Activity File: Interview Questions

The containerization of cloud computing is on the rise. “In 2019, only 20% of organizations had containerized applications. However, a Gartner report suggests that by 2023, 70% of organizations across the globe will have at least two containerized applications in production.”[1]

Containers are created by easily installing or configuring a container image. Docker container images can be downloaded and shared via Docker Hub. The most significant benefit of using containers is that they are small and easily deployable, meaning they take very little computing power and resources to implement and are therefore more efficient for running computer applications and processes. Provisioner containers, such as Ansible, also make deploying software to multiple machines much simpler and more streamlined, with Ansible using playbooks written in the YAML language that can be partitioned to any number of adjacent VM’s from a single Host VM.

One of the paramount advantages of using containers in cloud computing, and cloud security, is their expendability. Because the goal of cybersecurity is to “always protect the data,” containers can be very beneficial. Containers can easily provide a convenient platform for testing scripts and processes without taking the time to construct an entirely new machine. Additionally, with the previously mentioned convenience, the user reduces the permanent data trail that could perhaps be accessible to a threat agent. Speaking of a data trail, containerization is also useful in limiting a data trail by keeping application data separate from other application data and even the host system’s data, essentially adding another layer of separation and enhancing security.

The advantage of their disposability also does come with the disadvantage of possibly losing data. As a rule, never store data on a container. Although SSH keys and ansible-playbooks are generated and stored on the Ansible container in order to be used, they should always be backed up onto the Host VM for future use and reference. Fortunately, this is a straightforward process as containers can share data with the Host VM with one easy command. From the Host VM, simply run the sudo docker cp [container name/ID]:/path/to/file/or/directory /Host/VM/directory/ (. to add to present directory) command to copy the file from the disposable Docker container to the directory location of the Host VM.

Although it was much simpler to use Ansible to install and run the PENtest software to all of my Web (DVWA) VM’s simultaneously with one command, ansible-playbook PENtest-playbook.yml; I would have been able to complete the mission without using the Ansible container by using the JUMPBOXprovisioner VM to SSH directly into each individual Web/DVWA VM and then directly installing the Elastic Stack software packages onto each separate VM. That being said, the Elastic Stack software is most readily deployed on containers to monitor containers, and subsequently, their Host VM’s.

Because of the many proven advantages of using containers in the cloud computing format, container use is here to stay, subsequently adding another layer to computing and, therefore, another layer to cybersecurity. Leaving me to think, why would anyone deploy a cloud computing environment without using containers?

---

[1] Jordan MacAvoy, “How to Secure Containers for Cybersecurity”, https://containerjournal.com/topics/container-security/how-to-secure-containers-for-cybersecurity/ (accessed January 23, 2021)