Revista Arbitrada Venezolana
del Núcleo Costa Oriental del Lago

Impacto Científico

Universidad del Zulia

Junio 2023
Vol. 18 Nº 1

ppi 201502ZU4641
Esta publicación científica en formato digital
es continuidad de la revista impresa
Depósito Legal: pp 200602ZU2811 / ISSN:1856-5042
ISSN Electrónico: 2542-3207

UNIVERSIDAD DEL ZULIA
Serbiluz
Sistema de Servicios Bibliotecarios y de Información
Biblioteca Digital
Repositorio Académico

Impacto Científico
Revista Arbitrada Venezolana
del Núcleo LUZ-Costa Oriental del Lago
Vol. 18. N°1. Junio 2023. pp. 65-80

Herramientas del hacking ético como recurso para la detección de vulnerabilidades en los sistemas de información

Luisa Serra
Universidad del Zulia. Núcleo Costa Oriental del Lago. Venezuela
https://orcid.org/0000-0002-7561-2541
serra_sl@yahoo.com

Carlos Figueroa
Universidad del Zulia. Núcleo Costa Oriental del Lago. Venezuela
https://orcid.org/0000-0002-4013-6311
clfigueroa6822@gmail.com

Romer Sánchez
Universidad del Zulia. Núcleo Costa Oriental del Lago. Venezuela
https://orcid.org/0000-0002-2926-8399
sanchezromer3@gmail.com

Edglimar Marín
Universidad del Zulia. Núcleo Costa Oriental del Lago. Venezuela
https://orcid.org/0000-0003-1650-6383
edglimarmarin@gmail.com

Adriángel Gutiérrez
Universidad del Zulia. Núcleo Costa Oriental del Lago. Venezuela
https://orcid.org/0009-0001-1554-2318
adriangelgutierrez@gmail.com

Resumen

El objetivo de la presente investigación es determinar el nivel de aplicación del hackeo ético dentro de las empresas de la Ciudad de Cabimas del Estado Zulia. A fin de proveer el sustento teórico necesario, se utilizaron los postulados de Astudillo (2013), Benchimol (2011), Rault y otros (2015). El presente estudio se clasificó como descriptivo, con diseño no experimental-transversal. La población estuvo conformada por 22 gerentes de informática, sistemas y administradores de red de empresas de la

RECIBIDO: 16/03/2023 · ACEPTADO: 27/03/2023

localidad. Se utilizó la totalidad de sujetos como muestra. La técnica utilizada para la recolección de datos fue la encuesta mediante cuestionario cerrado con escala tipo Likert de 5 alternativas de respuesta, el cual fue sometido a validez de contenido por juicio de expertos. La confiabilidad se calculó con el coeficiente Alfa de Cronbach, obteniéndose un valor de 0.935, considerándose altamente confiable. Para el análisis de los datos se utilizó la estadística descriptiva. Se obtuvo una alta presencia en el uso de las herramientas de hacking ético como barredores de ping, escáneres de puertos, analizadores de vulnerabilidades y distribuciones Linux (Kali). Se concluyó que las organizaciones deben promover el uso de estas herramientas para proteger sus activos de información, redes y sistemas, dada la existencia de los llamados cibercriminales. Igualmente, se debe crear conciencia en el ciudadano común para resguardar información sensible sobre los servicios que utilizan.

Palabras Clave: Hacking ético, vulnerabilidades, sistemas de información

Ethical hacking tools as a resource for the detection of vulnerabilities in information systems

Abstract

The objective of this research is to determine the level of application of ethical hacking within companies in the City of Cabimas in Zulia State. In order to provide the necessary theoretical support, the postulates of Astudillo (2013), Benchimol (2011), Rault and others (2015) were used. The present study was classified as descriptive, with a non-experimental-transversal design. The population consisted of 22 IT managers, systems and network administrators from local companies. All subjects were used as a sample. The technique used for data collection was the survey through a closed questionnaire with a Likert-type scale of 5 response alternatives, which was subjected to content validity by expert judgment. Reliability was calculated with Cronbach's Alpha coefficient, obtaining a value of 0.935, considered highly reliable. Descriptive statistics were used for data analysis. A high presence was obtained in the use of ethical hacking tools such as ping sweepers, port scanners, vulnerability analyzers and Linux distributions (Kali). It was concluded that organizations should promote the use of these tools to protect their information assets, networks and systems, given the existence of so-called cybercriminals. Likewise, awareness must be created in the common citizen to safeguard sensitive information about the services they use.

Keywords: Ethical hacking, vulnerabilities, information systems

Introducción

Una de las tareas de los administradores de sistemas dentro de las organizaciones contemporáneas, es mantener seguros los activos de información. En ese sentido, deben procurar el monitoreo continuo de las vulnerabilidades que pudiesen existir en los sistemas de información a efectos de evitar la penetración indebida hacia la información de la empresa por parte de personas o entes no autorizados, intrusiones, ataques y otras acciones que puedan derivar en eventos inesperados o adversos, produciendo pérdidas significativas de información y otros recursos.

Por lo anteriormente expuesto, las organizaciones recurren a la contratación de personal de prueba o testers para que realicen las validaciones pertinentes en los sistemas de información en virtud de corroborar el cumplimiento de sus requerimientos o necesidades y al mismo tiempo, verificar los elementos de seguridad para evitar el acceso indebido de entes no autorizados, considerando elementos físicos y lógicos tales como puertos utilizados por los aplicativos de software, servicios activos en las redes, actualizaciones de los sistemas operativos, motores de bases de datos, complementos de los sistemas de información, entre otros.

A la luz de las ideas planteadas y considerando las actividades relacionadas con la detección de debilidades en los sistemas informáticos, es pertinente mencionar la existencia de profesionales de la informática, electrónica y disciplinas relacionadas, dedicados al descubrimiento de vulnerabilidades en dichos sistemas. Esto ha permitido el surgimiento del hackeo ético (ethical hacking), el cual es definido por Benchimol (2011) como un conjunto de actividades ejecutadas por profesionales con gran dominio del conocimiento de las ciencias de la computación cuyo propósito es la investigación, desarrollo de aplicaciones, experimentación con sistemas de información y estudio de la seguridad de los mismos para detectar debilidades e informarlas a los administradores para aplicar los correctivos y así, fortalecerlos.

En ese sentido, de acuerdo a Astudillo (2013) el hackeo ético tiene fines defensivos; es decir, la función del hacker será determinar lo que un intruso puede realizar sobre determinado sistema, velando por su protección. Por ende, debe poseer conocimientos profundos sobre hardware, electrónica, redes, telecomunicaciones y programación en lenguajes de alto, medio y bajo nivel. Cabe mencionar que Benchimol (2011) establece la utilización errónea del término en el cine y la televisión, dándole una connotación negativa cuando realmente, se hace referencia al cracker, es decir, alguien que viola la seguridad de un sistema ilegalmente con fines de lucro o beneficio personal. También se aplica al software, denotando personas que utilizan la ingeniería inversa con el objetivo de desprotegerlo o alterar su comportamiento.

Como complemento a lo anterior, existen empresas y organizaciones que han sido objeto de espionaje industrial, sabotaje o acciones similares por parte de personas inescrupulosas. De acuerdo a López (2014) en su artículo publicado en el diario elfinanciero.com.mx, la empresa de subastas en línea Ebay sufrió un ataque en Mayo

de 2014, donde un conjunto de ciberdelincuentes accedieron a información sensible de 145 millones de usuarios, lo cual dejó en evidencia la existencia de agujeros de seguridad. Igualmente, Sony confirmó ser víctima de crackers, que lograron sustraer información confidencial de más de 47 mil empleados entre los que se encontraban actores y directores.

En el ámbito de Venezuela, el diario El estímulo, (2017), publicó un artículo referido a un supuesto hackeo sufrido por Consejo Nacional Electoral (CNE) por parte de un grupo identificado como The binary guardians, quienes vulneraron la seguridad de las bases de datos y accedieron a información sensible de los votantes. Posteriormente, este grupo publicó un tweet indicando la acción que habían realizado y el ente electoral aplicó los procedimientos necesarios para reestablecer los servicios a través del apoyo recibido por los cuerpos de seguridad del Estado.

Sobre la base de las ideas expuestas anteriormente y ante la existencia de personas que utilizan el conocimiento en las ciencias de la computación e informática con fines tanto ofensivos como defensivos, surge la necesidad de estudiar la aplicación del hacking ético dentro de las organizaciones existentes en el Estado Zulia, específicamente, en la ciudad de Cabimas, ya que esto está relacionado con la praxis de un conjunto de valores con el propósito de fortalecer los sistemas de información, evitando daños por parte de usuarios no autorizados,. Por tales razones, todo profesional de la informática debe estar familiarizado con las actividades inherentes al hacking ético en virtud de poder desempeñarse en esta área, con la pertinencia, moral y responsabilidad que éstas implican.

El presente estudio resulta pertinente desde el punto de vista práctico, ya que evidenciará el nivel de aplicación de las técnicas relacionadas con el hacking ético en un conjunto de organizaciones de la Ciudad de Cabimas del Estado Zulia, brindando las orientaciones necesarias a los administradores de sistemas a fin de tomar acciones en pro del fortalecimiento de los sistemas de información y plataformas de trabajo. En ese sentido, también se establecen diferencias semánticas entre cracker y hacker, enfatizando los valores que debe poseer el profesional dedicado a la protección de los activos de información en los distintos entes tanto públicos como privados. A la luz de lo anterior, esta investigación tuvo como propósito, determinar el nivel de aplicación del hackeo ético dentro de las empresas de la Ciudad de Cabimas del Estado Zulia en el período comprendido entre octubre de 2022 y enero de 2023.

Fundamentación teórica

Hacking ético

De acuerdo al criterio de Astudillo (2013), cuando se habla de hacking ético se hace referencia a la acción de efectuar pruebas de intrusión controladas sobre sistemas informáticos; es decir, el consultor (hacker) actuará desde el punto de vista de un cracker a fin de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas, brindándole acceso al sistema afectado; pero siempre en un ambiente supervisado, donde no existan riesgos de operatividad de los servicios informáticos en la organización.

Como complemento a lo anterior, Benchimol (2011) establece que el hacker ético es un experto en informática, sistemas y redes capaz de utilizar sus conocimientos con fines defensivos. De esta manera, deberá pensar como cualquier intruso, partiendo de las acciones de éstos sobre los sistemas informáticos, velando por su protección y anticipándose a cualquier operación maliciosa perpetrada por ellos.

A la luz de los aportes de Astudillo (2013) y Benchimol (2011), se fija posición frente al hacking ético, definiéndolo como un conjunto de prácticas desarrolladas por profesionales experimentados en el área de la informática, computación, redes y electrónica, capaces de aplicar sus conocimientos con el fin proteger los sistemas informáticos, generando acciones defensivas para evitar cualquier ataque que vaya en perjuicio de los activos de información dentro de las organizaciones.

Herramientas utilizadas en el hacking ético

De acuerdo al criterio de Astudillo (2013), existen diversas herramientas de software que pueden utilizarse en el ejercicio del hacking ético y permiten la detección de vulnerabilidades dentro de los sistemas informáticos. A continuación, se mencionan algunas de ellas:

Ping sweepers o barredores de ping

Según lo expone Astudillo (2013), son un tipo de software que permite identificar los hosts o equipos activos dentro de los rangos de direcciones IP (Internet Protocol o Protocolo de Internet) dentro de una red. Los ping sweepers permiten definir un rango de IP's a probar y usando el protocolo ICMP envían solicitudes de eco (echo request). Luego, los hosts que responden a esta solicitud se marcan como activos.

Ahora bien, Benchimol (2011) indica que el inconveniente con los ping-sweepers cuando se usan en un hacking externo, es el bloqueo predeterminado de la respuesta al ping en los firewalls y routers; de hecho, los administradores de sistemas tienden a desactivarlo como medida de prevención para evitar el mapeo de red por parte de atacantes externos. Así mismo, tanto Rault y otros (2015) como Astudillo (2013), expresan que un barrido de pings hacia todos los hosts de un rango de IP's dado, despierta la atención de los dispositivos de prevención de intrusos (IPS), los cuales podrían detectar que se trata de un escaneo y tomar medidas como enviar instrucciones al firewall para que bloquee la IP de origen.

Desde el punto de vista de los autores del presente artículo, los ping sweepers se pueden considerar como herramientas de primer nivel en el hacking ético; ya que permiten detectar los hosts activos en una red; es decir, se puede determinar fácilmente la existencia de intrusos siempre y cuando respondan a la solicitud de eco; lo cual a su vez, representa su principal desventaja. En ese propósito, es necesario personalizar las opciones necesarias para evitar ser detectados por los IPS; aun cuando se deba invertir mayor tiempo en el escaneo. Adicionalmente, si el protocolo ICMP se encuentra bloqueado, una opción es aplicar un aplicativo de TCP-Ping; es decir realizar el ping mediante el protocolo de control de transmisión. Algunos barredores de ping conocidos son el Ping Scanner Pro y el IP Scanner.

Escáneres de puertos

De acuerdo a lo expresado por Astudillo (2013), los escáneres de puertos son un tipo de software capaz de identificar a los hosts activos y al mismo tiempo, determinan los puertos y servicios que se encuentran en estado de escucha o (listening) para atender requerimientos de los equipos de la red. No obstante, la línea entre los barredores de ping y estas herramientas se vuelve cada vez más difusa ya que en la actualidad, existen aplicativos que realizan más de una función desde una sola interfaz. Además, se aplican como prerrequisito para continuar con la detección de vulnerabilidades.

Por su parte, Benchimol (2011) destaca la existencia del Nmap el cual, es una herramienta de código abierto que permite detectar y controlar los puertos abiertos, establecer horarios de uso de servicios de red, control de los host, actividad en la red, así como la identificación de configuraciones dentro de los ordenadores (sistema operativo, firewalls, antivirus, software instalado, entre otros), esto con el propósito de identificar puntos vulnerables en el sistema de cómputo que pudiesen ser susceptibles de ataques.

En ese mismo orden y dirección, tanto Astudillo (2013) como Benchimol (2011) coinciden asegurar que con los datos recopilados mediante el barrido de ping y el escaneo de puertos, se inicia la detección de vulnerabilidades. Esto es, dependiendo de los servicios que se estén brindando, tales como acceso a la web, e-mail, transferencia de archivos (FTP), entre otros, en el sistema operativo base del equipo y las aplicaciones, se podrá determinar la existencia de vulnerabilidades conocidas y así poder explotarlas.

Cabe destacar que de acuerdo al criterio de los autores del presente artículo, los escáneres de puertos, están dirigidos a un nivel mayor de profundidad con respecto a los barredores de ping, ya que trabajan en la detección, identificación, monitoreo, habilitación e inhabilitación de puertos y servicios activos o en estado abierto o escucha. Se considera un éxito cuando un hacker puede ejecutar tareas de enumeración para acceder a dominios, equipos, cuentas de usuario o software. En tal sentido, el escaneo se considera como una etapa previa al análisis de vulnerabilidades, siendo esta última, una actividad compleja. A tales efectos, existen en el mercado herramientas como el Nmap, ZenMap, SuperScan, Hyena, entre otros.

Herramientas de enumeración y acceso

De acuerdo con Benchimol (2011), una fase fundamental dentro del hackeo ético es la enumeración de servicios. El objetivo de esta es obtener información relativa a los usuarios, nombres de equipos, recursos y servicios de red. Para esto, se generan conexiones activas con los sistemas y se realizan consultas directas para obtener la información. Al respecto, indica Astudillo (2013) que a diferencia del caso anterior, las consultas siempre se hacen al equipo objetivo y en forma activa, generando listados completos de cuentas de usuario, permisos, roles, entre otros.

Por su parte, Rault y otros (2015) expresan que entre este tipo de aplicativos se pueden mencionar el GetAcct, Dumpusers y DumpSec; algunos, basados en línea de comandos y otros con interfaz gráfica, cuyos propósitos van desde generar listados en pantalla hasta la creación de reportes en formatos separados por coma (.csv), los cuales pueden ser procesados y analizados detalladamente. Cabe mencionar también que los métodos, comandos y procedimientos de acceso varían conforme el sistema operativo. Es evidente que en Windows y Linux existe software disímil; aunque orientado hacia el mismo objetivo.

Analizadores de vulnerabilidades

En cuanto a los analizadores de vulnerabilidades Astudillo (2013) indica que facilitan la labor del auditor de sistemas; permitiendo ejecutar desde una sola interfaz escaneos y enumeraciones sobre el objetivo, a la vez que identifican debilidades presentes en los sistemas y al mismo tiempo, las clasifican de acuerdo a determinado nivel de riesgo. La identificación se realiza de acuerdo a la versión del sistema operativo y de los servicios y aplicaciones detectados comparándolos contra una base de datos de vulnerabilidades que se actualiza frecuentemente conforme nuevos orificios de seguridad son descubiertos.

En ese sentido, tanto Astudillo (2013) como Benchimol (2011) coinciden en la existencia de distintos niveles de seguridad, a saber: Alto, cuando el equipo presenta vulnerabilidades críticas fáciles de explotar y que podrían conllevar a tomar control total del sistema, comprometiendo la seguridad de la información. El nivel medio

cuando el equipo posee debilidades severas que requieren una mayor complejidad para poder ser explotadas y que podrían no brindar el mismo nivel de acceso al sistema afectado. Por último, el nivel bajo, se presenta cuando equipo tiene vulnerabilidades moderadas que podrían brindar información a un atacante, la cual podría utilizarse para realizar ataques posteriores.

A la luz de los planteamientos anteriores, se fija la posición de los autores del presente artículo, indicando que los analizadores de vulnerabilidades son herramientas integrativas que permiten desde la identificación de puertos o servicios en las redes hasta la evaluación de las actualizaciones existentes en los sistemas operativos, firewalls (cortafuegos) o antivirus, generando informes acerca del estado actual de determinado sistema; lo cual permite orientar las acciones protectoras a tomar en virtud de los niveles de vulnerabilidad detectados. En ese propósito, existen diversas alternativas tanto de código abierto como propietarias tales como OpenVas, Nexpose, Nessus y Retina. Todas ellas poseen funcionalidades en cuanto a escaneo de puertos y direcciones IP, interfaz gráfica, generación de reportes, entre otras.

Distribuciones linux para ethical hacking: kali linux

De acuerdo al portal oficial www.kali.org, Kali Linux es una distribución basada en Debian GNU/Linux diseñada especialmente para labores de auditoría y seguridad informática. Su mantenimiento está a cargo de la empresa Offensive Security Ltd. Mati Aharoni y Devon Kearns. Los mismos, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux. Contiene alrededor de 600 programas incluyendo escáneres de puertos, monitores de tráfico, analizadores de paquetes, crackeadores de contraseñas y software para pruebas de seguridad en redes inalámbricas. Ofrece adicionalmente, la ventaja de correr desde un Live CD, live-usb y también puede ser instalada como sistema operativo en el disco duro.

Por su parte, Astudillo (2013) complementa lo anterior expresando que Kali Linux contiene integradas herramientas como escáneres de puertos (Nmap), analizadores de vulnerabilidades (OpenVas, Nexpose), Frameworks para Metasploits (MFS, Armitage), entre otros, pudiendo aplicarse en equipos objetivo con distintos sistemas operativos como Windows y Linux. Adicionalmente, resulta ligero en comparación con otras distribuciones y puede utilizarse sin alterar el contenido del disco duro de la máquina hacker. Igualmente, la referida autora asegura que desde sus inicios como Backtrack (nombre original), ha gozado de aceptación entre los especialistas del área y se encuentra en constante revisión por parte de la empresa desarrolladora.

Como complemento a las ideas expresadas anteriormente, se procede a fijar posición indicando que el Kali Linux es una distribución que ofrece las prestaciones necesarias para desempeñar el hacking ético, ya que integra diversidad de herramientas que permiten desde la identificación de hosts hasta la toma de control por parte de usuarios remotos, bloqueo de servicios, análisis de tráfico, paquetes o vulnerabilidades

y emisión de reportes significativos acerca del estado de seguridad de la red, resultando un compendio de utilidades que todo profesional de seguridad informática debe conocer.

Metodología

El presente, estudio se catalogó como descriptivo, según Hernández *et al* (2010) quienes aseguran que la investigación de este tipo busca especificar propiedades o rasgos de cualquier fenómeno. En otras palabras, en esta investigación se detallan y desarrollan cada una de las características esenciales vinculadas al hacking ético con el propósito de verificar la forma en que se presentan o aplican dentro del contexto estudiado; es decir, las organizaciones de la Ciudad de Cabimas del Estado Zulia.

En el mismo orden de ideas, se cataloga como un estudio de campo, de acuerdo al criterio de Arias (2012) quien lo define como la recolección de datos directamente de la realidad donde ocurren los hechos sin la manipulación de variable alguna. Bajo esta premisa, este estudio corresponde con esta tipología, ya que la información se recopila directamente de la realidad donde se encuentra el objeto de estudio; es decir, las organizaciones de la Ciudad de Cabimas, en otras palabras, se trata de una fuente primaria, sin la presencia de factores o elementos intermediarios.

Como complemento a lo anterior, el diseño del presente estudio, es no experimental – transeccional ya que no se altera o modifica el fenómeno estudiado por parte del investigador. Por tanto, es observado tal como existe en la realidad a través de sus características o propiedades intrínsecas. En tal sentido, Hernández y otros (2010) indican sobre estos diseños que se realizan sin manipular deliberadamente las variables y sólo se observan fenómenos en su ambiente natural para su posterior análisis.

En ese mismo orden de ideas, el estudio corresponde a un diseño transeccional o transversal ya que el instrumento de recolección de datos tuvo una única aplicación en el tiempo. En tal sentido, Hernández y otros (2010), aseguran que en estos casos, se recolectan datos en un único momento; en un tiempo único sin evaluar el comportamiento del fenómeno a lo largo del tiempo.

La población del presente estudio está conformada por 22 personas, a saber, gerentes de informática, sistemas y administradores de red, adscritos a organizaciones públicas y privadas de la ciudad de Cabimas, Estado Zulia, tomando como criterios de inclusión aquellas empresas con manejo de data sensible y cuya actividad económica implique la aplicación de políticas de seguridad para la protección de la información almacenada en sus bases de datos. En ese propósito, se abarcaron instituciones educativas, empresas comerciales, de servicios diversos y entidades bancarias. En tal sentido, se establece un muestreo intencional, sobre el cual, Arias (2012) expone

que los elementos son escogidos con base en criterios o juicios preestablecidos por el investigador.

Con el propósito de recolectar la información, se utilizó un (01) instrumento con el fin de estudiar el comportamiento del hacking ético dentro de las organizaciones seleccionadas. El mismo, quedó estructurado por un total de quince (15) ítems, redactados en forma de proposiciones afirmativas, con escala tipo Likert y 5 alternativas de respuesta: siempre (5), casi siempre (4), algunas veces (3), casi nunca (2) y nunca (1). Se sometió a validez por juicio de cinco (05) expertos, quienes evaluaron la pertinencia de cada uno de los ítems.

Como complemento a lo anterior, se aplicó el criterio de la validez discriminante para lo cual, se realizó una prueba piloto a 10 gerentes con características similares a la población objeto de estudio. En ese sentido, Arias (2012), expone que es una de las pruebas más potentes, que consiste en el análisis de ítems. Es de fácil aplicación en escalas de actitudes tipo Likert. Esta se realizó luego de calcular las medias o promedios de cada ítem utilizando el Software SPSS aplicando la prueba t de Student para muestras independientes. Para la confiabilidad se utilizó el coeficiente Alfa-Cronbach y los datos se procesaron con el programa SPSS 23, El valor resultante fue 0.935, considerado de muy alta confiabilidad, de acuerdo a lo establecido en el baremo de Hernández y otros (2010).

En lo tocante a las técnicas estadísticas utilizadas, se aplicó la estadística descriptiva, enmarcada dentro del método cuantitativo. Como complemento a lo anterior, Hernández y otros (2010), indican la necesidad de usar los fundamentos estadísticos para la tabulación, procesamiento, análisis e interpretación de datos numéricos. Adicionalmente, la información obtenida se procesó utilizando el software SPSS versión 23, lo cual permitió dar respuesta al objetivo de la investigación. En ese propósito, se utilizó el siguiente baremo de interpretación para las medias aritméticas obtenidas:

Cuadro 1. Baremo de interpretación para la media aritmética

Rango	Intervalo	Categoria (nivel de utilización)
5	4.21 - 5.00	Muy alto
4	3.41 - 4.20	Alto
3	2.61 - 3.40	Moderado
2	1.81 - 2.60	Bajo
1	1.00 - 1.80	Muy bajo

Fuente: Elaboración propia (2023)

Análisis, interpretación y discusión de los resultados

A continuación se presenta la tabla de frecuencias relativas expresadas en porcentajes, correspondientes a las herramientas del hacking ético, utilizadas como recurso para la detección de vulnerabilidades en los sistemas de información. En cada caso, se destaca el valor de la respuesta obtenida así como las medias aritméticas asociadas a las mismas. Esto sirvió como base en virtud de proveer una interpretación adecuada, considerando el baremo preestablecido.

Cuadro 2. Resultados obtenidos con la aplicación del instrumento

Categorías	Barredora de ping			Escáneres de puertos			Herramientas de enumeración y acceso			Analizadores de vulnerabilidad			Distribuciones Linux		
Ítems	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Frecuencias	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Siempre	49	38	48	39	60	43	39	40	57	48	60	25	34	30	40
Casi siempre	35	48	43	44	40	47	40	36	33	43	40	44	46	39	41
A veces	13	13	10	17	0	10	20	24	9	10	0	26	17	29	17
Casi nunca	2	0	0	0	0	0	0	0	0	0	0	5	2	2	2
Nunca	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Media	4,14	4,14	4,27	4,09	4,55	4,23	4,05	4,00	4,36	4,27	4,55	3,68	3,95	3,77	4,00
Nivel de utilización	Alto	Alto	Muy alto	Alto	Muy alto	Muy alto	Alto	Alto	Muy alta	Alto	Muy alto	Alto	Alto	Alto	Alto

Fuente: Resultas obtenidos a partir del procesamiento estadístico (2023)

En primer lugar, los barredores de ping mostraron un alto nivel de utilización dentro de la población seleccionada, con una media de 4.14; lo cual se ratifica con los valores porcentuales obtenidos en las distintas categorías de respuesta. Las mismas evidencian una mayor concentración de valores en las opciones siempre y casi siempre con un 49% y 35% respectivamente. Esto sugiere que los administradores de red los utilizan con el propósito de identificar los hosts activos dentro de un rango de direcciones IP siendo esta acción de carácter primario para luego, poder acceder al equipo seleccionado como objetivo.

Igualmente, puede inferirse que el uso de los barredores de ping resulta una técnica de primer nivel por los practicantes del hacking ético debido a la posibilidad de reconocer equipos conocidos o no dentro de un rango de direcciones IP. Lo anteriormente expuesto, coincide con lo expresado previamente por Astudillo (2013), quien establece que con la identificación de los equipos de la red mediante su dirección IP, es decir, en capa de red del modelo OSI, se podrá acceder a ellos con distintas

finalidades, tales como habilitación de servicios, tomar el control del mismo, entre otros.

Por otra parte, se procedió a analizar el uso de los escáneres de puertos por parte de población objeto de estudio, encontrándose en niveles muy altos de aplicación. Esto se refleja en las medias obtenidas en los rangos de 4,09 a 4,55 y se ratifica con los valores porcentuales, denotándose valores entre el 40 y 60% con tendencia a mantenerse, lo cual implica que los sujetos encuestados utilizan herramientas como el Nmap para identificar servicios a partir de puertos conocidos (abiertos) y al mismo tiempo, aplicar políticas de protección como la reasignación de los mismos a rangos poco utilizados o recurrir al bloqueo o redireccionamiento. De esta manera, será más difícil para los delincuentes informáticos, penetrar dentro de las redes de las organizaciones.

Lo anteriormente expuesto coincide con los postulados de Benchimol (2011) quien indica que estas herramientas, permiten controlar la utilización de puertos asociados a servicios en la red, identificando aquellos en estado abierto o escucha e incluso, establecer horarios para el acceso a recursos dentro de la red. Además, recomienda las técnicas como el redireccionamiento o bloqueo de puertos para evitar la penetración de intrusos, protegiendo así los sistemas informáticos.

En otro orden de ideas, al estudiar las herramientas de enumeración y control de acceso, se pudo apreciar un alto nivel de utilización por parte de los sujetos encuestados, representado por una media que oscila entre 4.00 y 4.36 de acuerdo al baremo de interpretación. Así mismo, los porcentajes evidencian una alta concentración de frecuencias en las categorías superiores (casi siempre y siempre) sobre lo cual se infiere que el personal de tecnologías de la información (TI) utiliza software especializado para enumerar elementos de un dominio, por ejemplo: usuarios, equipos, grupos, recursos compartidos, entre otros con el propósito de determinar las posibilidades de acceso a ellos desde ubicaciones externas para aplicar medidas de protección que eviten la intromisión de personas no autorizadas.

Sobre la base de las consideraciones anteriores, se puede afirmar la existencia de aspectos coincidentes con respecto a las teorías expuestas por Astudillo (2013) el cual asegura que una vez identificado un host objetivo, es necesario recurrir a software especializado en la enumeración de servicios o recursos dentro de él o la red, esto con el fin de aplicar estrategias defensivas en virtud de evitar el acceso indebido por parte de personas no autorizadas. En tal sentido, mientras los crackers buscan listar dominios, usuarios, grupos, equipos o servicios abiertos para penetrar en ellos, el hacker ético se centra en la elaboración de reportes de vulnerabilidades detectadas a fin de ser entregados a los administradores de red en aras de aplicar acciones vinculadas con la protección de activos de información en las organizaciones.

Ahora bien, al estudiar el comportamiento de los analizadores de vulnerabilidades, existe un alto nivel de utilización por parte de la población objetivo. Esto se afirma a partir de las medias obtenidas que oscilan entre un 3.68 y 4.55. Adicionalmente, las frecuencias porcentuales evidencian una tendencia a utilizar estas herramientas

para generar reportes relacionados con servicios activos de red considerados como sensibles a ataques o agujeros de seguridad, tales como puertos abiertos, inyección SQL, ausencia de firewalls o falta de actualizaciones críticas de software entre otras.

En ese propósito, se infiere que los administradores de red y personal de tecnologías de la información (TI) encargado de la seguridad informática, recurre a ellas a fin de identificar puntos débiles que pudiesen ser aprovechados por los crackers para atacar la red o los sistemas de la empresa. Una vez hecho esto, se procede a levantar o revisar las políticas de seguridad y protección de los sistemas informáticos, elevando los informes resultantes a los niveles estratégicos.

Como complemento a las ideas anteriores, se encuentran aproximaciones con las teorías presentadas por Astudillo (2013) quien establece que los analizadores de vulnerabilidades son herramientas de segundo o tercer nivel que aplican la heurística o estrategias similares con el fin de identificar debilidades o brechas de seguridad en los sistemas. Igualmente, pueden estar dotados de características expertas para brindar orientaciones o sugerencias para corregir estos problemas.

Por último, al observar el uso de la distribución Kali Linux para el hacking ético, se pudo constatar un nivel alto de aplicación por parte de la población encuestada de acuerdo al baremo de interpretación. En tal sentido, los especialistas en seguridad informática, administradores de red y personal de TI muestran tendencia a utilizar este sistema operativo, ya que agrupa un conjunto de herramientas focalizadas hacia el monitoreo de puertos y tráfico de red, detección de vulnerabilidades, crackeador de contraseñas, enumeradores de servicios entre otras. De acuerdo al sitio oficial www.kali.org, posee más de 600 aplicativos que pueden ser utilizados dependiendo de las labores a realizar, incluso en modo “live”, es decir, sin la necesidad de instalar programas en el disco duro.

Sobre la base de los planteamientos anteriores y en concordancia con lo planteado por Astudillo (2013), el Kali Linux es una distribución muy utilizada en la actualidad, dada la versatilidad que ofrece ya que contiene herramientas robustas como Nmap, Wireshark, Metasploit e incluso software de índole forense. El mismo sigue estándares de código abierto, estando continuamente en revisión y actualización. Igualmente, es importante destacar que está disponible para distintas arquitecturas de 32 y 64 bits, pudiendo además compilar kernels personalizados al punto de integrar paquetes adicionales de acuerdo a las necesidades de los usuarios.

A la luz de las ideas anteriormente expuestas y desde el punto de vista de los autores del presente artículo, Kali Linux representa un conglomerado de utilidades destinadas tanto a tareas sencillas de enumeración o visualización de servicios como otras más complejas derivadas de la implementación de políticas de protección, a saber, monitoreo de tráfico inusual en la red, inhabilitación, habilitación o redireccionamiento de puertos, desencriptación de contraseñas, detectar vulnerabilidades, emitir reportes relacionados con la seguridad, entre otras. Adicionalmente, el respaldo con el que cuenta por parte de la empresa desarrolladora Offensive Security, LTD, así como su

filosofía de código abierto, permiten una curva de aprendizaje ascendente, favoreciendo así su permanencia en el mercado.

Ahora bien, para dar respuesta al objetivo terminal de la presente investigación, se pudo establecer un nivel de aplicación del hacking ético de alto a muy alto dentro de los especialistas de seguridad informática que cumplen funciones dentro del contexto estudiado, tal como se ha visto en los resultados presentados. Sobre lo anterior, se puede inferir que tanto los profesionales como las organizaciones contemporáneas poco a poco han tomado conciencia sobre la importancia de preservar los activos de información.

Así mismo, el establecimiento de políticas de seguridad, la aplicación de herramientas para la protección de los sistemas, de información y redes corporativas cobra relevancia debido a la telepresencia, auge de los servicios en la nuble y la globalización. Por ende, se debe seguir promoviendo la utilización del hacking ético en virtud de prevenir, detectar o contrarrestar, acciones indebidas por parte de personas inescrupulosas que utilizan el conocimiento para su beneficio personal o causar daños a terceros, sean personas naturales o jurídicas.

Conclusiones

En primer lugar, se pudieron puntualizar algunas herramientas relacionadas con el hacking ético entre las cuales se pueden mencionar los barredores de ping, escáneres de puertos, software de enumeración y acceso, analizadores de vulnerabilidades y el Kali Linux, encontrándose una alta utilización por parte del personal de tecnologías de la información dentro del contexto estudiado. Esto se traduce en un uso defensivo de este software en función de proteger los activos de información, mediante la implementación de políticas inherentes a la seguridad informática. En tal sentido, se infiere que tanto los niveles estratégicos como tácticos de las organizaciones encuestadas, han tomado conciencia de la existencia de los cibercriminales y por ende, han adoptado medidas defensivas en múltiples niveles.

Por consiguiente, a partir de los resultados obtenidos, se pudo apreciar la aplicación del hacking ético partiendo de herramientas básicas o de primer nivel para identificar hosts dentro de la red para luego realizar un reconocimiento de los puertos abiertos, los cuales están asociados a servicios y en ese sentido, aplicar estrategias como la reasignación o redireccionamiento de los mismos; es decir, en lugar de utilizar puertos conocidos, se sugiere utilizar rangos personalizados para evitar ataques a través de ellos, ya que resulta más difícil para los crackers identificar servicios o vulnerabilidades cuando se utilizan puertos no convencionales.

En ese mismo orden y dirección, se evidenció el uso de herramientas de enumeración y acceso a recursos o servicios de la red. Esto indica que una vez identificados los host

objetivo, se utiliza software para obtener listados o reportes acerca de los procesos o servicios existentes que puedan ser violentados por los crackers, brindando ayuda al personal de TI a fin de determinar posibles agujeros o debilidades de seguridad. Es allí donde entran en juego los analizadores de vulnerabilidades, cuyo fin es establecer elementos inseguros que puedan dar lugar a ataques.

Es allí donde los administradores de red o especialistas en seguridad informática deben aplicar políticas que permitan tanto prevenir como detectar ataques internos o externos implementando estrategias o técnicas en aras de preservar la integridad de los sistemas. En tal sentido, se recomienda el monitoreo continuo de los servicios habilitados dentro de la red, puertos, equipos, usuarios y demás elementos importantes. Igualmente, es menester mantener actualizados los manuales de configuración de los equipos de seguridad, realizar auditorías informáticas, respaldos periódicos con el respectivo resguardo tanto físico como digital. Adicionalmente, los antivirus, firewalls y sistemas de detección de intrusos, ayudarán a prever cualquier acción indebida por parte de usuarios inescrupulosos, por lo cual, se recomienda ampliamente su utilización.

A la luz de las conclusiones anteriores, el personal vinculado a los departamentos de tecnologías de información, deben preocuparse por conocer a profundidad, las distribuciones como Kali Linux y otras herramientas para el hacking ético, tales como encriptadores (TrueCrypt, OpenSSH, OpenSSL), herramientas para el hackeo Wireless (KisMAC, Aircrack) o analizadores de vulnerabilidades (Wireshark, Ettercap), entre otros, ya que se debe comprender las distintas formas de ataque por parte de los crackers. Así se podrán anticipar acciones preventivas, al asumir el esquema de pensamiento de un cibercriminal; pero también del hacker ético.

Por último, se hace énfasis en la concienciación del ciudadano común acerca de la existencia de los crackers y criminales informáticos ya que hoy en día, las personas manejan información sensible como cuentas de usuario y contraseñas bancarias redes sociales, y tarjetas de crédito entre otros servicios con el propósito de que él mismo se proteja contra ciberdelincuentes que traten de apropiarse indebidamente de cualquier información valiosa para producir daño, obtener lucro o acciones similares.

Igualmente, se debe cambiar el concepto tradicional (mal entendido) del hacker como alguien que busca ocasionar daño y sustituirlo por cracker, esto para dignificar a los expertos informáticos que cumplen actividades defensivas o de protección, aplicando el conocimiento para el bien de las empresas, organizaciones y las personas en general.

Referencias bibliográficas

Arias, Fidias. (2012). El proyecto de Investigación. Introducción a la metodología científica. (6ta. Edición). Editorial Episteme. Caracas, República Bolivariana de Venezuela. Pp. 143.

Astudillo, Karina (2013). Hacking ético 101. Cómo hackear profesionalmente en 21 días o menos.(s/e).

Benchimol, Daniel (2011). Hacking desde cero. (1ª Edición). Editorial Fox Andina. Buenos Aires, Argentina.

Diario El estímulo (2017). Denuncian supuesto hackeo de página de organismo electoral de Colombia desde Venezuela. Artículo en línea. Consultado el 12/05/2018. Disponible en: http://elestimulo.com/blog/colombia-asegura-que-pretendian-hackear-pagina-de-la-registraduria-desde-venezuela/Denuncian supuesto hackeo de página de organismo electoral de Colombia desde Venezuela

Hernández, Roberto; Fernández, Carlos; y Baptista, Pilar. (2010). Metodología de la Investigación. Editorial Mc. Graw Hill. México.

Hurtado Jaqueline. (2010). Metodología de la investigación Holística. Fundación Sypal. Caracas Venezuela.

Kali Linux. (2018). Sitio Oficial. Disponible en: https://www.kali.org/

López, Jair (2018). 5 hackeos que sacudieron al mundo. Artículo en línea Recuperado de: http://www.elfinanciero.com.mx/tech/hackeos-que-sacudieron-a-empresas-en-2014

Rault Raphael,Schalkwijk Laurent, Acissi, Agé Marion, Crocfer Nicolas, Crocfer Robert, Dumas David, Ebel Frank, Fortunato Guillaume, Hennecart Jérôme, Lasson Sébastien (2015). Seguridad informática. Hacking ético. Conocer el ataque para una mejor defensa (3a. Edición). Ediciones ENI. Barcelona, España.