Chapter: 5:

5.2 (2) Virtualization System - Specific attacks:

Virtualization System refers to when a System is converted to virtualize mode. the system will have minimum of two operating system at one.

Basically Virtualization reffers to multiple operating systems made to run a single physical component or system.

- While working with multiple operating one of the OS is reffered to as Host OS which is responsible for.

booting and this os cannot be deleted.

Remaining os is known as Guest os which is user friendly and can be installed or deleted according to user requirements

Specific attack :

It ~~kinds~~ Consists 3 kinds of attack
Guest hopping
VM Migration attacks
Hyper jacking.

Guest hopping :

Guest hopping is also called as Man - in - the - Middle attack.

Malicious or illegal attacks done in the guest operating system causes Guest hopping.

In Guest hopping, it is easy for attackers or third parties to attack the guest OS and get control over the data Compared to host Op os

By third party, the malicious code is being installed by an guest OS by attacker to steal the data, ~~machine~~ hardware, software or application

It is an kind of security threat where an attacker manages to escape the isolation of virtual machine and gain unauthorized access to other VM's running on the same physical host.

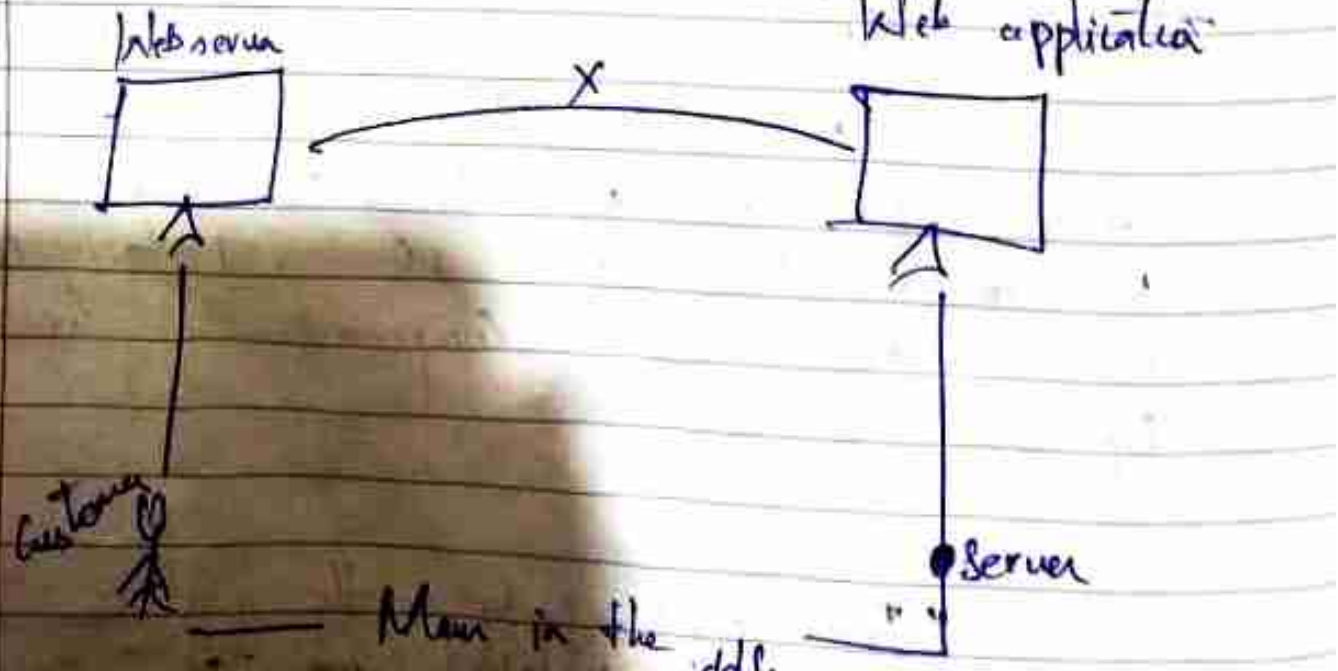
It helps attacks to hop from one guest VM to other VM.

Prevention techniques:

- Hypervisor Security patches.
- Strong Access Control
- VM Isolation.

disadvantage:

- data breach
- loss of VM isolation.
- Multi-tenant Security.
- Downtime



VM Migration:

VM Migration attacks occurs when an attacker intercepts or manipulates the migration process of a virtual machine.

This attack aim to compromise the integrity, confidentiality and availability of the virtual machine and its data.

This kind of attacks occurs when some malicious code is installed during migration process

These attacks occurs in three plane
* Control plane
* data plane
* Migration modules

Contol plane : it is responsible for controlling the entire process during the migration attacks

data plane : it is responsible for maintaining the data, How the cloud providers provides data to users

It consists of two kinds of attack.
* passive attack
* active attack

Migration module: It is responsible for managing the transfer of virtual machine or workloads between different physical hosts, or cloud environment

Prevention
- Network isolation
- Encryption.
- Strong authentication
- Access control polices

disadvantage:
- loss of Confidentiality
- Data breach.
- Data integrity issues.
- denial of service (DOS).

Services:
VM Migration Combine two services
- i. Hot migration
- ii) Cold migration

Hyper jacking:

Hyperjacking is a malicious attack where the attacker gains unauthorized access to the hypervisor.

By compromising the hypervisor, the attacker can potentially control all VMs running on the system

Here the attackers gain access to the Virtual machines running on it. , it target Virtualization layer.

The hypervisors are of two types, one is Type I (bare metal hypervisor) and Type 2 (hosted hypervisor).

Impacts or disadvantages of hyperjacking:

- Data breach
- Service Interruption.
- ~~Loss~~ loss of control

Prevention:

Hypervisor hardening.
Secure boot
Isolation and Access control
Monitoring & detection.