

Virtualización de servidores

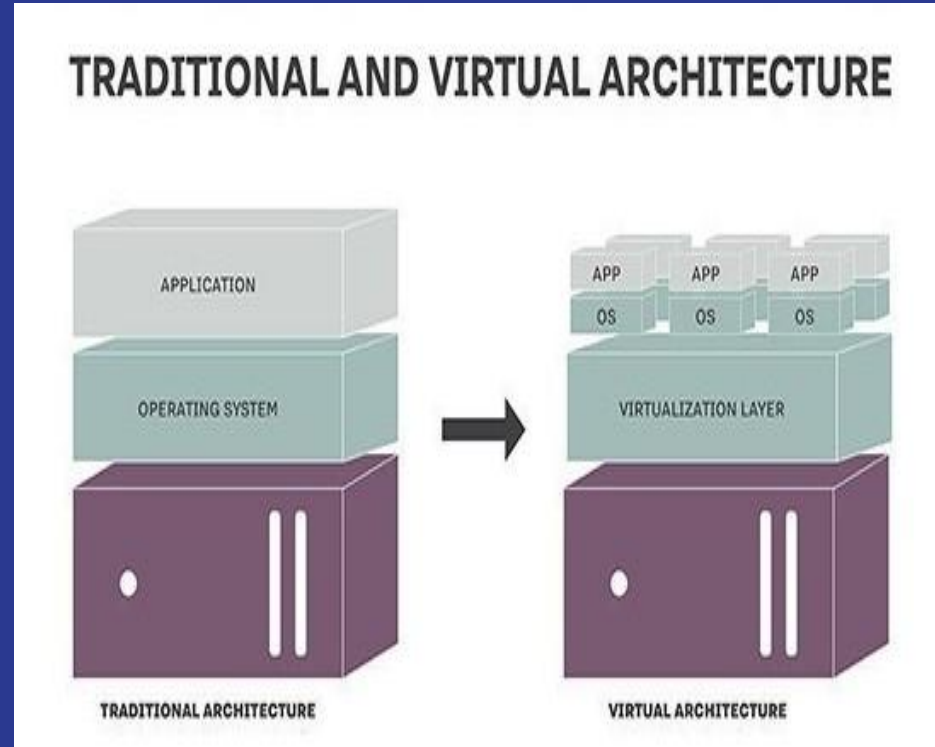
Grupo 1:

- Matías Agustín Larroque Leg. 56597
- Tomás Agustín González Orlando, Leg. 57090
- Lucero Guadalupe Fernandez, Leg. 57485
- Manuel Mollón, Leg. 58023
- Ezequiel Vijande, Leg. 58057

Introducción

Virtualización

Hace referencia a la separación de los recursos utilizados del medio físico que los provee



Virtualización de servidores

Es el proceso de dividir mediante software (Layer) un servidor físico en múltiples servidores virtuales cada uno con su propio sistema operativo (OS).

https://www.amazon.com/-/es/High-End-Dell-PowerEdge-R720-2-60Ghz/dp/B075Z3F37Z/ref=pd_lpo_147_img_1/143-4511091-3348803?encoding=UTF8&pd_rd_i=B075Z3F37Z&pd_rd_r=f6568715-a22f-4e64-8335-80b91f6ffc18&pd_rd_w=4MeE2&pd_rd_wg=S6Zv6&pf_rd_p=7b36d496-f366-4631-94d3-61b87b52511b&pf_rd_r=N5T94GKPFZP5A8C9FTG&pvc=1&refRID=N5T94GKPFZP5A8C9FTG

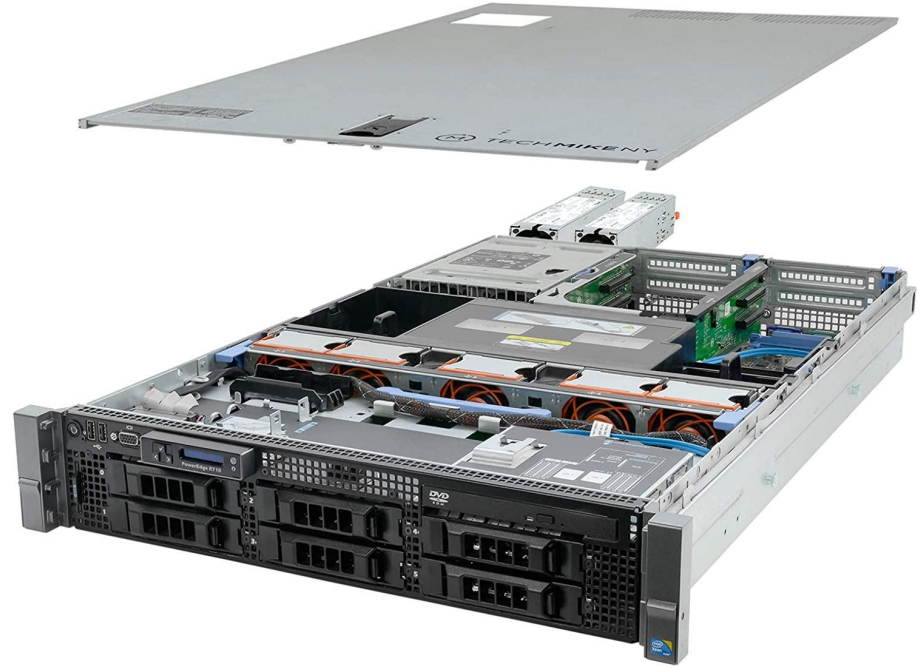


Ilustración de un servidor de virtualización
(PowerEdge R710)

Por qué virtualizar?

- Requiere menor infraestructura física.
- Permite organizar de manera más ordenada bases de datos independientes.
- Menor consumo energético que varios servidores físicos.
- Menor costo por servidor.
- Facilita actualizaciones del software.



Virtualización vs Cloud Computing

La diferencia fundamental es que el cloud computing trabaja con infraestructura como servicio (IaaS), dando acceso “on demand” a recursos computacionales en una “shared pool” que pueden ser provistos con mínimo esfuerzo del proveedor.

Mientras que la virtualización se basa en software como servicio (SaaS). Por lo que la nube es ventajosa para usos públicos, pero para una empresa puede llegar a ser mejor un enfoque por el lado de la virtualización.



Virtualización vs Cloud Computing

Característica	Virtualización	Cloud computing
Escalabilidad	Limitada	Fácil
Setup	Fácil	Tedioso
Flexibilidad	El acceso requiere autenticación	Muy flexible, requiere acceso a internet
Hardware dedicado	Se requiere hardware dedicado para máquina virtual múltiple	Múltiples hardware crean el cloud computing
Integración	Permite expansión de nuevas máquinas en la misma infraestructura	Permite expansión futura de usuarios, aplicaciones, etc
Dependencias	Múltiples sistemas operativos pueden ser instalados en un servidor	Múltiples usuarios pueden acceder usando un mismo link
Accesibilidad	Permiso requerido para entrar desde fuera de la red	Puede ser accedida desde cualquier parte del mundo
Disaster Recovery	Falla de una máquina puede hacer caer múltiples máquinas virtuales	No dependen de una sola máquina

Cuando conviene virtualizar?

- Si la alternativa requiere un gran número de servidores físicos.
- Se puede cubrir la inversión inicial requerida y reduce costos a largo plazo.
- Existen limitaciones de espacio.



Cuando NO es conveniente virtualizar?

- Se utilizan licencias de programas que no permiten virtualización.
- Aplicaciones que utilizan I/O en un alto grado.
- Si el sincronismo entre host y guest es de importancia crítica.
- Existen limitaciones de performance o capacidad en el servidor físico.



Estado actual del mercado

Magic Quadrant




Tabla de comparación

Prod.	Platform	Scalability	Overhead %	Markets	Cost	Migration	Key Differentiator
Vmware vSphere	x86	1,024 VMs per host	5 to 25	SMB-large enterprise	\$995 per CPU, plus \$273 per year support	Drag and drop or command line	Market leader in virtualization
Red Hat Virtualization	x86	up to 400 hosts	5 to 20	highly-scaled deployments with budget constraints.	\$999/per managed hypervisor socket pair each year	Manually or automated	Strong in Linux environments
Proxmox VE	x86/AMD64	Up to 32 nodes per cluster	5 to 10	Hyperconverged infrastructure, Ceph Storage cluster, software-defined data center, cloud computing.	€74.90 per CPU	One click in Web interface	Lower cost provider in Linux environment
Microsoft Hyper-V	x86	240 vCPUs per VM	9 to 12	Windows Server users, Microsoft/Azure customers	\$1,323 for up to 16 cores, free with MSC	Import/export enables easy VM move	Top offering Windows data centers
Citrix Hypervisor	X86	64 VMs per host	5 to 10	Citrix Virtual Apps and Desktops users, data center server consolidation, high-performance 3D graphics.	\$1149 per CPU socket, free to users of Citrix Virtual Apps and Desktops	Can move a running VM from one host to another	Lower cost alternative, popular among SMB
Oracle VM Server	X86, SPARC	256 vCPUs per guest	5 to 10	Oracle app users	Free	Move over secure SSL links	Geared for Oracle customers
IBM PowerVM	AIX, Linux and IBM i clients	1000 VMs on a single server	10 to 15	Virtualization for AIX, Linux and IBM i clients running IBM Power platforms	\$590 per core	Move active or inactive VMs	Very well suited for IBM environment
Virtuozzo	x86	About 50 virtualization instances per server	5 to 20	KVM users, open source users, SMBs	\$990 per month per business	Command line interface	Focused on open source

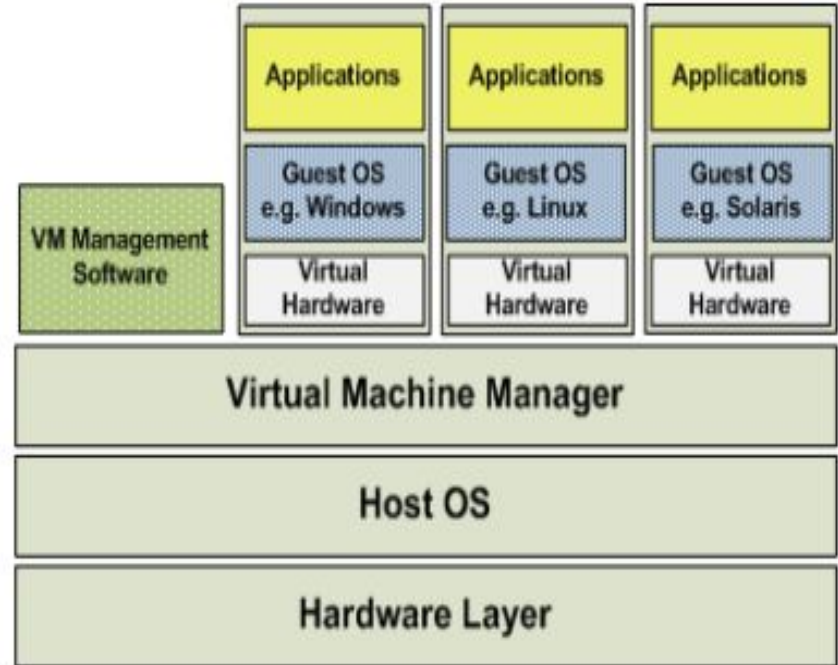
Funcionamiento

Características generales

- Existe un Layer dedicado a separar la capa física del host y los guests.
 - Este Layer maneja la asignación de recursos a cada guest.
 - El usuario interactúa directamente con las interfaces que corren en los guests.
 - El Layer se encarga de buscar tanto como modificar información almacenada en la capa física del host.
- 

Virtualización completa

- No hay interacción entre guests y se manejan de manera independiente.
- Cada guest puede tener un OS distinto.
- El hypervisor se encarga completamente de la asignación de recursos del host a cada guest.
- Algunos ejemplos son: VMware Workstation, Parallels y Virtual PC.

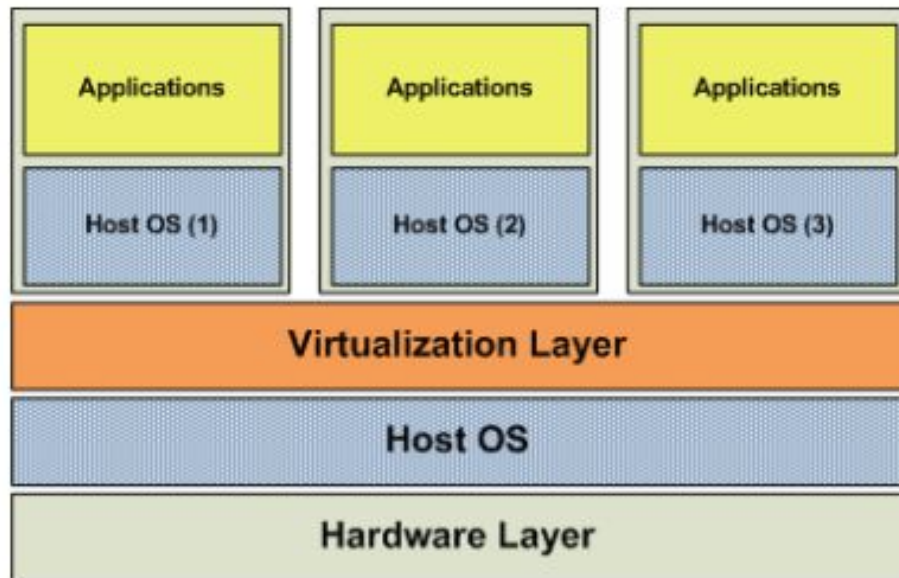


Virtualización parcial

- La abstracción entre el hardware del host y los recursos del guest es más simple que en la virtualización completa.
- También permite distintos OS por guest.
- El hypervisor resulta más simple que en la virtualización completa.
- Algunos ejemplos son Xen y Denali.

Virtualización por OS

- El rol del hypervisor es empleado completamente por el OS del host.
- Los guests tiene el mismo OS que el host.
- Al igual que para la virtualización completa, los guests no interactúan entre si.
- Algunos ejemplos son: OpenVZ y Linux VServer.



XEN

Caso de ejemplo

Tecnología de virtualización de código abierto desarrollada por la universidad de Cambridge.

Sigue el esquema de virtualización parcial.

Virtualización de memoria

- Otorga permisos de Read-Only directos para lecturas.
- Las actualizaciones de páginas se realizan mediante una comunicación sincrónica entre los guests y Xen denominada “hyperllamada”.
- Las actualizaciones pueden acumularse en un guest y luego atenderse juntas mediante una única hyperllamada, esto reduce el overhead.



Virtualización de CPU

Para este caso el hypervisor hace uso del CPU directamente por lo que es necesario que Xen tenga mayor prioridad que el OS propio del host.

Esto convierte a Xen en la función con mayor prioridad de todo el sistema por lo que para correr instrucciones privilegiadas es necesario virtualizarlas y ejecutarlas directamente mediante Xen.



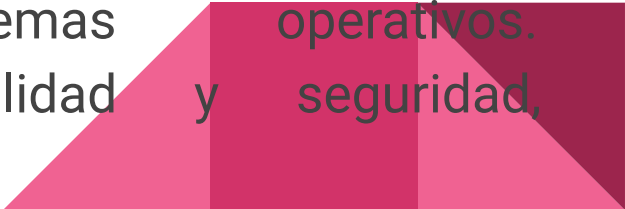
Estado del Arte

Antecedentes

La práctica surge como método para mejorar el particionado de los mainframes de IBM en 1960.

En 1980/90 se dejó en segundo plano su importancia debido a las minicomputadoras y PCs de menor costo que los mainframes.

Sin embargo, volvió a tomar importancia ya que los procesadores quedaban infrautilizados, y además las funcionalidades agregadas hacían más vulnerables a los sistemas operativos. Virtualización como solución de confiabilidad y seguridad, más que como multitarea.



Arquitecturas de virtualización

La manera en la que el hipervisor es instalado define dos arquitecturas de virtualización:

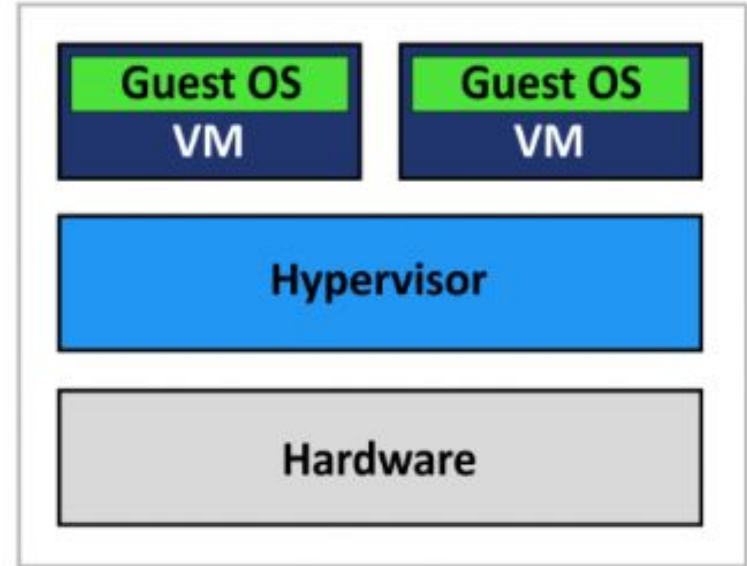
- El Tipo I de hipervisor, conocido como arquitectura *bare-metal*.
- El Tipo II de hipervisor, se conoce como arquitectura *hosted*.



Bare-Metal architecture

No hay OS, el VMM se sitúa directamente sobre el hardware.

El VMM intercepta las comunicaciones entre el hardware y las distintas máquinas virtuales.

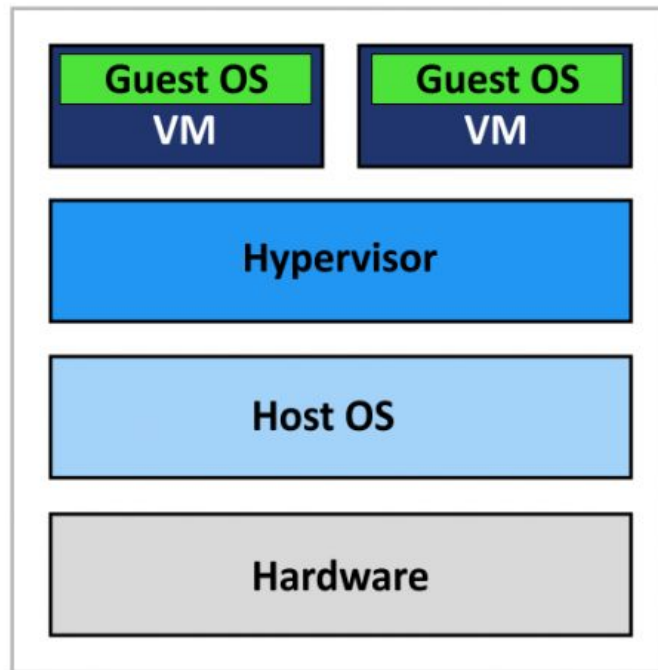


**Type 1 Hypervisor
(Bare-Metal Architecture)**

Hosted architecture

El VMM se encuentra sobre el SO anfitrión y funciona como una aplicación más. En este caso, el SO anfitrión es el encargado de proveer los drivers de entrada/salida. Un ejemplo es VirtualBox.


Esta arquitectura es más ineficiente dado que está montada sobre el SO. Sin embargo, cuenta con mayor compatibilidad de hardware ya que el SO es el encargado de interactuar con el hardware.



**Type 2 Hypervisor
(Hosted Architecture)**

Atributos principales de un VMM

Remueve dependencia entre hardware y SO. El hardware es particionado en unidades lógicas conocidas como máquinas virtuales (VM).

- **Aislamiento:** El VMM asegura que cada máquina virtual pueda correr independientemente de las demás, ya que se encarga de la interacción con el hardware físico y el OS del host (en caso de que hubiera).
 - **Interposición:** Las interrupciones generadas por el OS huésped son comunicadas al hipervisor que se encargará de procesar los eventos. Asimismo, intercepta solicitudes de periféricos del SO huésped y las mapea con los periféricos físicos correspondientes.
 - **Inspección:** El VMM tiene acceso al estado de todas las máquinas virtuales tanto como a los recursos físicos del servidor. Esto le permite guardar o reestablecer el estado de una máquina virtual.
- 

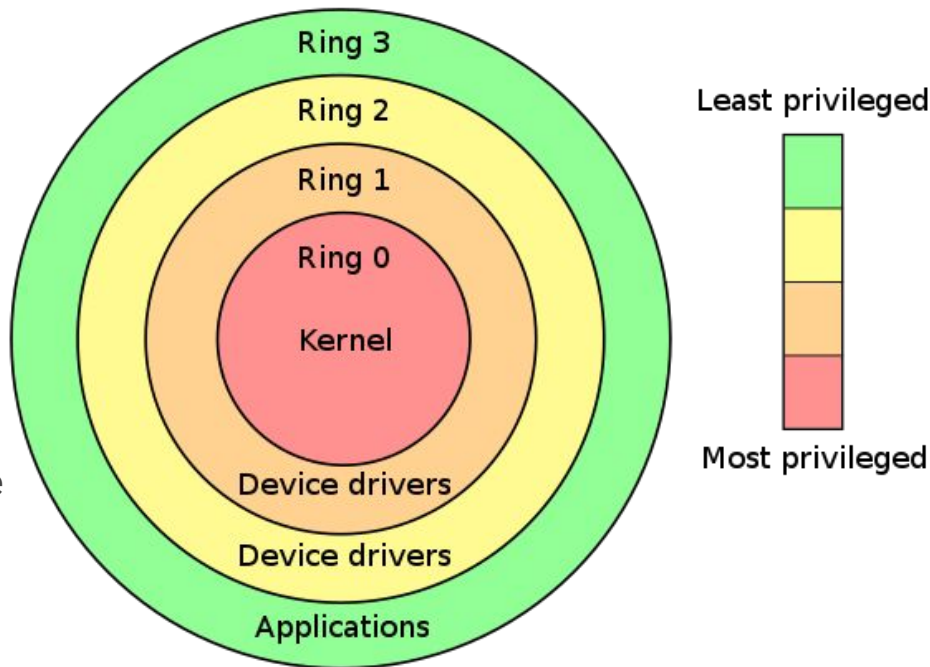
Anillos de protección

La arquitectura x86 ofrece cuatro niveles de privilegios. Se ordenan de manera jerárquica y ofrecen niveles de abstracción de privilegios.

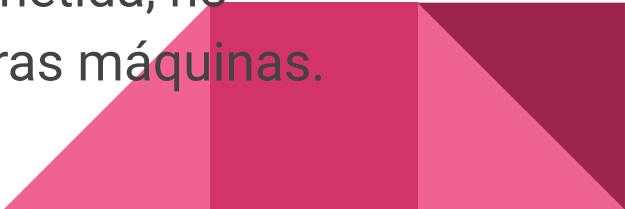
-Anillo 0: más privilegiado, menos restricciones e interactúa con hardware.

-Anillo 3: menos privilegiado y más restricciones.

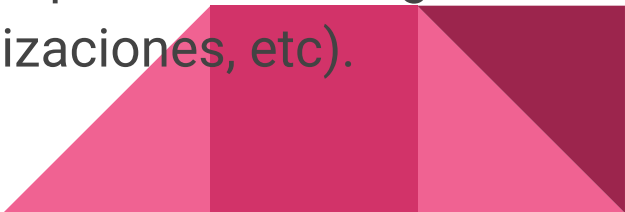
En un entorno de virtualización, el hipervisor corre en modo kernel (Ring-0) mientras que las VMs, en un nivel con menos privilegios.



Resumen de beneficios

- *Consolidación*: Combina las cargas de trabajo en recursos reducidos, permitiendo eficiencia. Siendo estas “cargas de trabajo” virtuales, se facilita la migración de sistemas a otros más nuevos.
 - *Fiabilidad*: Al permitir disponibilidades de operación en distintas máquinas virtuales, de manera aislada, se admite que algunos sistemas fallen sin que afecten a los demás.
 - *Seguridad*: Si una máquina virtual está comprometida, no necesariamente se propaga la inseguridad a otras máquinas.
- 

Resumen de desventajas

- Pérdida de performance: En algunos casos en donde se requiere hardware específico para cálculos computacionales que requieren gran capacidad de procesamiento.
 - Necesidad de redundancia: Si falla la plataforma que permite la virtualización, fallan todos los sistemas virtuales, por lo cual es necesaria una redundancia para esta capa en sistemas críticos.
 - Costos operativos: Es posible que se necesite de personal encargado de mantener el entorno virtual (licencias, actualizaciones, etc).
- 

Seguridad

Los aspectos clave a tener en cuenta en lo que concierne a seguridad de la información en una empresa son:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación
- Autorización
- Responsabilidad



Seguridad

Migrar a un ambiente virtual implica contraer en un solo sistema físico varias amenazas y vulnerabilidades de seguridad:

- Cada huésped por separado tiene sus propias vulnerabilidades y amenazas
- El sistema operativo anfitrión también tendrá sus propias vulnerabilidades y amenazas asociadas
- Nuevas vulnerabilidades y amenazas son introducidas por el hecho de utilizar virtualización y estar coordinando varios huéspedes en el mismo HW

Se deberá invertir en personal experto y en procesos acordeamente



Ataque DoS (Denial of Service)

El atacante bloquea los recursos de una máquina para que sus servicios no puedan ser utilizados.

Si se rompe el principio de aislamiento, un VM podría llegar a tomar control sobre los recursos de otro VM o del anfitrión. Podría tanto corromperlos como deshabilitarlos.



Algunos elementos de riesgo

Algunas características agregadas de un sistema de virtualización podrían llegar a provocar riesgos de seguridad adicionales. Especial atención es puesta en aquellas características que permitan violar el principio de aislamiento

Un sistema que permite el copiado y pegado de elementos de un VM a otro es una puerta de entrada a la inyección de código malicioso.

Es por esto que es de vital importancia mantener una revisión constante de las configuraciones del ambiente de virtualización y de los permisos disponibles.



Escape VM

Escape VM: Ataque bajo el cual una VM logra percatarse de que es una VM dentro de un sistema de virtualización.

Esta situación da lugar al **hyperjacking** y luego interactúa con el hipervisor, comprometiéndolo a este y por consiguiente a los demás huéspedes.

A través del **hyperjacking** se podrá, por lo tanto, controlar la ejecución de los distintos VM y tener acceso a los mismos



Visión del futuro

¿Continuidad de Virtualización?

¿Nuevas Tecnologías vs Virtualización?

Contenedores.

(Los contenedores crean una percepción de aislamiento para una aplicación que corre un sistema operativo)

Generalmente las capas no se reemplazan, por lo que conviven.



Bibliografía

1. Daniels, Server virtualization architecture and implementation. 2009.
2. F. Bazargan, C. Y. Yeun, and M. J. Zemerly, State-of-the-Art of Virtualization, its Security Threats and Deployment Models, International Journal for Information Security Research, vol. 3, no. 3, pp. 335343, Jan. 2013.
3. D. Marinescu and R. Kroger, State of the art in autonomic computing and virtualization. Wiesbaden, Germany, 2007.
4. G. Aljabari, Virtualization of IT infrastructure for small and medium businesses, 2012 International Conference on Communications and Information Technology (ICCIT), 2012.
5. Virtualization overview. 2006. <https://www.vmware.com/pdf/virtualization.pdf>
6. M. Rosenblum and T. Garnkel, Virtual machine monitors: current technology and future trends, Computer, vol. 38, no. 5, pp. 3947, 2005.
7. Server Virtualization, VMware. [Online]. Available: <https://www.vmware.com/topics/glossary/content/servervirtualization>. [Accessed: 16-Jun-2020].
8. Why choose virtualization?, TechAdvisory.org. [Online]. Available: <http://www.techadvisory.org/2014/05/why-choose-virtualization/>. [Accessed: 16-Jun-2020].
9. L. Gaille, 14 Advantages and Disadvantages of Virtualization, Vittana.org, 16-Dec-2019. [Online]. Available: <https://vittana.org/14-advantages-and-disadvantages-of-virtualization>. [Accessed: 16-Jun-2020].
10. Top 10 Reasons Not to Virtualize, ServerWatch. [Online]. Available: <https://www.serverwatch.com/servertrends/top-10-reasons-not-to-virtualize.html>. [Accessed: 16-Jun-2020].
11. Top 10 Useful Comparison Between Cloud Computing vs Virtualization, EDUCBA, 13-Apr-2020. [Online]. Available: <https://www.educba.com/cloud-computing-vs-virtualization/>. [Accessed: 16-Jun-2020].
12. Server virtualization explained, techtarget.com. [Online]. Available: https://searchitchannel.techtarget.com/feature/Server-virtualization-explained?_ga=2.168409764.429969061.1593021435-261563466.1592192264 [Accessed: 16-Jun-2020].

¿Preguntas?

¡Muchas gracias!

