the Solution Requirements

* If we consider that the VMs should not be publicly accessible from the internet, we need to monitor the SSH protocol and it should fire each time there is an attempt of an SSH from the internet. These VMs should be associated with these alerts to monitor if someone is trying to access or attack our webservers.

1. Explain the Solution Details

* There are so many options with Kibana and one of them is the watcher tool, I can use this to set alerts. All of the metrics and logs that are coming in through Kibana are being turned into visuals to make it easier to read and interact with. The alert would fire upon a failed and successful SSH attempt.

1. Identify Advantages and Disadvantages

* The malicious circumstances that the previous alerts discussed does not address are ping attacks. This is very important as we want to be altered to any ping attacks. Another circumstance would be if a hacker got ahold of login credentials. If this were to happen it would be extremely difficult to determine who the legitimate user is.