Análisis y Proceso de Hardening de Servidor Virtual Web, Facultad de Ingeniería (IngeTic)

Toto Ronald Sánchez Cari
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
totosancari@gmail.com

***Resumen*—En el presente trabajo se da a conocer el Análisis y proceso de hardening del Servidor Virtual Web de la Facultad de Ingeniería (IngeTic), el objetivo de la siguiente investigación es implementar estrategias y herramientas tecnológicas para mejorar la seguridad del servidor virtual aplicando hardening para la protección de la infraestructura tecnológica de la institución. El método a utilizar en esta investigación es descriptivo por que se realizará análisis OWASP que nos permitirá determinar y combatir las causas de la inseguridad. Luego de establecer las causas de vulnerabilidades o agujeros se realizará proceso de endurecimiento para asegurar el servidor virtual web reduciendo sus vulnerabilidades, posteriormente se determinar una solución en el uso de las buenas prácticas que nos brindan los proveedores para mantener una infraestructura asegurada**

Palabras clave—IngeTic, vmware, virtual, hardening, servidor virtual, infraestructura, web, base de datos, vulnerabilidad.

I. INTRODUCCIÓN

Actualmente los datos e información que maneja las instituciones Académicas como la Facultad de Ingeniería (IngeTic) es de vital importancia, ya que puede contener información delicada de los estudiantes. La seguridad de la información así el hardening de servidores virtuales web es importante para la protección, de los ataques y vulnerabilidades que siempre existirán y por ello es de suma importancia tener bien resguardados los datos.

El servidor virtual web es un software que forma parte del servidor físico y tiene como misión principal devolver información (páginas) cuando recibe peticiones por parte de los usuarios y facilitar su disponibilidad de forma constante.

The Open Web Application Security Project (OWASP), en su reporte nos indica que los riesgos de seguridad de aplicaciones web más críticos [1], realiza un análisis sobre las vulnerabilidades más comunes encontradas en servicios web:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Known Vulnerable Components
- Insufficient Logging & Monitoring

El objetivo de este artículo es realizar un análisis y proceso de la situación actual con respecto a dificultades de vulnerabilidad y buenas prácticas de seguridad para servidores web virtual e implementar medidas de hardening y buenas prácticas de seguridad en un servidor web virtual ejecutándose sobre sistema operativo Linux.

Realizar el estudio del endurecimiento de la seguridad de la infraestructura de un servidor Virtual Web de la institución Académica (IngeTic) nos ayudara descubrir y a la vez mitigar posibles ataques sin dejar de lado la funcionalidad del servidor virtual hacia los usuarios.

Las políticas de estabilidad de la información fijan los mecanismos y métodos que debería adoptar el departamento de tecnología de toda organización académica, para salvaguardar y defender la información que dichos servidores contienen.

Servidores virtuales (VPS): Un servidor virtual es aquel que tiene una partición dentro de otro servidor físico que habilita varias máquinas virtuales por medio de varias tecnologías [2]. Un servidor virtual no es un objeto físico. Más bien, es creado por un software diseñado para imitar la función de un servidor dedicado. Se pueden alojar varios servidores virtuales en una sola máquina, compartiendo recursos de hardware.

Servidores Compartidos: Los servidores compartidos, también llamados alojamiento Web compartido o hosting compartido, son la mejor opción para empezar a disponer de un sitio Web. Generalmente, en su comienzo, el tráfico de una Web no precisará de la capacidad de un servidor dedicado o housing. Tampoco ocupará mucho espacio ni será probablemente una aplicación compleja, de modo que un servidor virtual compartido puede ser la solución más rentable [3].

Servidores Virtuales Dedicados (SVD): En el caso del servidor dedicado tenemos una máquina física que realiza todos los procesos. Los servidores dedicados funcionan en máquinas físicas, completamente independientes, a las que sólo tiene acceso el cliente. Son capaces de las mismas posibilidades de personalización que los VPS, con la ventaja adicional de asegurar que los recursos del servidor están completamente dedicados para el cliente. A continuación, se resume cada uno de los tipos de servidor de acuerdo a su funcionalidad [4].

Servidor web: Los servidores web son uno de los aspectos más importantes de Internet, ya que se trata de los encargados de despachar las páginas a los usuarios [5]. Es un sistema que recibe requests (peticiones) desde varios clientes locales o de

Para referenciar este artículo (IEEE):
[N] T. Sánchez, «Análisis y Proceso de Hardening de Servidor Virtual Web, Facultad de Ingeniería (IngeTic)», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 189-192, 2020.

internet y almacena archivos como texto, imágenes, videos que pueden ser visualizados a través del navegador, el servidor permanece ejecutando el servicio www "World Wide Web"

Hardening: (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc. innecesarios en el sistema; cerrando puertos que no estén en uso; evitar mantener la configuración por defecto [6]; además de muchas otros métodos y técnicas [7].

Herramientas para Virtualizar Servidores:

VMware: Es un de las soluciones más potentes y con más paquetes de software disponibles para virtualización. En cuanto a las soluciones de las que disponemos de licencia pagada, y también gratuita, esta aplicación lo que hace es convertir una máquina física Linux o Windows y otras máquinas virtuales en una máquina virtual VMware. https://www.vmware.com/.

Virtual Box: Es un programa para crear entornos de virtualización con múltiples sistemas operativos dentro de la máquina física totalmente funcionales y con posibilidades conectarles en red de forma física. En ella podremos instalar máquinas Linux, Mac y Windows en todas o casi todas sus versiones. Es gratuita.

Linux Ubuntu: El sistema operativo Ubuntu es una distribución de código abierto basada en Debian, cuyo punto común es Linux, la madre de todos los softwares gratuitos que actúan como sistemas operativos en los ordenadores de medio mundo. La empresa responsable de su creación y de su mantenimiento, actualizaciones y desarrollo de nuevas versiones incluidas, es Canonical, fundada por el empresario sudafricano Mark Shuttleworth [8].

II. MÉTODOS

La metodología que aplica en el desarrollo de este trabajo obedece a un esquema descriptivo, sobre la investigación de buenas prácticas.

Descriptivo**.** Se hace un análisis de las investigaciones realizadas por entidades que se encargan de documentar el estado actual en materia de seguridad web; cuáles son las vulnerabilidades más frecuentes de hallar. Además, se hace una investigación de los servidores virtuales web más utilizados, con la intención de elegir la mejor solución.

En un entorno en que prácticamente dependemos del internet y es recomendable tomar en cuenta la responsabilidad con la seguridad de la información e hardening o endurecimiento es el proceso de asegurar un sistema reduciendo sus vulnerabilidades.

Se implementará un ambiente virtual para determinar las vulnerabilidades que pueden existir en la red aplicando las buenas prácticas, instalando sistema operativo Linux Ubuntu.

En la última fase se realizará las pruebas correspondientes aplicando las herramientas open source para poder determinar las vulnerabilidades en los servidores virtuales web.

Nikto es un escáner Open Source para el servidor web, el cual realizar pruebas muy completas sobre diversos asuntos contra servidores web, incluyendo más de 6700 archivos/CGIs potencialmente peligrosos, verificación de versiones desactualizadas sobre más de 1250 servidores y problemas específicos de versión en más de 270 servidores. También verifica temas de configuración en el servidor tal como la presencia de varios archivos index, opciones HTTP del servidor, e intentará identificar servidores web y software instalado. Los temas de escaneo y plugins son frecuentemente actualizados de manera automática [9].

ModSecurity es un firewall de aplicaciones Web embebible bajo licencia GNU que se ejecuta como módulo del servidor web Apache, provee protección contra diversos ataques hacia aplicaciones Web y permite monitorizar tráfico HTTP, así como realizar análisis en tiempo real sin necesidad de hacer cambios a la infraestructura existente [10].

*Arachni***.** Se trata de un framework desarrollado con Ruby y creado para ofrecer a los usuarios diferentes características para el escaneo de aplicaciones web, Es multiplataforma, compatible con los principales sistemas operativos como son Windows, Mac OS X y Gnu/Linux. Se distribuye a través de paquetes que permiten una implementación instantánea. Es gratuito y su código fuente es público [11].

Es difícil que un sistema o aplicación esté 100% segura, de hecho, es una utopía, es más probable encontrar alguna vulnerabilidad.

Lo que se busca es evitar la desconfianza de los docentes y estudiantes de las tecnologías de Información y comunicación, también uno de los beneficios es evitar que los atacantes exploten o exploren un o muchas vulnerabilidades en los servidores virtuales web, para no acceder a los archivos o bases de datos y que puedan remplazar la información original por mensajes ofensivos o simplemente puedan redirecciones la web hacia otros sitios maliciosos.

La Facultad de Ingeniería de la Universidad Mayor de San Andrés está conformado por 12 Carreras y 4 programas. La cantidad de estudiantes aproximadamente de 9365. Cuenta con 3 servidores virtuales web, por lo tanto, la protección es indispensable aplicando hardenización en los servidores y la infraestructura de red.

III. RESULTADOS

A. Proceso de Hardening

1) Servidor web Apache

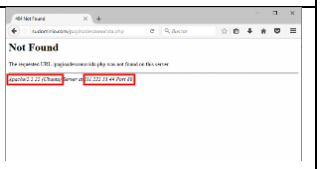
Se propone realizar las siguientes acciones para mejorar la seguridad del servidor web Apache:

- Actualizar el Servidor Web Apache
- Prevenir Ataques de Denegación de Servicio
- Prevenir Ataques de Fuerza Bruta
- Ocultar la Versión de Apache y del Sistema Operativo
- Seguridad de Encabezados

2) Actualizar el Servidor Web Apache

A pesar de que Apache tiene mucho tiempo en el mercado y su nivel de seguridad es bastante sólido, siempre existen riesgos de que se descubran nuevos problemas cuya solución puede ser implementada en nuevas actualizaciones. Es recomendable instalar las actualizaciones del sistema operativo y del software instalado allí. Puede comprobar cuál versión de Apache tiene instalada con el siguiente comando:

TABLA I. PROCESO ACTUALIZAR EL SERVIDOR WEB APACHE

Características de los comandos	Comando	Resultado
Para comprobar cuál versión de Apache está instalada se utilizó siguiente comando	httpd -v	Server version: Apache/2.2.22 (Ubuntu) Server built: Agosto 20 2018 15:32:46
El siguiente comando /CentOS/Fedora. Se Ejecutó el siguiente comando si utiliza Ubuntu:	apache2 -v	
Para actualizar Apache a su última versión se utilizó los siguientes comandos de acuerdo con su sistema:	yum update httpd Para RHEL, CentOS o Fedora. apt-get install apache2	

Configuraciones seguras: Esta actividad es importante a la hora de implementar hardening en un servidor, los permisos a usuarios y servicios mal configurados hacen vulnerable el acceso a información que pueda facilitar aún más la intrusión, por lo cual una configuración de seguridad y un dispositivo perimetral puede evitar que el atacante tome control total del sistema operativo manipulándolo de forma que se pueda acceder a otros equipos en red.

Un ataque de denegación de servicio (Dos) es un intento malintencionado de afectar la disponibilidad del sistema atacado como en este caso los servidores virtuales del IngeTic, Los atacantes suelen generar grandes volúmenes de paquetes o requerimientos para, finalmente, sobrecargar el sistema objetivo. En el caso de un ataque de denegación de servicio distribuidos (DDoS) el atacante utiliza múltiples fuentes de vulnerabilidad o fuentes controladas para generar el ataque.

Para evitar estos ataques se ha tomado en cuenta la protección de las diferentes capas del modelo OSI.

TABLA II. CAPAS DEL MODELO OSI

#	Capa	Aplicación	Descripción	Ejemplo de vector
7	Aplicación	Datos	Procesamiento de red para la aplicación	Inundaciones HTTP, inundaciones de consultas DNS
6	Presentación	Datos	Representación de datos y cifrado	Abuso de SSL
5	Sesión	Datos	Comunicación entre hosts	N/D
4	Transporte	Segmentos	Conexiones integrales y confiabilidad	Inundaciones SYN
3	Red	Paquetes	Determinación de la ruta y direccionamiento lógico	Ataques de reflexión UDP
2	Enlace de datos	Marcos	Direccionamiento físico	N/D
1	Físico	Bits	Medios, señal y transmisión binaria	N/D

En general, los ataques DDoS pueden ser segregados según la capa del modelo de interconexión de sistemas abiertos (OSI) que atacan generalmente en las siguientes capas: red (capa 3), transporte (capa 4), presentación (capa 6) y aplicación (capa 7).

3) Prevenir Ataques de Fuerza Bruta

Se ha aplicado para Linux -DenyHosts y Fail2ban- que permite usarse por separado o de forma conjunta. En este caso se ha utilizado ambas en combinación. Esto permitió generar reglas dinámicas en el propio firewall de Linux, crear reglas vivas en IpTables.

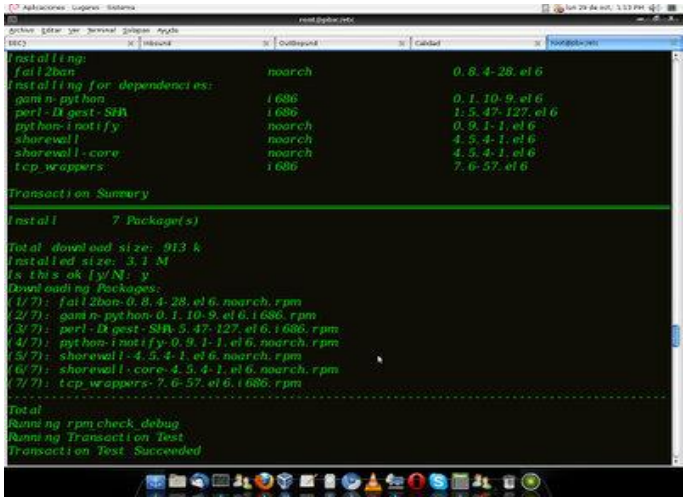


Fig. 1. Instalación y configuración de Fail2Ban

TABLA III. INSTALACIÓN Y CONFIGURACIÓN DE FAIL2BAN Y LA APLICACIÓN DE LA MISMA

Características de los comandos	Comando	Resultado
Para la instalación basta con un	yum install fail2ban	
Si no les aparece el paquete, debemos agregar el repositorio necesario:	rpm -Uvh http://mirror.metrocast.net/fedora/epel/6/i386/epel-release-6-7.noarch.rpm	Ya con esto debe empezar a instalar la aplicación junto con sus dependencias
Ahora hay que configurar Fail2Ban para que analice los logs	rpm -Uvh http://mirror.metrocast.net/fedora/epel/6/i386/epel-release-6-7.noarch.rpm	En este archivo se debe realizar lo siguiente: •Modificar es el valor bantime, este valor determina el tiempo en segundos que quedará bloqueada la IP del atacante, por defecto el valor viene en 600 segundos.

4) Configurar Fail2Ban y SSH

Para que busque intentos fallidos de logueo por SSH se modificó el archivo hasta que quedó como en la siguiente figura:

```
[ssh-iptables]
enabled = true
filter = sshd
action = iptables[name=SSH, port=22, protocol=tcp]sendmail-whois[name=SSH, dest=FredySnake@outlo
maxretry = 3 # cualquier IP que tenga tres o más intentos erroneos se bloqueara.
bantime = 86400 # Tiempo de baneo de 24 horas expresado en segundos
```

Fig. 2. Configurar Fail2Ban y SSH

5) Defensa en profundidad

Cada amenaza se clasifica según su impacto y se define en una escala de gravedad donde se puede afirmar la penetración del ataque según la línea de defensa que vulnera, con esto se puede analizar qué tipo de ataque, su efectividad, información del mismo y la forma de vulnerar las líneas de defensa.

Para lo anterior es importante incluir el log de actividades, bitácoras de incidentes y alertas de posibles intrusiones sobre la infraestructura que permitan actuar de manera inmediata ante un ataque.

6) Seguridad de encabezados

Las cabeceras HTTP pueden contener información muy útil para un atacante. Por ejemplo, cuando se realiza una petición

hacia un servidor web, en la respuesta HTTP se incluye la cabecera Server que generalmente contiene información sobre el software que ejecuta el servidor web.

Para evitar este ataque se aplicó lo siguiente: Hay dos directivas que necesitas cambiar en el archivo de configuración /etc/httpd/conf/httpd.conf:

ServerSignature Off
ServerTokens Prod

El ServerSignature aparece en la parte inferior de las páginas generadas por Apache, el error 404 (documento no encontrado).

La directiva ServerTokens sirve para determinar lo que pondrá Apache en la cabecera de la respuesta HTTP del servidor.

7) Buenas practicas

Políticas de seguridad. Una política de seguridad informática es una forma de establecer responsabilidades y lineamientos, en función de recursos y servicios informáticos. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger, el personal debe ser consiente del uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

IV. Conclusiones

En este artículo se muestra que muchas instalaciones de Apache presentan el número de versión del servidor, el sistema operativo y un informe de módulos de Apache instalados; información que los usuarios malignos tienen la posibilidad de utilizar para atacar tu servidor Virtual.

La gran mayoría de vulnerabilidades internas se encuentran asociadas a la actualización de aplicaciones, sistemas operativos y parches de seguridad que no han sido aplicados, también se encuentran aplicaciones y sistemas operativos sin soporte que representan un riesgo importante para la infraestructura de la Institución.

Referencias

[1] B. D. Rivera, «Qué es OWASP y por qué todo desarrollador debería conocerlo,» Pleets Blog, 07 12 2019. [En línea]. Available: https://blog.pleets.org/article/conoce-owasp. [Último acceso: 14 12 2020].

[2] F. Segarra, «¿Qué es un VPS? Todo lo que necesitas saber sobre servidores virtuales,» Hostinger, 11 01 2021. [En línea]. Available: https://www.hostinger.es/tutoriales/que-es-un-vps. [Último acceso: 10 2021 2021].

[3] F. Sánchez, «Human Level,» ¿Qué es un servidor compartido? Ventajas y desventajas principales, 03 02 2021. [En línea]. Available: https://www.humanlevel.com/diccionario-marketing-online/servidor-compartido. [Último acceso: 10 02 2021].

[4] M. León , «arsys,» ¿VPS o Dedicado? ¿Qué tipo de servidor necesita mi proyecto?, 27 03 2019. [En línea]. Available: https://www.arsys.es/blog/soluciones/cloud/servidores-vps-dedicados/. [Último acceso: 15 02 2021].

[5] S. Borges , «Servidor Web,» Infranetworking, 04 01 2019. [En línea]. Available: https://blog.infranetworking.com/servidor-web/. [Último acceso: 16 02 2021].

[6] P. Security, Guía de, ENDPOINTPROTECTIONPLUSoAP, 2020.

[7] P. Castro, «TIPS TECNOLÓGICOS, DE CONFIGURACIÓN Y NEGOCIO QUE COMPLEMENTAN TU SEGURIDAD,» Smartekh, 3 05 2012. [En línea]. Available: https://blog.smartekh.com/que-es-hardening. [Último acceso: 20 02 2021].

[8] . A. Rodríguez, «¿Qué es Ubuntu y para qué sirve?,» GoDaddy, 21 08 2020. [En línea]. Available: https://es.godaddy.com/blog/que-es-ubuntu-y-para-que-sirve/. [Último acceso: 21 02 2021].

[9] A. E. Caballero Quezada , «Alonso Caballero /Reydes,» ReYDeS, 27 05 2014. [En línea]. Available: http://www.reydes.com/d/?q=Nikto2. [Último acceso: 27 02 2021].

[10] A. D. Crespo, «Seguridad en Apache: modSecurity,» OpenWebinars, 18 09 2013. [En línea]. Available: https://openwebinars.net/blog/seguridad-en-apache-modsecurity/. [Último acceso: 03 1 2021].

[11] D. A, «Arachni, un escáner de aplicaciones web en Ubuntu,» Ubunlong, 10 Abril 2017. [En línea]. Available: https://ubunlog.com/arachni-escaner-aplicaciones-web/. [Último acceso: 3 3 2021].