**Interview Questions**

**Domain: Cloud Security**

**Question3: Containers**

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

Increasingly so companies are beginning to use containers when running cloud deployments. In this recent project, I was able to experience working with containers to complete an ELK Stack deployment. In order to monitor Kibana activity data and logs using Filebeat and Metricbeat, it was necessary use a docker hub to configure the .yml files that would run the ansible-playbook tools. To facilitate this activity, I created a virtual network in Azure. This network consisted of a Resource Group that contained two virtual networks. One network contained four virtual machines that used public/private SSH key pairings to gain access through the JumpBox VM, and one virtual machine for our ELK environment that connected the filebeat and metricbeat containers to our virtual network.

The initial access from my personal terminal to the JumpBox came from allowing access through port 22. With this access, I was able to SSH into the JumpBox and install the docker.io container. By adding access to port 80 and using the public/private SSH key pairings for my three Web VMs, I was able to configure and install the ELK stack to the ansible-playbook. This allowed access to the DVWA website on the internet through the IP of the static key generated for the Web VMs. I was able to verify that the container was running correctly by the error messages of the ansible-playbook and by the fact that I was able to visit the website using the IP address of the virtual machine.

I used a similar process with the ELK Network and the Elk VM. I was able to configure both the filebeat-playbook.yml and the metricbeat-playbook yml. They were configured using the Elk IP but monitor the three Web VMs that are all connected through the SSH public/private ansible key. The verification that these containers were running correctly came through verification given in the Kibana website that showed that data was received.

Is it possible to achieve the same outcome of securely access websites without using your personal computer if you do not use container? Yes, virtual machines without containers could be used, but the risk of a single point of failure could be a timely and costly problem. If one of the three Web servers did not work, none of them would work. Troubleshooting such an issue could be time inefficient. The other alternative is multiple servers to run the function of each container. This is a very expensive solution that also has potential physical ramifications to loss of data. A natural disaster, fire, or physical building breach compromise the integrity of the data. Ultimately, there are also risks in using containers. Misconfiguration of security rules also poses security threats that could leave the network vulnerable to attacks, but if the network is properly secured, containers provide and efficient resource for sharing OS resources and maintaining data.