Exercise – 6

Abdurrehman Syed
2308546

Task – 1

Container

A container is a lightweight, isolated environment running on the host system's kernel but with its own file system, processes, and network interfaces. Usually, it's managed by some tool like Docker or Kubernetes.

Security Capabilities:

- Containers introduce isolation between applications to prevent unauthorized access and interference.
- Containers are lightweight compared to virtual machines because they require less usage of system resources.
- Movement and deployment of containers across diverse environments can be easily done and consistently assured.

Security Limitations:

- Even with some sort of isolation done by containers, sharing of the host system kernel might provide an attack surface.
- Breach in the namespace of the container might lead to unauthorized access to the host system or other containers.
- The container's security is dependent on the security of the host system it's running on; hence, it is vulnerable to attacks at the host level.

Virtualization

Virtualization enables running multiple virtual machines on the same physical server, where each VM has a private OS and resources. The most generally used virtualization technologies include VMware and Hyper-V etc.

Security Capabilities:

- VMs can isolate a workload from another with high-level access and protect the workloads from each other.
- The modern virtualization technologies use hardware-based functionalities for enhancing security and performance.
- VMs can be easily reverted to previous states in the event of a security incident or accidental edits.

Security Limitations

- VMs use significantly more system resources than containers, which could affect performance.

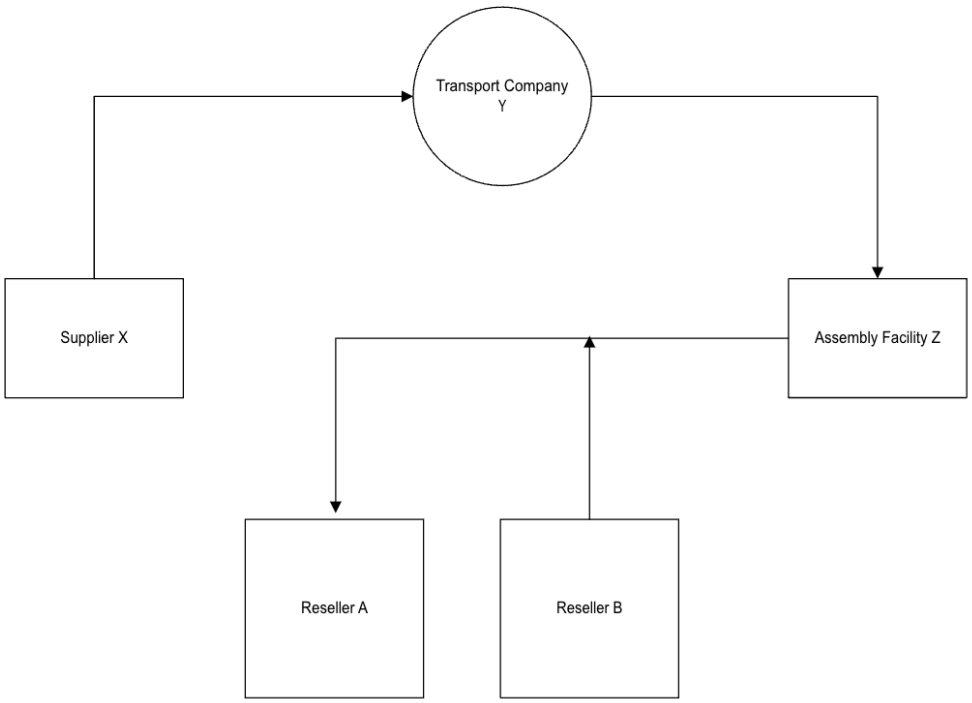
- The hypervisor itself, which manages the virtual machines, is another point of vulnerability.
- Each VM has an operating system of its own with its own set of vulnerabilities to exploits.

References:
Docker: https://docs.docker.com/
Kubernetes: https://kubernetes.io/
Containers: https://www.freecodecamp.org/news/how-docker-containers-work/
VMware: https://www.vmware.com/
MS Hyper-V: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/
Virtualization: https://www.nutanix.com/info/virtualization

Task – 2

Supply chain security for such a company, manufacturing and selling routers, software, and networking accessories, would therefore be in fact specific actions entailing. There are a number of players in the supply chain; each of them requires special care regarding security to prevent tampering or other kinds of threats.

For instance, third-party supplier X manufactures antennas required for the routers. In this case, the potential risk is tampering with the hardware components. We can further mitigate this by introducing the antennas with a TPM module. This TPM module will introduce enhanced security through key generation, and it ensures sensitive data to be safe. It also verifies if the authenticity of components in either production or transport has been tampered with. This involves using tamper-proof



packaging during shipment, ensuring interference will be identified prior to the components reaching our assembly line.

Once the components reach the assembly factory, tampering with the hardware can occur at the time of assembly. We will employ UBA to monitor activities conducted by the assemblers to identify suspicious/abnormal behavior that may indicate an intent toward malicious activity.

We would like to utilize NDR tools during the process of software development in order to block external dangers that may filter into the corporate network and, while developing the software, may get malicious code from unauthorized actors. Regular code reviews and team meetings should also form a part of the development process to prevent vulnerabilities from coming into a system, either by mistake or on purpose.

Third-party contracted developers will perform full security testing of the code provided. EDR tools will also be utilized to ensure that only authorized code will be deployed. In addition, we will apply multi-factor authentication when there are third-party companies hosting internal tools in order to guarantee secured access to critical systems.

Besides these technical measures, it would be necessary to create an effective incident response plan at each point of the supply chain. That would serve to ensure that if there were any security breaches or threats, they would be handled with due efficiency, including communication protocols from one party to another.

These are the hardware and software security strategies that will help enhance the overall supply chain security. Some of the tools to be used include TPM, UBA, and EDR, which will reduce the chances of tampering or other types of security threats against our products, right from manufacturing up to their very delivery.

Took some help with AI on task – 2 (understanding and diagram ideas)