Tipo de artículo: Artículo original

Seguridad ofensiva mediante hacking ético para fortalecer infraestructuras en redes de telecomunicaciones

Offensive security through ethical hacking to strengthen telecommunications network infrastructures

Carlos Gabriel Cuadros Navarro[1*] , **https://orcid.org/0000-0001-7299-7872**
Vicente Félix Veliz Briones[2], **https://orcid.org/0000-0003-4092-1421**
Jorge Luis Veloz Zambrano[3], **https://orcid.org/0000-0002-9001-4478**
Marely del Rosario Cruz Felipe[4], **https://orcid.org/0000-0003-1937-1568**

[1] Instituto de Posgrado, Universidad Técnica de Manabí. ccuadros7268@utm.edu.ec
[2] Facultad de Ciencias Informáticas, Universidad Técnica de Manabí. vicente.veliz@utm.edu.ec
[3] Facultad de Ciencias Informáticas, Universidad Técnica de Manabí. jorge.veloz@utm.edu.ec
[4] Facultad de Ciencias Informáticas, Universidad Técnica de Manabí. marely.cruz@utm.edu.ec

*** Autor para correspondencia: ccuadros7268@utm.edu,ec**

Resumen

Con el crecimiento exponencial del uso del internet y debido a la alta incidencia de ataques cibernéticos destinados a encontrar vulnerabilidades en los servicios de redes y comunicación; en los últimos años se ha incrementado la adopción de medidas de seguridad en las direcciones de Tecnologías de Información y Comunicación (TIC) de las instituciones públicas. El objetivo de la presente investigación es generar un plan de aseguramiento de la información, aplicando normas destinadas a cumplir con este objetivo, como es el caso de la ISO 27001 y usando la metodología de Seguridad Ofensiva (OS). Para este propósito, se estableció un esquema controlado para la realización de una auditoria de seguridad informática mediante pruebas de penetración utilizando técnicas de hacking ético a infraestructuras de redes de telecomunicaciones, con el objetivo de detectar las vulnerabilidades para poder determinar con efectividad las medidas necesarias a tomar.

Palabras clave: Hacking ético, seguridad de la información, ciberataques.

Abstract

With the exponential growth of Internet use and due to the high incidence of cyber attacks aimed at finding vulnerabilities in network and communication services, in recent years there has been an increase in the adoption of security measures in the Information and Communication Technology (ICT) departments of public institutions. The aim of this research is to generate an information assurance plan, applying standards designed to meet this objective, as is the case with ISO 27001 and using the Offensive Security methodology (OS). For this purpose, a controlled scheme was established to carry out a computer security audit by means of penetration tests using ethical hacking techniques to telecommunications network infrastructures, with the aim of detecting vulnerabilities in order to effectively determine the necessary measures to be taken.

Keywords: *Ethical hacking, information security, cyber attacks.*

Recibido: 20/08/2021
Aceptado: 27/11/2021

Introducción

El aumento de la interconectividad informática y la popularidad del Internet están ofreciendo a las organizaciones todo tipo de oportunidades sin precedentes para mejorar sus operaciones, reduciendo significativamente los costos al compartir información. Sin embargo, el éxito de muchos de estos esfuerzos depende, en gran parte, de la capacidad de la organización para proteger los tres pilares fundamentales de la seguridad de la información que son: la integridad, la confidencialidad y la disponibilidad de los datos y de los sistemas informáticos.

Día a día las empresas están sometidas a riesgos que ponen en peligro los tres pilares fundamentales de la seguridad de la información, los cuales pueden ser: externos e internos.

Aunque la seguridad de la información juega un papel importante en la protección de los datos y de los activos de una organización, a menudo oímos noticias sobre delitos informáticos, como la alteración de sitios web o robo de datos. Las organizaciones tienen que ser plenamente conscientes de la necesidad de dedicar más recursos a la protección de los activos de información y seguridad de la información, la cual debe convertirse en una de las principales preocupaciones de una empresa. ¿ Pero cómo lograr esto?, ¿cómo enfrentar los riesgos a los cuales están expuestas las empresas?. Para ello han surgido varias normas, leyes e inclusive metodologías para que las empresas puedan crear sus propias políticas, procesos y procedimientos.

Un buen comienzo es saber que tan expuesto se está; para ello, las empresas deben realizar ya sea con personal interno o con empresas externas, una serie de pruebas a toda la infraestructura tecnológica para encontrar las vulnerabilidades de riesgo bajo, alto y otras que puedan llegar a ser aprovechadas por algún atacante, ya sea externo o interno.

A esas pruebas realizadas se las conoce como pentesting o pruebas de penetración aplicando técnicas de hacking ético, dónde se busca que las empresas sepan sus fallos de seguridad y las consecuencias que existen, para tomar los controles pertinentes.

Es necesario que las organizaciones tomen medidas preventivas contra los ataques informáticos, cómo las auditorías de seguridad. Para ello, debe considerarse una metodología que se adapte a las necesidades de la empresa. Entre las metodologías de auditoría informática más conocidas son: Manual de métodos de prueba de seguridad de código abierto (OSSTMM), Marco de evaluación de sistemas de información de seguridad (ISSAF), Aplicación del Proyecto de Seguridad de la Web Abierta (OWASP), Certificado de Hacking Ético (CEH) y Seguridad Ofensiva (OS). (Maya & Jaramillo, 2016)

Desde el punto de vista de (Tori, C., 2015), la seguridad de información es definida como una implantación y gestión de un conjunto de acciones pertinentes, con la finalidad de resguardar y proteger los datos e información, ajustadas a mantener en todo momento la confidencialidad, disponibilidad e integridad de la plataforma digital.

En el entorno actual de las TI, las organizaciones son cada vez más dependientes de sus sistemas de información. La información es un activo que, como otros activos comerciales es muy importante y esencial para el negocio, por lo tanto necesita ser protegido adecuadamente, ya que la información está expuesta a un número cada vez mayor de usuarios y por tanto a una variedad más amplia de amenazas cada vez son más sofisticadas.

Con el crecimiento exponencial en el uso del Internet en los últimos 10 años, tanto las empresas grandes como las pequeñas, se han visto obligadas en asegurar su componente vital que es la tecnología de la información. Actualmente las empresas, cuenta con el valioso recursos de TI, tales como computadoras, redes de datos, sistemas informáticos, etc. Para la protección de los activos de una empresa, se sugiere que haya tenido al menos una auditoría de seguridad, con el fin de obtener una imagen clara de los riesgos de seguridad que enfrentan y saber la mejor manera de tratar con esas amenazas.

El propósito de una auditoría de seguridad no es para culpar o desmerecer el diseño de una red, sino para garantizar la eficacia, integridad y el cumplimiento de las políticas de seguridad de la empresa. La auditoría ofrece la habilidad de probar los sistemas, encontrar riesgo y comprobar si los controles son los apropiados para mitigar la exposición a los diferentes riesgo, cabe recalcar que la auditoría de seguridad no sólo trata de cómo ejecutar un sin número de herramientas de hackers, en un intento de entrar en la red (Maya & Jaramillo, 2016).

La ISO/IEC 27001:2013representa el estándar internacional desarrollado como una guía para el análisis, implementación, control y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), a través del establecimiento de un grupo de requisitos a cumplir con este motivo. Dado su enfoque orientado a los procesos de negocio, es una norma general aplicable a una gran gama de empresas, adaptándose a los diferentes giros de negocio y activos de información que éstas puedan tener. La versión correspondiente al año 2013 presenta una nueva estructura según el estándar definido por ISO/IEC para todas las normas referentes a sistemas de gestión, facilitando la integración y trabajo conjunto entre los diferentes estándares de gestión publicados por dicha entidad.

A diferencia de su versión anterior – ISO/IEC 27001:2005 – la norma actual no nombra el ciclo de Deming (Plan, Do, Check, Act) como metodología para definir el ciclo de vida – y mejora continua – del sistema de seguridad a implementar, dejando abierta la posibilidad de la entidad a elegir un modelo de mejora continua distinto y que se adapte mejor a sus necesidades (Álvarez, 2015).

Como se muestra en la Figura 1, la norma se basa en el cumplimiento del SGSI, que tiene el principio de ofrecer Confidencialidad, integridad y disponibilidad de la información.

Figura 1. Áreas de evaluación de la seguridad de la información.

Según (Mejia, J., & Hernández, A., 2015), pentesting es una técnica que consiste en simular el ataque de entornos informáticos controlados o virtualizados, con una misión de descubrir y explotar vulnerabilidades, logrando el objetivo de documentar el ataque y recopilar información sobre debilidades, para dar una evaluación de seguridad de un sistema u organización. La simulación, se centra en un ciberataque que pretende manipular la información, robarla o controlar el sistema; aprovechando fallas y vulnerabilidades conocidas por los expertos. Es de resaltar que, dado los avances en la generación de software con código malicioso, es frecuente el uso de esta técnica de ciberseguridad en las instituciones y organizaciones, integradas en los procedimientos de análisis de seguridad en el ámbito de información.

Se puede definir que un *hacker* es alguien capaz de traspasar las barreras de seguridad, consiguiendo hacer cosas que van desde lo curioso hasta lo asombroso. Las personas que se puede definirse como *hacker* emplean sus conocimientos para violentar debilidades de los sistemas de información, esto es el resultar de muchas horas de estudio y prácticas de estas técnicas, así como también empleando o generando herramientas (Gupta, S., 2019).

La sola palabra *hacker* no define si una persona usa su conocimiento para el bien o el mal, es por ello que el término se ha dividido en tres tipos, según la obra de (Begum, S., & Ashhar, S. K., 2016).

El Hacking Ético o test de penetración es visto como un procedimiento de ciberseguridad pues se trata de emular un ataque real para filtrarse en un sistema informático o una red bajo el consentimiento del propietario con la intención de descubrir debilidades y vulnerabilidades que un cibercriminal podría utilizar. Esto permite a la compañía entender las necesidades en seguridad que afronta y mejorar sus sistemas según lo requirieran (Berger & Jones, 2016).

Cuando se empieza en el tema de la seguridad se presenta algo de confusión entre un hacking ético y una auditoría informática. De hecho mucha gente lo confunde en el medio, sin embargo existen grandes diferencias.

La auditoría informática trata las políticas de seguridad de la compañía y el cumplimiento de estas o cómo se están llevando en los procesos. Se busca validar que existan controles de la seguridad y en muchos casos puede no ser técnica.

El hacking ético se enfoca en vulnerabilidades que pueden ser explotadas por terceros y que puedan ser explotadas, para de esta manera comprobar la resistencia que ofrece el sistema ante este tipo de ataques (K. Beaver, 2014).

El Hacking ético como servicio de auditoría, debe de estructurarse como tal, y como lo que es «Una serie de pruebas técnicas de auditoría», cuyos resultados deben de valorarse, y estar soportados con base a diferentes variables.

Materiales y métodos

Para este proyecto de investigación se usó la Metodología de Seguridad Ofensiva (OS) como marco referencial, siendo aplicable desde cualquier ubicación; cuyo propósito es identificar y delimitar el sistema bajo estudio, identificar las vulnerabilidades y realizar las pruebas de penetración a la red informática explotando sus debilidades, con el fin de verificar si los controles aplicados mejorarán la seguridad informática, reduciendo así los posibles ataques a los que se estuvieran expuestos. Esta metodología cuenta con 5 fases, como se muestra en la figura 2, las mismas se detallan a continuación.

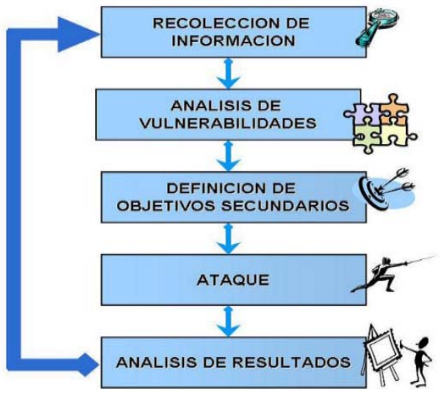

Figura 2. Áreas de evaluación de la seguridad de la información.

Recolección de información

En esta etapa se realiza una evaluación de la situación actual de la empresa. En este caso de estudio se usará el sistema operativo Kali Linux y herramientas como theHarvester y Maltego para recolectar la información. También se emplearán el uso de cuestionarios. Según (Balestrini A. Mirian, 2006), estos cuestionarios exponen cierta falta de preparación, experiencia y herramientas frente ataques cibernéticos, y permiten filtrar la metodología a aplicar en la fase de experimentación a una más eficiente, enfocándola principalmente a aquellas ramas que se notan claramente más débiles y explotables del sistema, según el análisis preliminar realizado.

Análisis de vulnerabilidades

Una vez recolectado la información, se deben encontrar las vulnerabilidades que existen en la red institucional. Para ello se usa Kali Linux que es un aplicativo que está conformado por un compendio de herramientas diseñadas para probar y encontrar vulnerabilidades en plataforma de información (Santo, D., 2018). Se utiliza herramientas como Nmap para el escaneo de puertos; Footprinting para encontrar información crítica que es pública para el usuario; y escanear vulnerabilidades usando Nessus.

Definición de objetivos secundarios

En la mayoría de los escenarios, el objetivo del ataque no está al alcance o es visible; es decir, hay barreras o etapas que deben ser superadas para alcanzar el objetivo principal. Para ello, deben determinarse las medidas de acceso y deben superarse estos obstáculos. En esta investigación, se establecen como objetivos secundarios los siguientes: redes inalámbricas, computadoras y los dispositivos de conmutación y enrutamiento.

Ataques

Un ataque es cualquier acción que viole la seguridad de un sistema o red informática. En esta etapa comienza la explotación de las vulnerabilidades de la infraestructura de la red; en este caso se usan herramientas como Wireshark, Metasploit que vienen instaladas en Kali Linux, ya que es una herramienta robusta para realizar auditorías informáticas.

Análisis de resultados

En este apartado se analizan los resultados de los ataques realizados para proponer soluciones efectivas.

Resultados y discusión

Las pruebas llevadas a cabo para la presente investigación se desarrollaron en una Red de Área Local bajo la arquitectura cliente servidor. La ejecucion de las pruebas se realizó implementando los módulos de herramientas que correspondan a cada una de las fases planeadas para el desarrollo del test de penetración.

Para tomar como referencia el análisis de riesgo de la empresa, se usa la herramienta MSAT versión 4.0.2.35, cuyos resultados se muestran en la Figura 3, donde se observa de acuerdo a los índices Perfil de riesgo de la empresa (BRP) y el Índice de Defensa en Profundidad (DiDI) que el riesgo empresarial es alto.

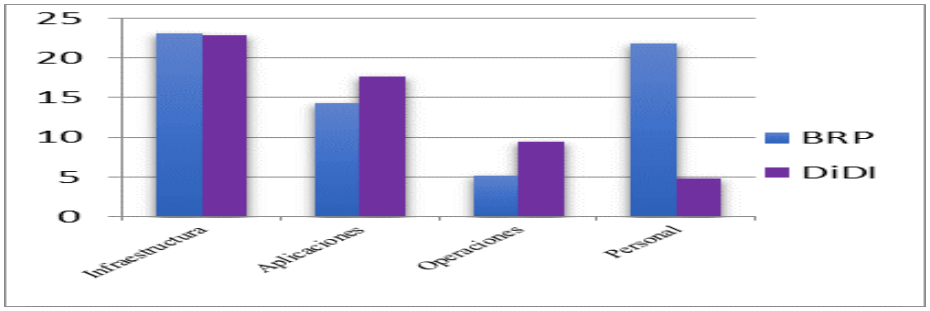

Figura 3. Resultados obtenidos con la herramienta MSAT 4.0.2.35.

Para entender los resultados, se explica a continuación en que consiste cada índice:

Perfil de riesgo de la empresa (BRP): Medida del riesgo al que está expuesta una organización, según el entorno y el sector en el que opera. La puntuación del BRP va de 0 a 100. Una puntuación más alta representa un mayor riesgo para que la institución esté expuesta en esta área de análisis.

Índice de Defensa en Profundidad (DiDI): Medición de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para ayudar a reducir los riesgos identificados en una organización. DiDI también tiene una puntuación de 0 a 100. Una puntuación más alta significa un entorno en el que se han adoptado más medidas para aplicar las estrategias de la DiDI en la esfera del análisis específico. La puntuación DiDI no indica la eficacia general de la seguridad o incluso la cantidad de recursos destinados a ella, sino que cuantifica la estrategia general utilizada para defender el medio ambiente (Cuzme-Rodríguez et al., 2019).

Por lo general, es mejor contar con una calificación de DiDI igual a la de BRP para la misma categoría. Un desequilibrio en cualquier dirección, puede indicar la necesidad de volver a alinear sus inversiones de TI.

Aplicación de la metodología en seguridad ofensiva

- Recolección de Información

Se emplea la herramienta theHarvester como vemos en la Figura 4, donde se muestran los datos de los subdominios, cuentas de correos, direcciones ip, entre otras. Con la ayuda del script cewl se crea un diccionario para poder hacer ataques mediante diccionario.

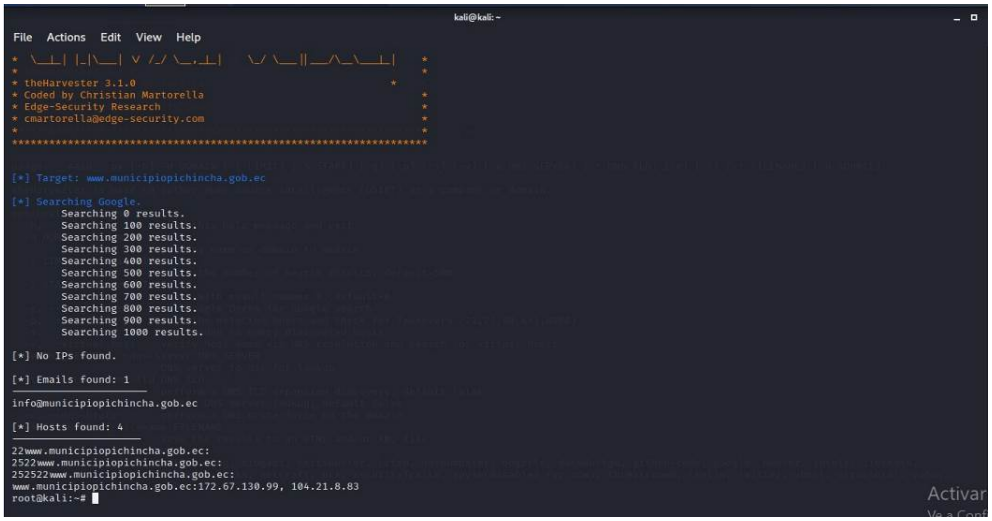

Figura. 4. Resultados obtenidos con la herramienta theHarvester.

- Identificación de Servicios

Se procedió a realizar un sondeo en los puertos para encontrar los servicios que se estén ejecutando.

Para el análisis y sondeo de puertos se utilizó la herramienta NMAP que viene preinstalada en Kali, para la exploración tanto de los puertos como de los servicios de cada uno de los equipos en cuestión, como se muestra en la Figura 5.

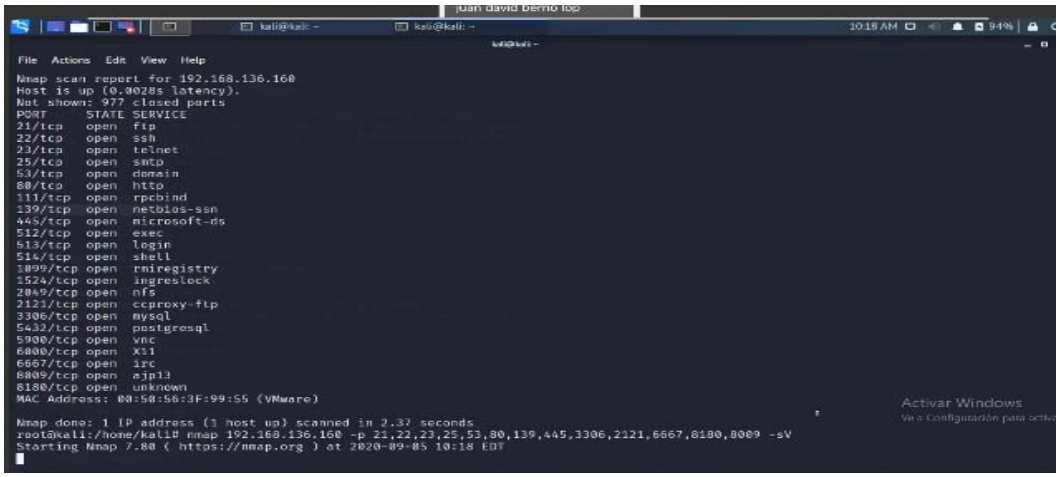

Figura 5. Resultados obtenidos con la herramienta Nmap.

- Identificación de Vulnerabilidades

Para ejecutar el punto actual se utilizaron las herramientas de detección de vulnerabilidades como Nessus.

En la Figura 6 se observa el nivel de criticidad de los Servidores Windows Server.

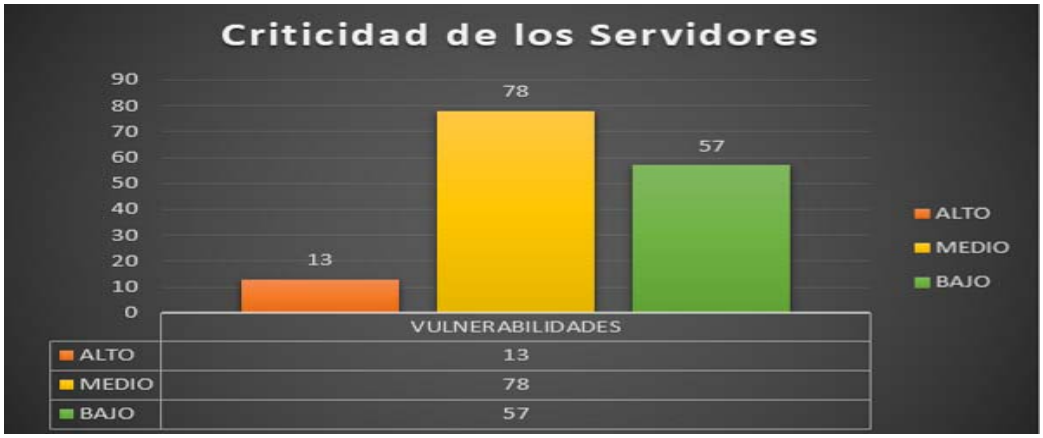

Figura 6. Criticidad de los servidores.

A pesar de haber identificado un bajo número de vulnerabilidades categorizadas con riesgo alto, las mismas fueron suficientes para acceder a los sistemas y comprometer la infraestructura como es el caso del servidor SQL Server, correspondiente a este caso de estudio.

En la Figura 7 se observa el análisis realizado al servidor de base de datos.

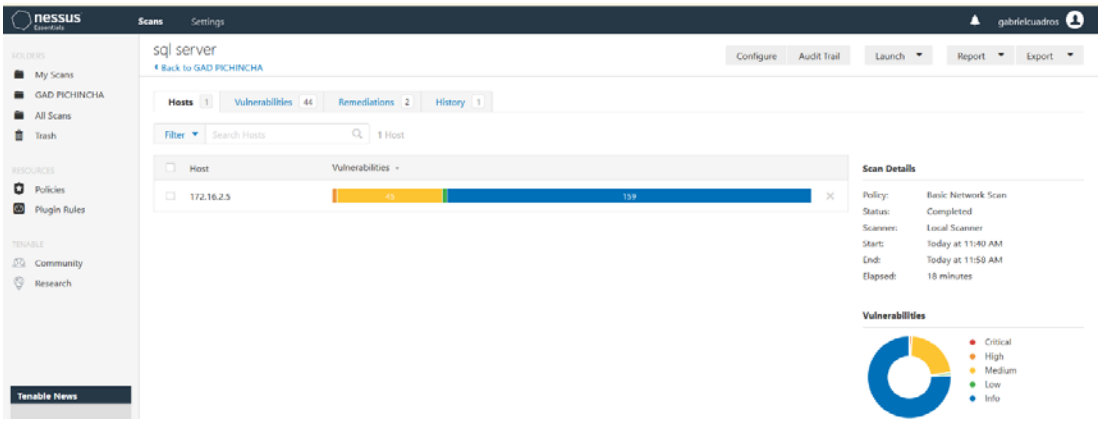

Figura 7. Análisis completo al servidor de Base de datos con herramienta Nessus.

- Ataques

La información obtenida de las etapas anteriores servirá para ejecutar ataques de explotación utilizando la herramienta Metasploit, como se muestran en las Figuras 8, 9 y 10, donde se aprovecha de la debilidad del servidor sql server por tener el servicio iniciado de manera local, lo que permite al atacante ingresar con todos los privilegios de acceso haciendo una conexión reversa luego de romper las contraseñas usando ataque por diccionario.

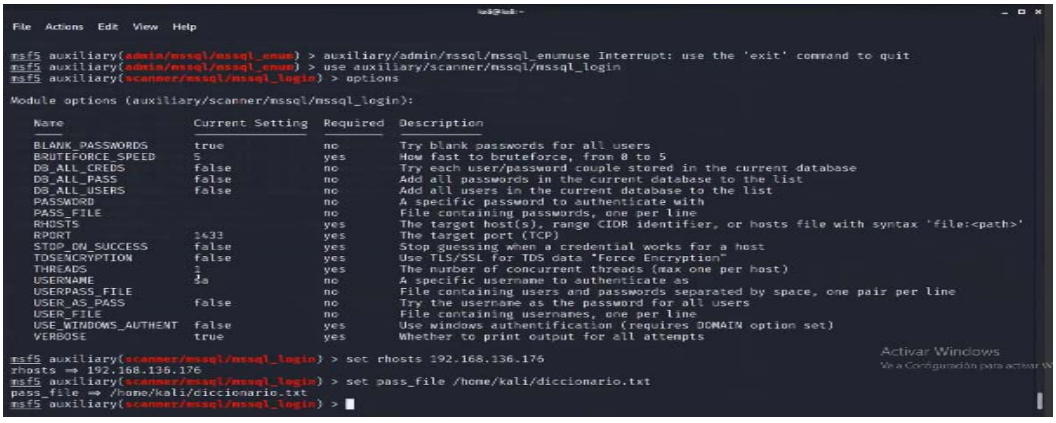

Figura 8. Uso de herramienta Metasploit

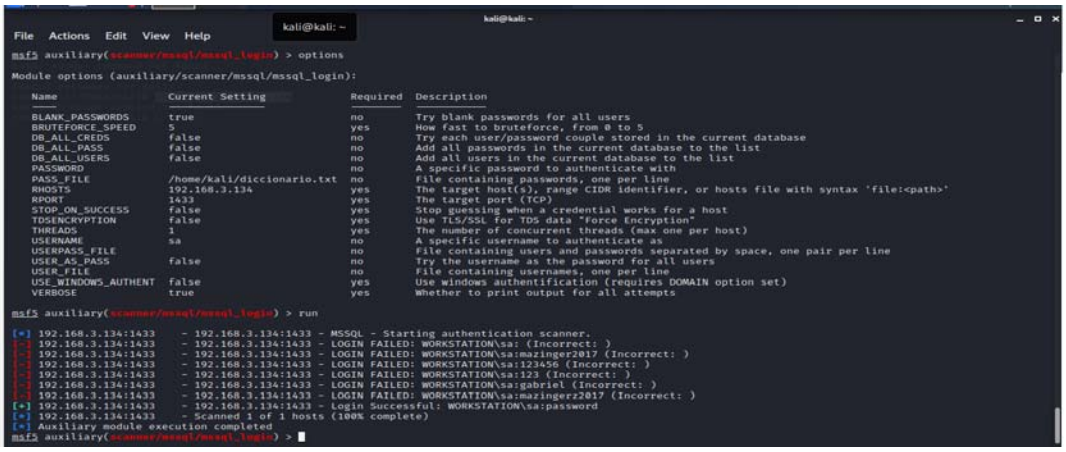

Figura 9. Ataque de fuerza bruta por diccionario.

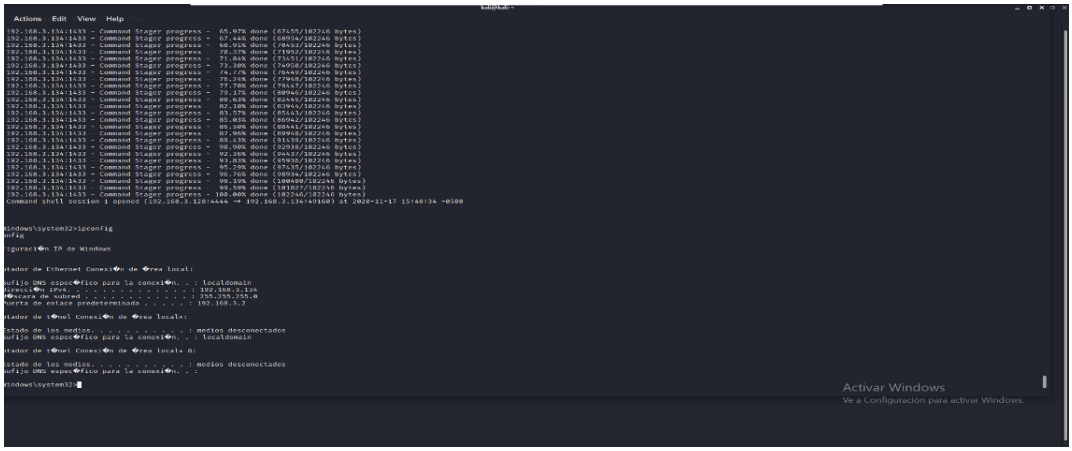

Figura 10. Conexión por puerta trasera.

Para erradicar esta vulnerabilidad se emplean las siguientes soluciones:

- Se debe configurar el servicio del Servidor SQL Server como servicio de red para que los privilegios de acceso sean limitados.
- Al no tener una DMZ y carecer de firewall, se propone el uso de un firewall gratuito y potente como el pfsense, para que el administrador de la red, pueda percatarse de alguna actividad sospechosa.
- Se debe actualizar la versión del php y del apache a una versión superior.

Una vez aplicadas las posibles soluciones, se ejecuta nuevamente la herramienta Nessus, cuyos resultados se plasman en la figura 11, donde se demuestra que las vulnerabilidades altas existentes en el servidor SQL Server se erradicaron, quedando solamente las informativas.

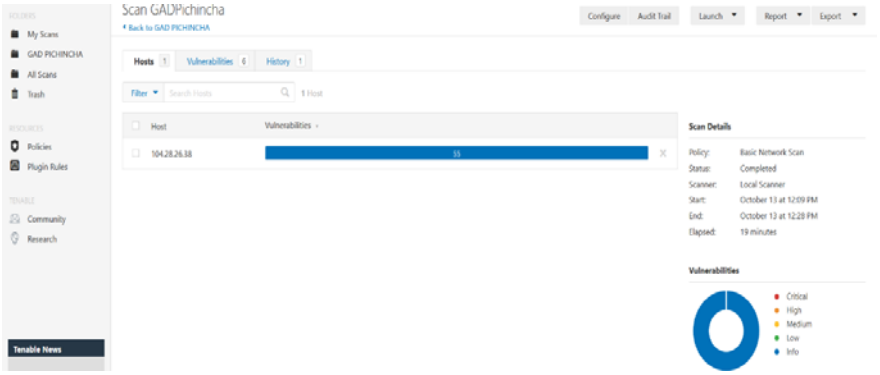

Figura 11. Análisis completo al servidor de Base de datos con herramienta Nessus, luego de aplicar las recomendaciones.

De la misma forma, la criticidad general de los equipos servidores se redujeron, como se observa en la Figura 12.

Figura 12. Resultados finales (Criticidad de los servidores)

- En el presente trabajo investigativo se opta por usar la metodología de Seguridad Ofensiva, ya que ésta, permite realizar una serie de ataques de acuerdo a las vulnerabilidades encontradas en la fase de recolección de información.
- Con técnicas de explotación y post explotación se obtienen las soluciones.
- Las soluciones presentadas en este artículo son consistentes con los problemas de seguridad más comunes en la red informática de las instituciones.

Conclusiones

- El Pentesting permite evaluar y encontrar riesgos que existen en los diferentes dispositivos de red, para poder prevenir cualquier amenaza que pueda existir.
- La metodología de Seguridad Ofensiva fue elegida porque, a diferencia de otras metodologías, ésta identifica en tiempo real el grado de exposición que tiene una organización y que tan afectado se estaría ante cualquier ataque que se produjera.
- La norma ISO / IEC 27001 es la guía para la realización de manuales de políticas y procedimientos de seguridad.
- Los resultados obtenidos del análisis de riesgo con la herramienta MSAT 4.0.2.35, el análisis de vulnerabilidades con la herramienta Nessus, el escaneo de puertos con Nmap y la recolección de información obtenida con la herramienta theHarvester permitieron descubrir los fallos en seguridad.
- Se debe emplear el uso de un firewall para fortalecer la seguridad de la infraestructura tecnológica.

Conflictos de intereses

Los autores de la presente investigación declaran que no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Carlos Gabriel Cuadros Navarro.
2. Curación de datos: Marely del Rosario Cruz Felipe
3. Análisis formal: Jorge Luis Veloz Zambrano
4. Adquisición de fondos: Vicente Félix Veliz Briones.
5. Investigación: Carlos Gabriel Cuadros Navarro.
6. Metodología: Jorge Luis Veloz Zambrano
7. Administración del proyecto: Marely del Rosario Cruz Felipe.
8. Recursos: Carlos Gabriel Cuadros Navarro.
9. Software: Carlos Gabriel Cuadros Navarro.
10. Supervisión: Marely del Rosario Cruz Felipe.
11. Validación: Marely del Rosario Cruz Felipe.
12. Visualización: Carlos Gabriel Cuadros Navarro.

13. Redacción – borrador original: Carlos Gabriel Cuadros Navarro.
14. Redacción – revisión y edición: Vicente Félix Veliz Briones.

Financiamiento

La investigación ha sido financiada a partir de medios propios de los investigadores.

Referencias

Álvarez, V. R. T. (2015). Alvarez y Vasco -2015- Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. *2015*.

Balestrini A. Mirian. (2006). *Como elaborar el Proyecto de Investigación. BL Consultores Asociados. 7ª edc. Caracas (Venezuela).*

Begum, S., & Ashhar, S. K. (2016). *Begum, S., & Ashhar, S. K. (2016). A Comprehensive study on ethical hacking. International journal of engineering sciences y reseach, 214-219.*

Berger, H., & Jones, A. (2016). Cyber Security & Ethical Hacking For SMEs. *Proceedings of the The 11th International Knowledge Management in Organizations Conference on The Changing Face of Knowledge Management Impacting Society - KMO '16*, 1-6. https://doi.org/10.1145/2925995.2926016

Cuzme-Rodríguez, F., León-Gudiño, M., Suárez-Zambrano, L., & Domínguez-Limaico, M. (2019). Cuzme-Rodríguez et al. - 2019 -Offensive Security: Ethical Hacking Methodology on the Web. En M. Botto-Tobar, L. Barba-Maggi, J. González-Huerta, P. Villacrés-Cevallos, O. S. Gómez, & M. I. Uvidia-Fassler (Eds.), *Information and Communication Technologies of Ecuador (TIC.EC)* (Vol. 884, pp. 127-140). Springer International Publishing. https://doi.org/10.1007/978-3-030-02828-2_10

Gupta, S. (2019). *Gupta, S. (1 de Enero de 2019). Ethical Hacking – Orchestrating Attacks. Recuperado el 27 de abril de 2021, de https://link.springer.com/video/10.1007%2F978-1-4842-4340-4*.

K. Beaver,. (2014). *K. Beaver, Hacking for dummies 4th Edition, New Jersey: John Wiley & Sons, Inc., 2014.*

Maya, E. A., & Jaramillo, D. D. (2016). Maya y Jaramillo—2016 -Auditoría de seguridad informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en las normas NTP ISO/IEC 17799:2007 y la metodología OSSTMM v2. *2016*, 8.

Mejia, J., & Hernández, A. (2015). *Mejia, J., & Hernández, A. (1 de Febrero de 2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. ReCIBE, Revista electrónica de Computación, Informática Biomédica y Electrónica., IV(1), 1-18.*

Santo, D. (2018). *Santo, D. (2018). Kali Linux. Madrid, España: Ra-Ma.*

Tori, C. (2015). *Tori, C. (2015). Hacking Ético. Buenos Aires.*