KnE Engineering

SIIPRIN-CITEGC
Ibero-American Symposium on Computer Programming jointly held with the International Congress on Technology Education and Knowledge Management
Volume 2020

Knowledge E
enriching | engaging | empowering

Conference Paper

Use of exploit for vulnerability detection of Linux Servers

Uso de exploit para la detección de vulnerabilidades de Servidores Linux

Mario Aquino Cruz[1], Manuel Ibarra[1], Wildor Loayza Carrasco[1], Edwar Ilasaca-Cahuata[2], José Abdón Sotomayor Chahuaya[3], and Alejandro Apaza-Tarqui[4]

[1]Escuela Académico Profesional de Ing. Informática y Sistemas
Universidad Nacional Micaela Bastidas de Apurímac, Perú
[2]Departamento Académico de Ciencias Básicas
Universidad Nacional Micaela Bastidas de Apurímac, Perú
[3]Escuela Académico Profesional de Administración
Universidad Nacional Micaela Bastidas de Apurímac, Perú
[4]Escuela Profesional de Estadística e Informática
Universidad Nacional del Altiplano Puno, Perú

Corresponding Author:
Mario Aquino Cruz
mario.ac23@gmail.com

Received: 24 December 2019
Accepted: 2 January 2020
Published: 8 January 2020

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the SIIPRIN-CITEGC Conference Committee.

Abstract

At present, any computer equipment connected to the Internet is exposed to various threats, and the risk to which the servers are exposed when providing services in the cloud is no stranger. One way to prevent it is to act early, detecting the potential vulnerabilities that can be exploited by the attackers. In this way the probability of success of the attacks made is reduced. This article shows techniques for the detection of vulnerabilities with the use of exploit on Linux servers, making use of ethical hacking practices; since the use of these servers is in great demand by software developers and architects, whether it is because of the open source license it has, the ease of use and implementation of different services in these servers, and the security issue. For this, different phases were developed called recognition, port scanning, enumeration of services, vulnerability scanning, obtaining access and maintaining access. They are necessary to carry out each of the phases for their execution. The results obtained with the use of exploits were satisfactory for the detection of vulnerabilities of the different services that work on a linux server; With this information you can reduce the risks to which these servers are exposed, providing different services and working with valuable information.

Resumen. En la actualidad cualquier equipo de cómputo conectado a internet está expuesta a diversas amenazas, y no es ajena el riesgo a los que están expuestos los servidores al brindar servicios en la nube. Una manera de prevenirlo es actuar anticipadamente, detectando las vulnerabilidades potenciales que pueden ser aprovechadas por los atacantes. De esta manera se disminuye la probabilidad de éxito de los ataques realizados. El presente artículo muestra técnicas para la detección de vulnerabilidades con el uso de exploit en servidores linux, haciendo uso de las prácticas de hackeo ético; ya que el uso de estos servidores tiene mucha demanda por los desarrolladores y arquitectos de software, sea por la licencia open source que tiene, la

OPEN ACCESS

facilidad de uso e implementación de distintos servicios en estos servidores, y el tema de seguridad. Para esto se desarrollaron diferentes fases llamadas reconocimiento, escaneo de puertos, enumeración de servicios, escaneo de vulnerabilidades, obtener el acceso y mantener el acceso. Son necesarios realizar cada una de las fases para la ejecución de las mismas. Los resultados obtenidos con el uso de exploits fueron satisfactorios para la detección de vulnerabilidades de los diferentes servicios que funcionan en un servidor linux; con esta información se puede reducir los riesgos a los cuales están expuestos estos servidores que brinda diferentes servicios y trabajan con información valiosa.

Keywords: Computer security, ethical hacking, vulnerability detection, exploit, server.

Palabras clave: Seguridad informática, hackeo ético, detección de vulnerabilidades, exploit, servidor.

1. Introducción

Debido al avance tecnológico, la seguridad de toda organización pública o privada, es importante para mantener protegida todos sus activos, como datos, sistemas y servicios. La información que fluye por la red puede ser susceptible a diferentes tipos de ataques. De esta manera la información valiosa de la organización puede caer en manos equivocadas y pueden comprometer la integridad de la organización [1].

Es por eso que en la actualidad ha surgido la necesidad de implementar procesos de seguridad más efectivos y robustos y con ello efectuar técnicas de intrusiones bajo un ambiente controlado, lo cual simule un ataque real [2]. Esta simulación permite detectar vulnerabilidades, que podría aprovechar un atacante para infiltrase en la red y servidores de una organización, para manipular o colapsar servicios, u otras actividades propias de un delincuente informático [3].

La seguridad informática surge de la necesidad de proteger todos los elementos críticos que forman parte de un sistema de información que son: datos, hardware y software [4].

La seguridad informática se considera como un proceso, que consiste en mantener un nivel aceptable de riesgo, asegurar que los recursos y servicios sean usados para el fin que fueron creados.

La seguridad informática tiene como objetivo la protección de la infraestructura de una red, en especial la información que circula por la misma; para lo cual utiliza un conjunto de métodos, protocolos, herramientas, estándares, políticas orientadas a proteger la privacidad de los datos, y por ende minimizar los posibles riesgos de alteración, modificación o reemplazo de información [5].

Los elementos fundamentales de la seguridad informática son:

Confidencialidad, para garantizar que solo las personas autorizadas tienen acceso a la información.

Disponibilidad, para garantizar que los usuarios autorizados tengan acceso a la información en el momento que lo requieran

Integridad, para asegurar que la información no ha sido modificada y así garantizar la exactitud de la información

Autenticidad, para garantizar el origen de la información

No repudio, para garantizar que cualquier entidad que envió o recibió información alegue, que no lo hizo

Estos aspectos hacen necesaria la utilización de herramientas para la detección de vulnerabilidades en el desarrollo de sistemas e implementación y configuración de servidores. Las herramientas más populares para la detección de vulnerabilidades de distintos servicios que se ejecutan en los servidores.

La función de un hacker ético es efectuar ataques controlados hacia una infraestructura informática específica para detectar y explotar vulnerabilidades potenciales pero sin poner en riesgo los sistemas y servicios auditados [6].

En este trabajo se pretende obtener datos acerca de la interacción de la herramienta Kali linux, para aprovechar las vulnerabilidades de los distintos servicios, sistemas que se ejecutan en un servidor y poder tener acceso y control.

Kali Linux trae preinstalados una gran cantidad de programas relacionados con el tema de la seguridad informática (más de 600 programas), siendo algunas de las más conocidas Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (Un crackeador de passwords) y la suite Aircrack-ng (Software para pruebas de seguridad en redes inalámbricas), además del inigualable Metasploit, la gran suite de explotación de vulnerabilidades [7].

Kali Linux, en el framework de metasplot cuenta con exploits, auxiliary, post, payloads, encoder y nops, que permite ejecutar y desarrollar *exploits* contra sistemas objetivos [8].

El resto del trabajo se estructura como sigue: En la sección 2 se realiza una revisión de los principales trabajos relacionados con el análisis de escáneres de vulnerabilidades. La sección 3 describe el método y técnicas utilizas, describiendo cada componente utilizado en los experimentos realizados. La sección 4 analiza los resultados obtenidos. Por último, las conclusiones obtenidas y el trabajo futuro de este trabajo se presentan en la sección 5.

2. Trabajos relacionados

En la actualidad existen distintas herramientas de código abierto y otras de pago para poder realizar auditoria, ataques a los distintos servicios que se ofrecen en los sitios web. Se han desarrollado varios trabajos de investigación en donde se intenta evaluar las capacidades y limitaciones de las distintas herramientas de detección

En [9] se diseñó una metodología para la detección de vulnerabilidades en redes de datos. Para esto se desarrollaron diferentes fases llamadas reconocimiento, escaneo de puertos y enumeración de servicios, y escaneo de vulnerabilidades, cada una de las cuales es soportada por herramientas de software. En otros trabajos como realizados en la Universidad de las Fuerzas Armadas ESPE [10] se pudo tener un conocimiento real de las vulnerabilidades y fallas del sistema informático, estado de equipos y parches de seguridad, determinar configuraciones erróneas o de baja seguridad en los equipos de red como routers y switchs, y por último redactar las políticas de seguridad y uso de los sistemas informáticos para un manejo correcto de los recursos. En [11] se realizó un estudio para aprovechar vulnerabilidades en sistemas operativos windows y llegaron a la siguiente conclusión, que la protección de un host con sistema operativo Windows no alcanza niveles altos de seguridad. Si se quiere que la víctima active el exploit, este debe estar oculto en un archivo que no pueda ser detectado como amenaza. Al utilizar la herramienta meterpreter no se encuentran dificultades con el antivirus, ya que este trabaja a nivel de memoria. En [12]se realizó una aplicación web para el análisis de la capa SSL de páginas web, enfocándolo a usuarios interesados en conocer las vulnerabilidades, información de certificados, tipos de cifrados que soporta y protocolos. Esta herramienta permite el análisis en tiempo real y de forma remota URLs, IPs o servidores. Además de esto, permite un registro para los usuarios que realicen análisis diariamente, puesto que es necesario mantener el control de los usuarios que puedan o tengan la intención de hacer mala praxis de la aplicación. Así mismo, permite la inclusión de nuevos exploits, bajo previa validación del administrador de la aplicación para aumentar el número de vulnerabilidades analizadas en el test.

Cuenta también con la posibilidad de ver las estadísticas de los exploits (cada uno por separado) y también la de todos ellos juntos.

En [13] una aplicación para el departamento de Seguridad de TSystems que permite gestionar todo el ciclo de vida de la gestión de vulnerabilidades de sus clientes así como generar reportes y realizar seguimiento del estado de seguridad de los sistemas.

La aplicación tiene como entrada de datos información acerca de los servidores gestionados y scans de vulnerabilidades realizados con distintas herramientas. Una vez introducidos los datos en la aplicación, ésta los normaliza e integra para que los usuarios puedan mediante distintas tablas gestionar las vulnerabilidades. La gestión que realizan los usuarios va desde agrupación de servidores para realizar los scans de vulnerabilidades, asignación de distintos estados a las vulnerabilidades dependiendo de la fase en la que se encuentren de su ciclo y gestión de tickets que permiten que las vulnerabilidades se soluciones o se acepte su riesgo. Con todos estos datos gestionados por el usuario, la aplicación genera dashboards con múltiples gráficas que permiten ver se forma visual el estado general de seguridad de un cliente además de un indicador global que mide el nivel de securización de los activos. Finalmente, la aplicación permite generar reportes según la criticidad o riesgo de las vulnerabilidades en formato Word de forma automatizada, en los que se incluyen gráficas y tablas descriptivas para los clientes.

3. Métodos y técnicas

La metodología utilizada para las pruebas de penetración consta de las siguientes fases para un hackeo ético: 1 reconocimiento, 2 escaneo, 3 obtener el acceso, 4 mantener el acceso y 5 borrar huellas. A continuación se describe cada una de las fases:

Fase de reconocimiento: como primer objetivo del trabajo se ha seleccionado un servidor linux con diferentes servicios que se ejecutan en él, con servicios suficientemente representativos, como se muestra en la Figura 1.

Fase de escaneo: para mostrar los servicios que funcionan y se ejecutan en el servidor, se utilizó la herramienta kali linux, se trabajó en el terminal de kali linux y se utilizó la herramienta nmap para realizar el rastreo de puertos y servicios con el siguiente comando y tomando en cuenta algunos parametros: **nmap --Pn --T3 --sV IPServidor***;* donde namp: nos realiza el escaneo o rastreo de puertos; -Pn: es no hacer ping al servidor; -T3: es la intensidad en la duración y ejecución; sV: es la detección de la versión de los servicios que se ejecutan en el servidor; IPServidor: es el IP el servidor a hacer el rastreo.

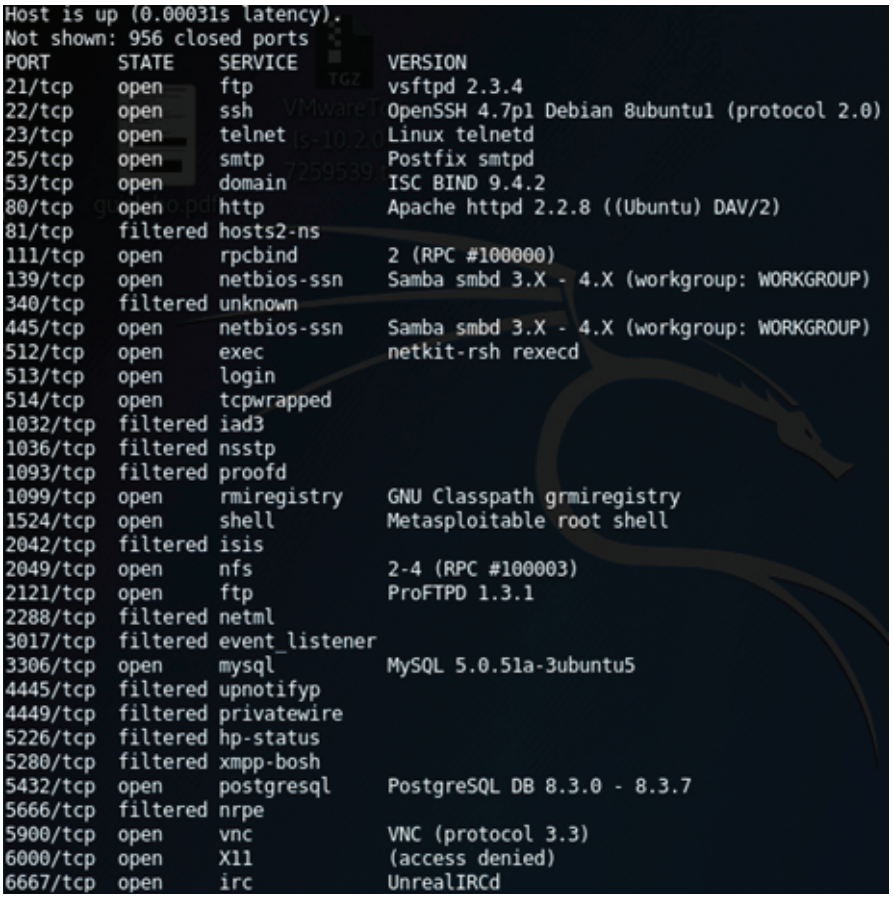

Figure 1: Lista de servicios que se ejecutan en el servidor.

En los servicios que se muestran en la figura 1, podemos visualizar el número de puerto de los servicios y su estado, asimismo la versión del servicio, este último es importante para seleccionar y utilizar el exploit adecuado para realizar el ataque.

Los servicios más conocidos que se visualizan son ftp, mysql, samba, http, postgres, vnc, entre otros. En estos servicios se realizaran procedimientos para detectar vulnerabilidades que pueden ser explotadas.

*Fase de obtener el acceso: a*l concluir el proceso con nmap y zenmap, se obtuvieron los siguientes resultados: el puerto que utilizan, el estado de los puertos y los servicios con la versión que están corriendo tal como se muestra en la figura 1.

Se verificó que existen exploits disponibles para varios servicios en el framework de metasploit de kali linux, así mismo se descargó exploits adicionales para agregar a la base de datos de kali linux del siguiente sitio web https://www.exploit-db.com.

Para esta fase se analizó uno por uno cada servicio y se ejecutó o ataco las veces que sean necesarias a los servicios haciendo uso de sus respectivos exploits, a continuación mostraremos el procedimiento de selección, utilización y ataque con exploits.

Explicaremos el primer ataque al servicio ftp por el puerto y la versión que se muestra en la figura 2

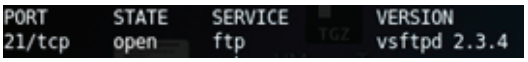

Figure 2: Servicio ftp a ser atacado.

En este paso se ejecuta el framework de metasplot de Kali Linux, con el comando *msfconsole* para poder utilizar esta herramienta, y se busca el exploit para el servicio ftp con su versión respectiva con el comando *search ftp*, tal como se muestra en la figura 3; donde se aprecia una relación de auxiliares.

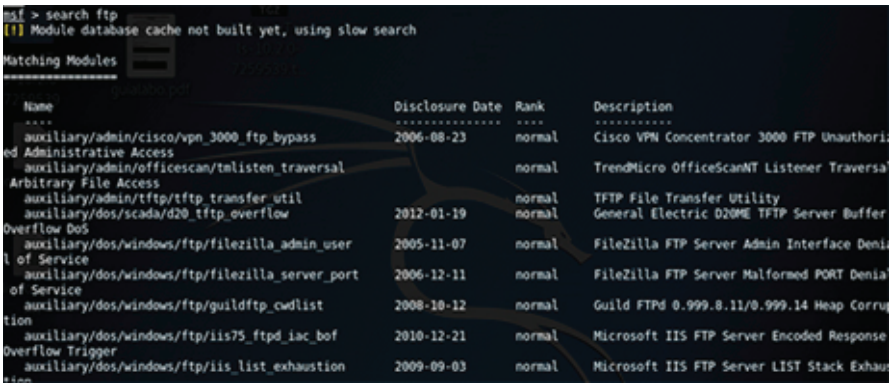

Figure 3: lista de auxiliares.

Y en la figura 4; una relación de exploit.

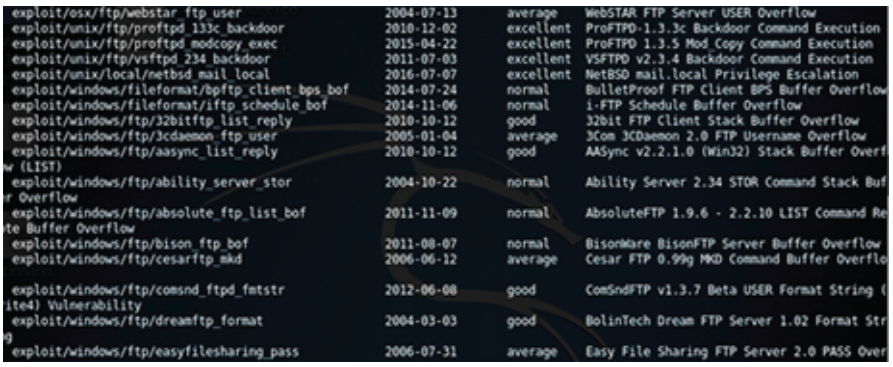

Figure 4: lista de exploit.

Podemos realizar la busqueda del exploit con la versión exacta del servicio, en este caso el servicio ftp con version vsftpd 2.34. Tal como se muestra en le figura 5.

Al encontrar el exploit adecuado para el servicio a atacar, tal como se muestra en la figura 5, seguidamente utilizamos el exploit, seleccionando la ruta establecida de dicho exploit con el comando *use*. Tal como se muestra en la Figura 6.

A continuación utilizamos el comando *show options* para ver los parámetros a configurar en el exploit seleccionado, tal como se muestra la Figura 7.

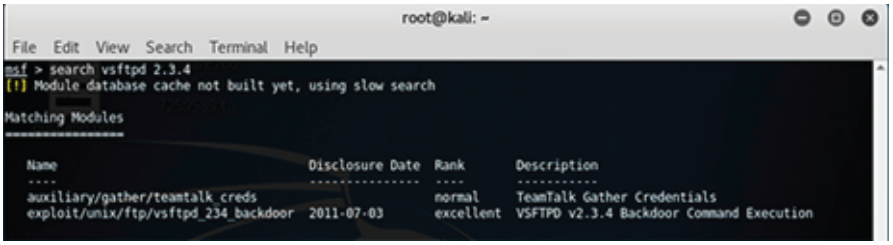

Figure 5: exploit para el servicio ftp versión vsftpd 2.3.4.

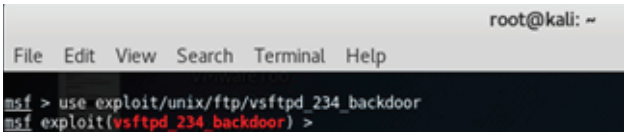

Figure 6: selección y uso del exploit.

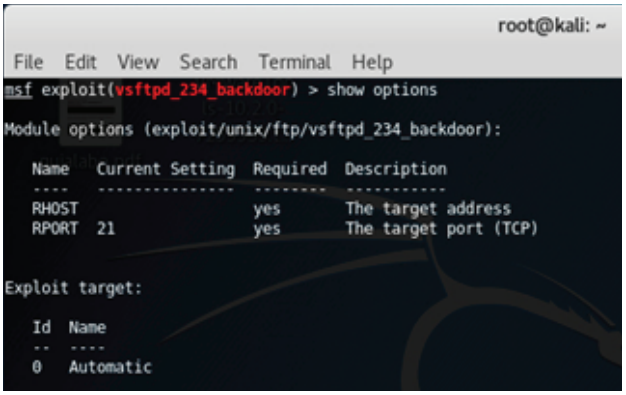

Figure 7: Visualización de los parámetros del exploit.

Agregamos el IP del servidor de kali linux, para configurar el *RHOST*, para lo cual utilizamos el comando *set*, tal como se muestra en la figura 8.

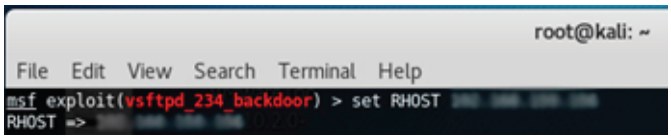

Figure 8: Configuración del IP del servidor kali linux.

Verificamos que la configuración este correcta utilizando nuevamente el comando *show options*, de esta manera queda completamente listo el exploit para ser ejecutado y lanzar el ataque al servidor víctima, tal como se muestra en la figura 9.

Finalmente se ejecuta el exploit *vsftpd_234_backdoor*, y se lanza el ataque con el comando *exploit*, y como vemos en la figura 10, el resultado es el esperado, el ataque es exitoso y se obtiene la primera sesión abierta y tenemos el acceso completo al servidor víctima.

Se realizó el mismo proceso con todos los servicios que corren en el servidor víctima, y se pudo acceder al servidor por los siguientes servicios irc, samba, php y postgres.

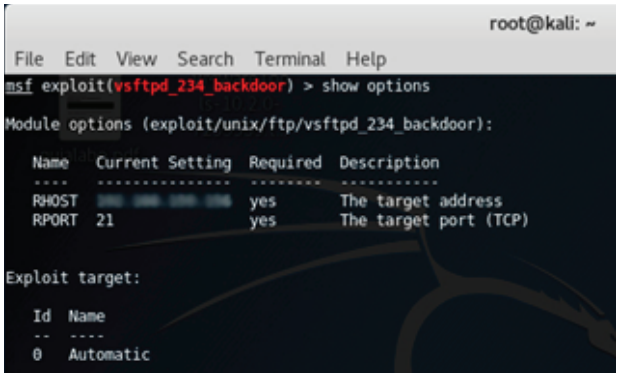

Figure 9: exploit configurado.

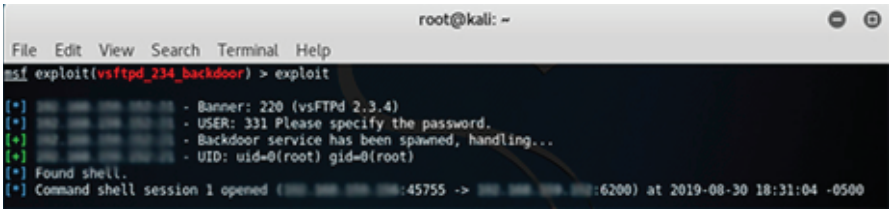

Figure 10: Sesión abierta y acceso al servidor victima.

Fase de mantener el acceso: esta fase solo se realiza si se tuvo éxito en la fase de obtener el acceso, y se trata de mantener la conexión o el acceso obtenido por el servicio que se realizó el ataque. Al mantener el acceso, el servidor se puede utilizar como plataforma para lanzamiento de nuevos ataques a otros servidores.

Fase de borrar huellas: en esta fase se trata de descubrir y destruir toda la evidencia de presencia en el servidor, alterando los log files, eliminando todos los registros del sistema que indique sobre el acceso obtenido.

4. Resultados

Los resultados obtenidos luego de realizar el hackeo ético, haciendo uso de la metodología descrita en la sección anterior fueron los siguientes, los cuales se muestran en la tabla 1.

TABLE 1: Cantidad de sitio web con CMS.

SERVICIO VULNERADO	EXPLOIT UTILIZADO
FTP	vsftpd_234_backdoor
IRC	unreal_ircd_3281_backdoor
SAMBA	username_map_script
PHP	php_cgi_arg_injection
POSTGRES	postgres_payload

Para llegar a estos resultados, se tuvo que tener perseverancia y paciencia, asimismo descargar algunos exploit para actualizar la base de datos de framework de metasploit, que eran necesarios para realizar el hackeo ético.

5. Conclusiones y trabajos futuros

En el presente trabajo de investigación se ha realizado la detección de vulnerabilidades de los diferentes servicios que corren en un servidor linux, este análisis y comprobación se realizó haciendo uso de la herramienta kali linux; utilizando el framework de metasploit a través del comando msfconsole, utilizando los auxiliares para ver los detalles de los servicios y los exploits, para realizar el ataque, todos estos procedimientos se realizaron poniendo en práctica el hackeo ético.

Mediante este trabajo de investigación se pudo concluir que con un poco de tiempo, perseverancia y conocimiento de estas herramientas, se puede vulnerar los servidores a través de los servicios que corren en él, como en este caso de estudio que se vulneraron a través de los servicios de ftp, irc, samba, php y postgres.

Es importante que las organizaciones hagan una evaluación de vulnerabilidades de los servicios que ofrecen sus servidores antes, durante y después de su implementación y puesta en funcionamiento para la atención de los usuarios.

La metodología, herramientas y técnicas utilizadas en el presente trabajo de investigación, ayudo a obtener buenos resultados, los cuales se visualizan en la tabla1, vulnerando 5 servicios, se recomienda actualizar estos servicios para minimizar los riesgos de vulnerabilidad, darle importancia al momento de instalar el sistema operativo y los diferentes programas a utilizar en el servidor ya que muchos de ellos se ponen por defecto, y estos pueden ser innecesarios, o pueden causar que servicios no deseados se ejecuten en el servidor, sin que el administrador se entere, lo cual puede causar trafico indeseado, o un camino de entrada para delincuentes informáticos.

Es de vital importancia que todas las organizaciones dentro del proceso de la evaluación de la seguridad de la información dentro de una organización, que el personal que lleve a cabo esta evaluación realice pruebas de penetración y tenga una formación adecuada y experiencia, esto garantizara que el proceso sea transparente, garantizando buenos resultados al terminar la evaluación.

Finalmente las recomendaciones que se hacen luego de este trabajo de investigación, sería que le den importancia al tema de seguridad informática particularmente a los servicios que ofrecen los servidores ya que están expuestos a diferentes ataques

informáticos en la red, hacer frecuentemente un análisis en la detección de vulnerabilidades en sus servicios. Realizar actividades de concientización y capacitación a los responsables directos que administran estos servicios, de esta manera minimizar los riesgos asociados a seguridad informática. Asimismo es muy importante que los servicios de los servidores estén constantemente actualizados. De esta manera ser menos propenso a estos tipos de ataques.

Los trabajos futuros a desarrollar luego de esta investigación, serian realizar pruebas de penetración con diferentes servidores tanto propietarios como windows y de licencia libre como Linux. Asimismo utilizar otras herramientas de código abierto que se encuentren disponibles para realizar este tipo de ataques de penetración haciendo uso del hackeo ético.

References

[1] l. a. mendaño mendalo y h. s. m. helena, «Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red,» Quito, 2016.

[2] H. Jara y P. Federico, Ethical Hacking 2.0, Implementación de un Sistema para la Gestión de Seguridad, Buenos Aires: Redusers, 2012.

[3] J. M. Baltazar Gálvez y J. C. Campuzano Ramírez, «Diseño e implementación de un esquema de seguridad perimetral para redes de datos,» Mexico, 2011.

[4] L. R. Roba Iviricu, J. R. Vento Alvarez y L. E. García Concepción, «Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux,» *Revista Cientifica Avances,* vol. 18, no 4, pp. 334-344, 2016.

[5] P. Aguilera López, Seguridad Informática, Madrid: Editex, 2010.

[6] K. Astudillo, Hacking Etico 101: Como Hackear Profesionalmente En 21 Dias O Menos!, Createspace Independent Pub, 2013.

[7] R. Singh Patel, Kali Linux Social Engineering, Packt Publishing Ltd, 2013.

[8] D. Santo Orcero, Pentesting Con Kali, BLURB Incorporated, 2017.

[9] D. A. Franco, J. L. Perea y P. Puello, «Methodology for Detecting Vulnerabilities in Data Networks,» *Información Tecnológica,* vol. 23, no 3, pp. 113-120, 2012.

[10] S. Castañeda y D. Mercedes, «Análisis y diagnóstico de vulnerabilidades informáticas en la red de datos de la empresa YOUPHONE Cía. Ltda. Utilizando Hacking Ético,» Sangolqui, 2016.

[11] S. Arévalo, G. Infante, D. Valdivia y J. Velásquez, «Aprovechamiento de vulnerabilidades del,» *Revista Electrónica de la Faculta de Ingeniería,* vol. 2, no 1, pp. 53-60, 2014.

[12] I. Sánchez Prieto, «Herramienta de análisis automático de vulnerabilidades SSL,» Madrid, 2016.

[13] S. Cuevas López, «Herramienta de gestión de vulnerabilidades en sistemas,» Madrid, 2017.