Containers

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

1. Restate the Problem

Cloud deployment is more advantageous than on-premises networks, but it requires proper cloud management. Containers offer a solution to cloud management as they are light weight virtual machines that can easily be downloaded, distributed, cost effective, destroyed or redeployed as needed.

1. Provide a Concrete Example Scenario
   * In Project 1, when did you use containers?
     + We used Docker which was a runtime engine for specific containers that were installed including:
       - Ansible: cybersecurity/ansible
         * A provisioning tool to ensure scripts run identically anywhere
       - 2 Damn Vulnerable Web Application: cybersecurity/dvwa
         * A web application that is purposely vulnerable allowing security professional to test their skills
       - Elk: sebp/elk:761
         * Centralized log server, management web interface by using Elasticsearch, Logstash and Kibana stack
2. Explain the Solution Requirements
   * Why was this an appropriate use for containers?
     + Containers are a better option than conventional VMs as they are lightweight so they use fewer resources by sharing resources they have in common with other containers
     + Since we needed two instances of the same container for the DVWA, it was easy to duplicate and deploy thanks to the Ansible configuration playbook
     + The VM that had ELK installed also required similar set up as the DVWA and again was easy to install
     + If containers were not used, then then duplicating the entire VM would create a lot of overhead, not be cost effective and end up wasting resources
   * What security benefits did you expect from using containers?
     + Containers are meant to be immutable as it is much easier to apply read-only environments with containers than with VMs
     + No user access expected on the container which eliminated the need for credentials, tools to support users
     + Short lived containers are unlikely bases for attackers
     + Containers allow pre-deploy image scanning for vulnerabilities that automatically evaluate containers for known issues
3. Explain the Solution Details
   * In Project 1, how did you configure VMs to be able to run containers?
     + Docker and ansible were used
   * How did you select and install the correct container?
     + We pulled the images from Docker Hub
     + Downloaded/Installed it with the help of Ansible
     + sudo docker pull cyberxsecurity/ansible
   * How did you verify that it was running correctly?
     + First start the container:
       - docker run -ti cyberxsecurity/ansible:latest bash
       - docker start [container\_name]
       - docker attach [container\_name]
     + Verify by running command:
       - docker container list -a
     + To troubleshoot we also checked to see if ansible configuration was done correctly with ping command:
       - ansible -m ping all
4. Identify Advantages/Disadvantages of the Solution
   * How would you have achieved the same thing without containers?
   * What are the advantages to doing it without containers?
     + It is possible that one of the images were compromised when we pulled them, and in that case, would mean a potential risk for that container
     + All the OS resources are available for the services to use which could result in better performance
     + Fully isolated which could mean less security risk
   * What are the disadvantages?
     + Repetitive tasks when it comes to installing, configuring and integration to ensure infrastructure is still intact
     + Portability is significantly harder when compared to containers