Gestión de Seguridad en Virtualización de Servidores

Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Autor: Felipe Emiliano Arévalo Cordovilla

Tutor: Pau del Canto Rodrigo

Índice

Objetivos

Maximizar el nivel de seguridad en el los entornos servidores virtuales de **IaaS,** tanto a nivel de máqu virtual como de máquina física.

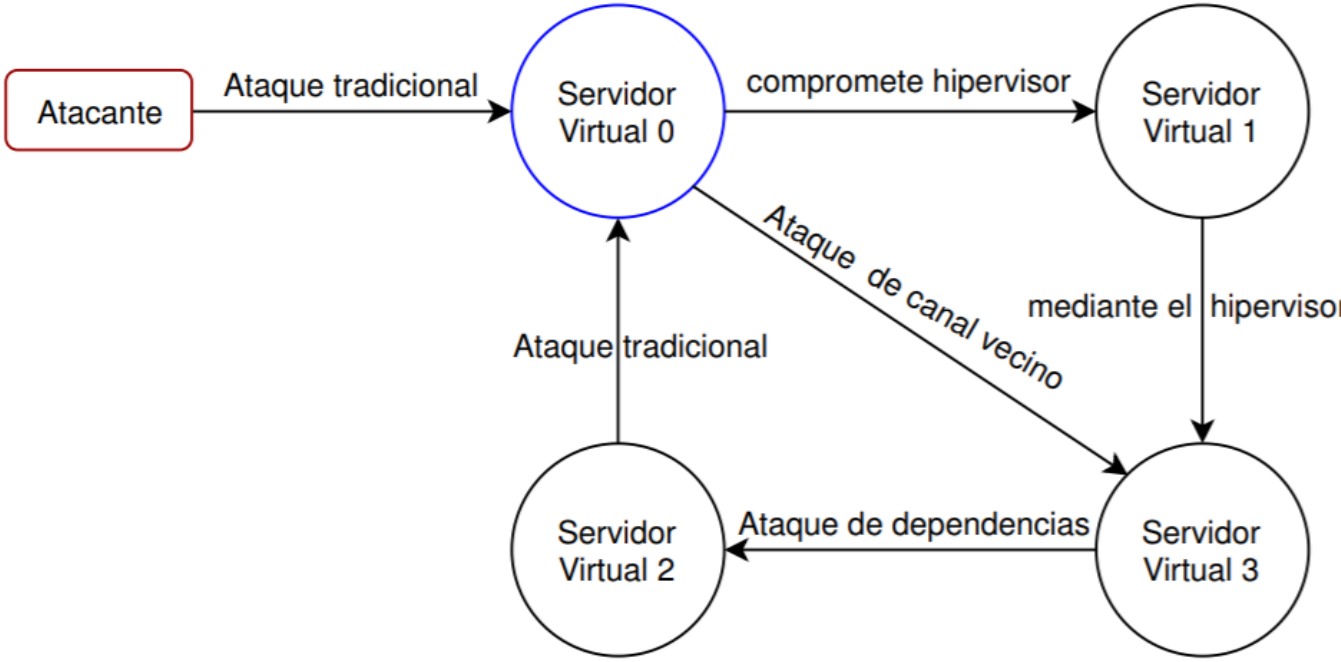
1. Proponer un mecanismo de ubicación de una maqu virtual en un servidor físico que permita minimizar el rie de incidentes de seguridad en el entorno IaaS.
2. Recolectar información sobre la protección de entor físicos y entornos virtualizados.
3. Conocer las organizaciones mundiales que estandariza publican los nuevos hallazgos relacionados a la seguridad el Cloud.
4. Diseñar el Manual de Gestión de seguridad para entor virtualizados.

Seguridad en IaaS Cloud

Problema en Iaas Clouds

Determinar la ubicación de la máquina virtual que se desea a equipo físico en la infraestructura del proveedor de IaaS Cloud.

Una máquina virtual vulnerable puede comprometer a máquinas vecinas en el mismo servidor



Seguridad en IaaS Cloud

Evaluación de la seguridad de servidores virtuales en IaaS Clouds

Existe una base de datos de vulnerabilidades pública periódicamente actualizada por un entidad gubernamental de Estados Unidos de Norte América

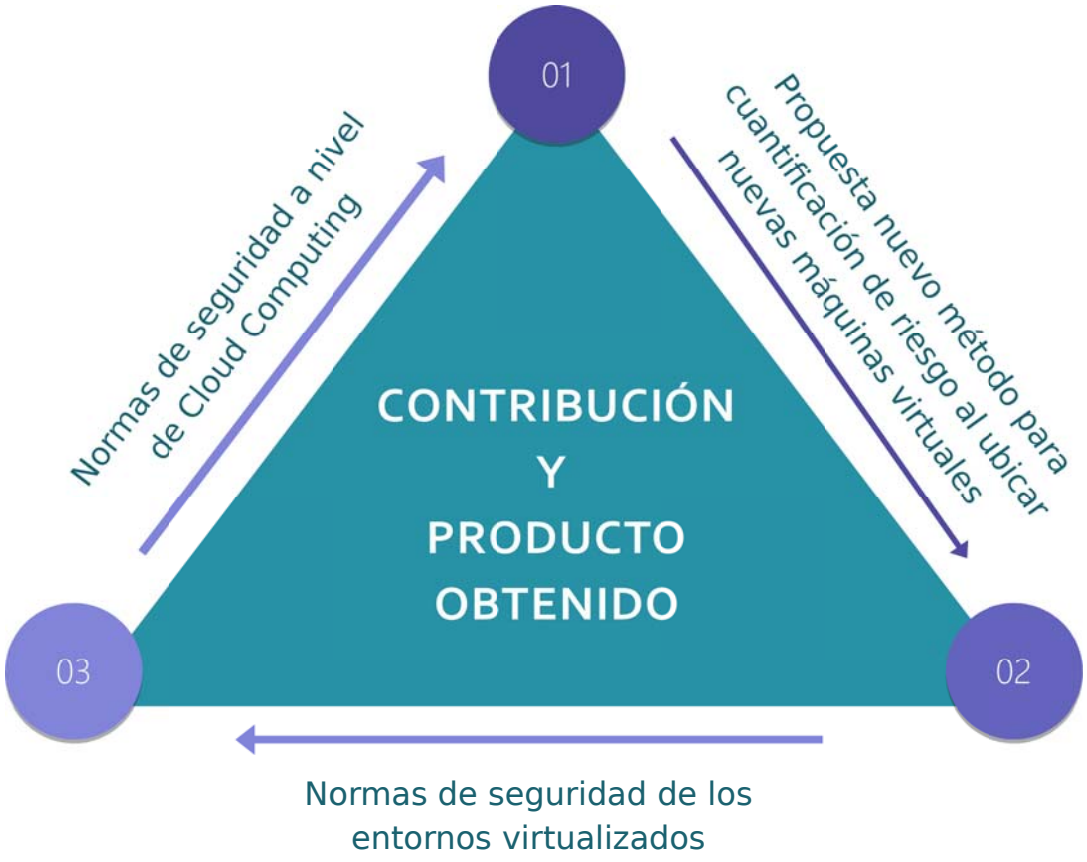
NVD National Vulnerability Database.

CVSS Common Vulnerability Scoring System.

CVE Common Vulnerabilities and Exposures.

Principal contribución y producto obtenido

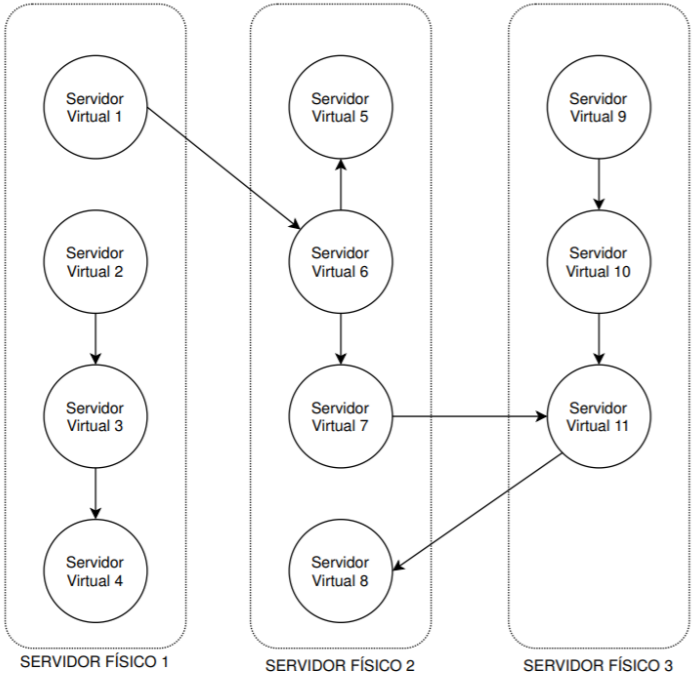
Se presenta una propuesta de solución al problema de seguridad en IaaS cloud. La primera trata sobre un método asignación de nuevas máquinas virtuales en servidores físicos segunda es un manual de políticas a seguir para maximiza seguridad en los servidores virtuales instalados.



Evaluación de la seguridad del Servidor Virtual

Grados de vulnerabilidad otorgados por la NVD

Gravedad	Ponderación
nula	0.0
baja	entre 0.1 y 3.9
media	entre 4.0 y 6.9
alta	entre 7.0 y 8.9
crítica	entre 9.0 y 10.0



Mapeo de servidores virtuales

Índice de vulnerabilidad del servidor físico IV_{SF}

$$IV_{SF} = \frac{\sum_{i=1}^{n} IV_{MV_i}}{n}$$

Índice de compatibilidad IC el servidor físico SF y la maquina virtual MV_a a ubicada en ese servido

$$IC = |(IV_{SF} - IV_{MV_a}) \times$$

Ecuación 1: IV_{SF}

$$IV_{SF} = \frac{\sum_{i=1}^{n} IV_{MV_i}}{n}$$

Ecuación 2: IC

$$IC = |(IV_{SF} - IV_{MV_a}) \times 0{,}1|$$

Ejemplo (caso 1): Según la NVD, la máquina virtual nueva a ser ubicada en un servidor físico posee un índice de vulnerabilidad IV=9. El servidor físico posee 5 máquinas virtuales instaladas (MV_1, MV_2, MV_3, MV_4 y MV_5) con índices de vulnerabilidad IV_{MVi} de (9, 10, 7, 5 y 8) respectivamente.

Según las ecuaciones propuestas:

Ecuación 1, el índice de vulnerabilidad del servidor es **IV_{SF} = 7,8.**

Ecuación 2, el índice de compatibilidad entre la máquina virtual y las otras máquinas virtuales instaladas en el servidor físico es **IC = 0,12.**

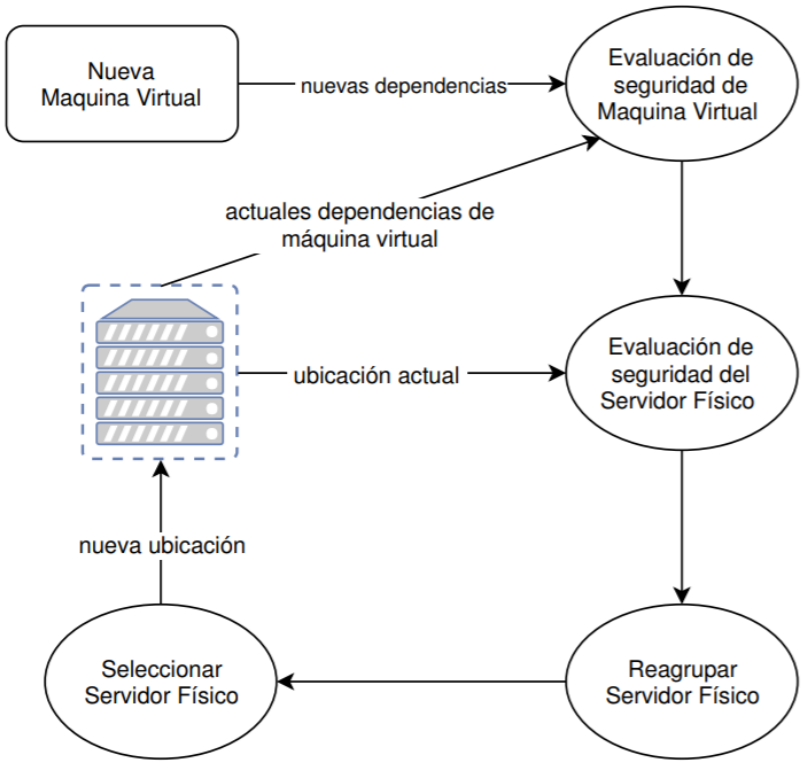
Ejemplo (caso 2): Según la
máquina virtual nueva a ser ul
un servidor físico posee un
vulnerabilidad IV=1. El servi
posee 5 máquinas virtuales
(MV_1, MV_2, MV_3, MV_4 y MV_5) c
de vulnerabilidad IV_{MVi} de (9, 1
respectivamente.

Según las ecuaciones propuest

Ecuación 1, el índice de vuln
del servidor es **IV_{SF} = 7,8.**

Ecuación 2, el índice de comp
entre la máquina virtual y
máquinas virtuales instalada
servidor físico es **IC = 0,68.**

Método de asignación de nuevas máquinas virtuales en una máquina física



Esquema general de ubicación de máquinas virtuales

Algoritmo 1 Ubicación de servidores virtuales (mv, SF, MV)

1: **Datos de entrada**: mv: nueva maquina virtual a ser ubicada
   SF: Lista de servidores físicos disponibles en el cloud
   MV: Lista de máquinas virtuales presentes en cada servidor físico
2: **repeat** (para cada $sf_i \in SF$)
3: **repeat** (para cada $mv_j \in sf_i$)
4: Calcular IC según ecuación 5.2
5: Agrupar o reagrupar la mv_j en un sf_i dependiendo de su CI
6: **until** no existan más máquinas virtuales
7: **until** no existan más servidores físicos

Políticas de seguridad para servidores virtuales

Normas de seguridad de los entornos virtualizados (24)

Normas de seguridad a nivel de Cloud Computing (17)

Conclusión

Para querer implementar medidas de seguridad de los siste
virtualizados se debe dar inicio por ofrecerle seguridad en prim
instancia al entorno físico para continuar con el del ento
virtualizado.

Organismos como los CERTs o CSIRTs, NVD o el FIRST deben
usados como una fuente de información actualizada para po
obtener datos reales sobre las nuevas vulnerabilida
encontradas recientemente.

Actualizar su Sistema Operativo de manera periódica.

Trabajo Futuro

Uso de técnicas de deep learning para contrarrestar la polarida
de los promedios

Enfocarse en soluciones de isolación de maquinas virtuales para
evitar ataques en cadena en el mismo servidor físico