UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO DE SISTEMAS

CARRERA:
INGENIERÍA DE SISTEMAS

TEMA:
"SOFTWARES DE PENETRACIÓN UTILIZADOS POR LOS PIRATAS INFORMÁTICOS: UNA REVISIÓN SISTEMÁTICA (2015-2020)"

AUTOR:
Est. PÉREZ GONZÁLEZ RAÚL FRANCISCO

TUTOR:
Msg. Joe Frand Llerena Izquierdo

Abril 2021
GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **PÉREZ GONZÁLEZ RAÚL FRANCISCO**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Nombre: Raúl Francisco Pérez González
CI. 0941408494

Nombre: Joe Llerena Izquierdo
CI. 0914884879

SOFTWARES DE PENETRACIÓN UTILIZADOS POR LOS PIRATAS INFORMÁTICOS: UNA REVISIÓN SISTEMÁTICA (2015-2020)

Raúl Pérez González [1[0000-0003-2218-2389]] y Joe Llerena Izquierdo [1[0000-0001-9907-7048]]
[1]Universidad Politécnica Salesiana, Guayaquil, Ecuador
rperezg1@est.ups.edu.ec, jllerena@ups.edu.ec

Resumen. Esta investigación, se basa especialmente en el estudio o análisis científico de los softwares que son más empleados por los piratas informáticos, estos softwares **es**tán cada día evolucionando su comportamiento al momento de realizar un ataque o vulnerar un sistema; Sin embargo, estos programas tienen un alto riesgo al caer en manos equivocadas. Como objetivo principal, la categorización de estos softwares es muy recomendable al instante de instruirse en un sistema tanto indefenso como custodiado de la seguridad informática. El método analítico se utilizó en la investigación para escoger, dividir y distribuir información hacer a de las acciones de cada programa informático. Los resultados principales que se determinaron narran las estadísticas definitivas de los softwares según sus porcentajes de usabilidad y en qué años fueron participes de acciones malogradas para una industria mediática, diversificando su comportamiento actual con el periodo tiempo establecido entre estos últimos 5 años. Conforme a la conclusión principal, haber tratado o analizado trabajos investigativos, ha sido una excelente manera de estudiar, analizar, organizar y contrastar los planes de cada software de seguridad para un respectivo funcionamiento.

Palabras claves: Hacking Ético, Malware, Seguridad Informática, Vulnerabilidades, Pirata Informático.

Abstract. This research is especially based on the scientific study or analysis of the software most used by hackers. These software are evolving their behavior day by day when carrying out an attack or violating a system; However, these programs have a high risk of falling into the wrong hands. As the main objective, the categorization of these softwares is highly recommended when being instructed in a system that is both defenseless and protected by computer security. The analytical method was used in the research to choose, divide and distribute information about the actions of each computer program. The main results that were determined narrate the definitive statistics of the software according to their usability percentages and in which years they participated in failed actions for a media industry, diversifying their current behavior with the period of time established between these last 5 years. According to the main conclusion, having treated or analyzed research works has been an excellent way to study, analyze, organize and contrast the plans of each security software for a respective operation.

Keywords: Ethical Hacking, Malware, Computer Security, Vulnerabilities, Hacker.

1 Introducción

En primer lugar, dentro de los procesos requeridos para una simple o estricta transmisión de datos, dar a conocer los implementos, técnicas y software para la respectiva penetración de los sistemas alojados en un ambiente vulnerable, siendo estar relacionado con las responsabilidades de un hacker ético. Siendo concurrente a la hora de tomar datos pertenecientes de un individuo dentro de una organización pública o privada. Por otra parte, los softwares de libre comercialización estallan y se dispersan a través de los cibernéticos quienes son parte o actores secundarios de los ataques informáticos en medio de un escenario muy probable de ataques ilegales.

En 1997, el factor clave para Harrison fue muy insuficiente la tecnología de información el cual se podía limitar a los conocimientos de ataques y softwares de esta tecnología, considerando en ese entonces un plan para la toma de decisiones y sobre estudio de empresas pequeñas validando sus fallas de crecimientos, esta táctica estuvo muy vinculado con la tecnología de la información [1].

En los años de 1971, con la creación de un programa que tendría la eficiencia y eficacia para replicarse decenas o cientos de veces se fueron formando las terminologías en softwares encontrando como resultado las apariciones de los riesgos informáticos, se podría comprobar ante la seguridad informática las posibilidades de casos de usabilidad en cualquier tipo de sistema tecnológico [2]. La implementación y observación de estos programas que vinieron evolucionando por individuos desarrolladores, fueron encontrando vulnerabilidades para lo que hoy se da al previsto de los fallos de identidades con la comunicación. Siendo así un aliado para los individuos informáticos conocer estos conceptos y técnicas procedentes hacia sistemas internos de organizaciones tanto públicas como privadas. Mejorando la seguridad poco a poco hubo procesos para la defensa de infiltrados dentro de un sistema, en donde la escalabilidad fue en aumento ascendente, acentuando así su capacidad de recibir, controlar y discutir errores cuantitativos y cualitativos de arquitecturas creadas en una trayectoria bidireccional de ataques [3].

Cabe añadir las categorías de cómo están relacionados los softwares de los piratas informáticos, por medio de un estudio generalizado el cual se puede categorizar cada software que vulneran los sistemas de manera sigilosa priorizando ciertas fallas de la seguridad informática, manejada por los personales internos quienes justifican la decencia de absorber el código dañino para fortalecer sus necesidades y el ataque de los datos pueda ser juzgado por el administrador de red junto al plantel colectivo de ciberseguridad [4].

Los softwares de los piratas informáticos están categorizados comenzando con el lado de la conectividad inalámbrica (WIRELESS), evaluando el tráfico de las redes como también penetradores de sistemas, intervención de firewalls y sobre todo cabe recalcar como reportar agujeros (BUG), creados en dispositivos o sistemas designados para el usuario final [5].

2 Metodología

Esta investigación fue analizada, estudiada y correlacionada con los tratamientos y asuntos por los investigadores del hacking ético; quienes han podido llevar a cabo hechos en sus resultados. Con la ayuda del método analítico se ha podido desmembrar fragmentos de información relacionada, lo cual se la presentan de la siguiente manera:

2.1 Programas de hackers mediante estudios científicos

Al buscar una perspectiva de como se ha ido evolucionando los programas de piratería, se puede notar una diferencia entre el HACKTIVISMO y el pirata informático que indican ser parte de los estados del desempeño hacia una tecnología revolucionara. La ciberseguridad o seguridad informática es una clave para de aprendizaje en un medio donde se pueda realizar cambios tecnológicos y conocerlos de una manera global, por lo que educar esta profesión lleva de la mano mucho riesgo para el personal o individuo a conocer los softwares de piratería. De igual importancia es prescindible evaluar las herramientas necesarias a utilizar para el usuario final como la lógica o el pensar, si se presentaría un medio con muchas vulnerabilidades. Estos programas informáticos son de mucha cautela, ya que podrían penetrar un escenario con finalidades políticas, financieras, educativa, entre otros [6].

El poder que tienen estas herramientas va mucho más allá de la transformación social de una escala mundial en el territorio escogido. Penetrar un sistema y dejar un MALWARE, es un riesgo tanto para el sistema en general como la seguridad e integridad de una entidad y de una o muchas personas, sabiendo que este malware puede reproducirse e incrustarse en sistemas externos vinculados al entorno declarado, como lo puede ser un AIX que vendría ser el sistema operativo de IBM [7].

2.2 Métodos de Contraataque

Los métodos más utilizados por piratas informáticos se deben a sus propias necesidades a elegir, permitiendo generar actividades de gran importancia en su entorno, estos métodos que utilizan los hackers comúnmente en el último sexenio son los siguientes:

Lanzamiento de Malware.

Los lanzamientos de malware fueron unos de los primeros métodos e inevitables por los piratas informáticos, para comenzar a realizar acciones en manipular, robar y sobre todo averiguar en otros sistemas internos de un mismo centro de operatividad. Por lo tanto, la reproducción de un malware podría llevar consecuencias graves en una entidad tanto pública como privada, este método está en lo más alto de la cima en una escala de alta peligrosidad.

Hombre en el medio (Man in The Middle).

El ataque intermediario u hombre en el medio, se ha convertido en uno de los favoritos para los jóvenes cibernéticos, porque ven opciones de vulnerabilidades entre ambos usuarios entre sí, por lo que este método el atacante interceptara mensaje e

informaciones para el poder manipular al gusto e incrementar las posibilidades de fallo en el sistema con solo tener esa posibilidad de contar con el usuario final y el sistema [7], [8].

Ingeniería social (Social Engineering).

Es uno de los métodos con mucho interés de engañar al rival, pero no están eficiente al momento de poner en prueba el subconsciente del individuo, aún por eso no es menos peligroso que los demás métodos, ya que puede en fracciones de segundos obtener información valiosa, atacar con los RANSOMWARE y es por esta simple metodología que se sigue utilizando en muchos ámbitos.

Fuerza bruta (Brute Force).

Este procedimiento, es antigua en sus derivadas experiencias de tener el poder de descifrar contraseñas o más bien un nombre de usuario, para ir aplicando pruebas de los mismos errores de las localidades donde se encuentra el usuario y contraseña. Con la ayuda de diccionarios se puede complementar este método para tener buenos resultados como estrategia de pon de un modo periódico [9].

Criptografía (Cryptography).

Un pirata informático también protege su identidad en cierta forma que, al atacar escuda su información con este método de encriptar datos e informaciones, para poder llevar una acción de asalto de informaciones. Estos criptógrafos tienen la facilidad de afianzar sus aplicaciones, softwares o herramientas de penetración sobre todo los datos e informaciones con claves simétricas o asimétricas que perdurarán según el pasar del tiempo [10].

Auditoria web (Web Audit).

Las auditorias webs, son eficientes o más bien decir un paso hacia las puertas de la víctima, porque con ello habrá que darse cuenta de que se pueden analizar o distinguir las posibles fallas en el sitio web deseado, una forma en que los hackers recomienda de este método es realizar auditorías web después de haber penetrado un sistema, para poder realizar un planeamiento de las posibles fallas y debilitar el sistema.

Inyección de SQL (SQL injection).

Los hackers han realizado una denotación acerca de este método, por la ofensividad en sobrescribir códigos o sentencias de bases de datos claramente maliciosas, para la respectiva vulnerabilidad de aplicaciones webs realizadas por usuarios desarrolladores, cabe reconocer que una aplicación web recibe datos de los respectivos clientes autorizados para trabajar sobre él. Al inyectar SQL prácticamente se estaría utilizando o en el peor de los casos alterando códigos de bases de datos maliciosas para la extracción de información de dicho aplicativo web.

Secuestro (Hijacking).

Una de las técnicas reconocidas por los hackers en el lado de la ley, es aplicar seguridad al momento exacto de un posible ataque, que a su vez nos indica el secuestro de

información valiosa por parte del hacker. Secuestradores de datos e información, están siempre pendiente de dejar su MALWARE en un lugar o espacio de la víctima, manipulando los DNS y redireccionar a otras páginas por medio de publicidades en común.

Table 1. Métodos para Atacar y Estudiar Sistemas Vulnerables.

Método	Autenticidad y Seguridad	Nivel de Efectividad
Launch de Malware	**si**	**Bajo**
Man in the Middle	**no**	**Bajo**
Social Engineering	**no**	**Medio**
Brute Force	**no**	**Medio**
Cryptography	**si**	**Medio**
Web Audit	**si**	**Alto**
SQL injection	**si**	**Alto**
Hijacking	**si**	**Alto**

2.3 Categorizando las Herramientas o Softwares más utilizados según el periodo de tiempo 2015-2020

De acuerdo con el análisis de estudio, existen una gran cantidad de listados de softwares utilizados por los hackers, por este motivo categorizar las herramientas o softwares más relevantes de estos últimos 5 años es una eficiencia para tener en cuenta el grado de efectividad. Estos softwares los podemos categorizar de la siguiente manera:

Según los Sistemas Operativos.

Las herramientas más comunes utilizadas en este lapso se han venido equiparando con el conocimiento de los sistemas operativos libre comercio, por lo cual las distribuciones necesarias para un pirata informático son tan conocidas por la familia GNU/Linux permitiendo una gran serie de actividades de forma libre y sin ningún obstáculo de licencias, son de gran ayuda en la rama de la ciber seguridad, permitiendo la manipulación, creación, la escritura/lectura, manejo de diccionarios de claves, cifrados, ataques de vulnerabilidades, entre otras. Fueron creadas con el objetivo de brindar seguridad en ciertas partes de la tecnología moderna. Estas distribuciones son las siguientes: **Backtrack, Kali Linux, Pentoo, Helix** [11].

Según la Piratería Inalámbrica.

En esta categoría los piratas informáticos son inducidos a vulnerar diferentes anomalías de conectividad en un medio donde están enlazados los dispositivos o usuarios en la red. Desencriptar una clave de wifi es una de las decenas de ejemplos que puede llevar a cabo en el proceso de ataque inalámbrico, olfatear y verificar los detalles de cada cibernauta, por esta razón los hackers van navegando o infiltrándose en el acceso más deseado y priorizado que son los routers o cuartos de racks. Estos softwares apenas son: **NetCat, Beini, Aircrack-ng, Cain y Abel** [12]**.**

Según el Barrido o la Exploración de Puertos.

En esta categoría la detección de puertos para un pirata informático es muy importante porque cuidar de sí mismo en medio de un ataque, puede optimizar, verificar que puertos se encuentran hábiles para su seguridad y así mantenerlo al margen por cualquier alerta de posibles ataques, producidos por victimas en defensas. Estos softwares que ayudan a los hackers son: **Nmap, Zenmap, Angry ip Scanner** [13]**.**

Según el Manejo de Cifrado.

El manejo de softwares que cifran datos o informaciones es una ventaja que tiene todo personal informático para resguardar o escudar su información mediante la poderosa escritura secreta del cifrado. Un criptoanalista utiliza softwares conocidos para encriptar y desencriptar dicha información enviada al receptor, con el secreto fundamental de otorgarle una llave pública o privada a su receptor. Los softwares que utilizan los criptoanalistas son los que se mencionaran a continuación: **AES Crypt, DiskCryptor, TrueCrypt, Stunnel** [7]**.**

Según la Detección de Intrusos.

La gran mayoría de los hackers se protegen de las cibernautas o hackers éticos, quienes son los principales actores en realizar ataques de denegación de servicios utilizando herramientas para detección de intrusos, es una forma de satisfacer la seguridad de ambos actores al momento de un ataque de intrusión que comprometa la integridad, confiablidad y la disponibilidad de una técnica en ejecución. Estos programas comunes se los reconoce a continuación: **Snort, Homedale, Wifi Analyzer, Netcop.**

Según el Monitoreo y Gestión de Redes.

El recolectar o analizar datos de información a través de transmisión de red, es una prevención y ejecución al riesgo para pirata informático, ya que él se va a encargar de olfatear los dispositivos y ruteadores que emitan o reciban información[14]. Analizar y monitorear el tráfico de red, registra el número de los paquetes a ser vulnerados a través de dispositivos intermediarios. Estas herramientas más usadas son: **Ntopng, Nagios, NetFlow Traffic, Pandora FMS, Dsniff.**

Según los Ataques y Escaneos de Vulnerabilidades.

El atacante informático lo primero que realiza para penetrar sistemas robustos es un análisis minucioso con el sigilo mayor posible de no crear alarmas en el sistema que va a atacar. A esto se deben los ataques ya las recolocaciones de información escaneando puertos necesarios vulnerables y sensibilidades de sistemas externos, también pueden verificar y asegurar los posibles anillos de seguridad que tiene dicho sistema, gestionando y ejecutando las herramientas necesarias o suministradas para el atentado informático. Estas herramientas para el ataque o penetración sistemas y sobre todo el escaneo de vulnerabilidades que utilizan las podemos notar de la siguiente manera: **Metasploit, Social Engineer Toolkit, OpenVas, NetSparker, SQL injection, Zed Attcak Proxy, Beef, SQLmap.**

Según los cortafuegos (FIREWALLS).

Los cortafuegos o más conocidos como firewalls, son capaces de monitorear y controlar el tráfico existente entre el usuario final y cierto escenario escogido por el atacante, Al penetrar un medio, los análisis o estudios que realizan los hackers son el control o el monitoreo de información que se emite o se recepta del escenario o medio que ha penetrado el hacker o pirata informático, dando como resultado el olfateo (SNIFFER) para buscar el omento exacto de agredir o asaltar al medio u organizaciones. Estos softwares que utilizan los hackers son: **NetDefender, Zone Alarm, Comodo Firewall, Glasswire** [7]**.**

Según la Depuración.

Para los hackers la depuración es una de las maneras de combatir todo error sucio al querer atacar a un medio u organización. En la actualidad, depurar el sistema del lado del hacker se vuelve interesante ya que sus softwares depuradores analizan los malwares del mismo hacker, con esto se lleva a cabo una limpieza de los diferentes archivos creados por el atacante. Los depuradores que se pueden presentar dentro del sistema del hacker son: **CCleaner, Glary Utilities, Wise Disk Cleaner, GDB** [15]**.**

Table 2. Softwares de piratería más utilizados y ordenados según su porcentaje de Usabilidad.

Nombre	Categoría	Porcentaje de Usabilidad	Nivel de Efectividad
AES Crypt	Manejo de Cifrado	**96,65%**	**Alto**
Metasploit	Ataques y Escaneo de Vulnerabilidades	**94,50%**	**Alto**
Kali Linux	S. O	**92,89%**	**Alto**
Pentoo	S. O	**87,71%**	**Bajo**
GDB	Depuración	**85,94%**	**Medio**
Beini	Piratería Inalámbrica	**83,39%**	**Bajo**
Beef	Ataques y Escaneo de Vulnerabilidades	**79,45%**	**Medio**

2.4 Contrastando softwares de piratería

Realizando las comparaciones entre los METASPLOIT y la herramienta AIRCRACK-NG, son parecidas al momento de realizar ataque de vulnerabilidades como el phishing que, manipulando sus acciones por medio de las codificaciones, lo que las diferencias una de la otra es que el Metasploit ataca penetrando al sistema y el Aircrack-ng ataca por el lado de la conectividad, es decir la red. El software NETFLOW TRAFFIC y WIFI ANALYZER son programas muy importantes para un pirata informático, porque ambas analizan, rastrean o monitorean información necesaria la defensa o conocimiento del hacker para una penetración o un ataque eficaz, el programa Netflow Traffic lo que permite realizar es una recopilación de tráfico de red estos pueden ser paquetes de datos

para analizar los puntos estadísticos de la víctima de otro modo, el programa Wifi Analyzer el pirata informático obtiene información con detalles del wifi o red de la víctima al quien se estaría atacando, estudiar a su víctima de esta manera es como operan los hackers al momento de realizar una agresión a un sistema vulnerable [4], [16], [17].

El programa ANGRY IP SCANNER tiene una variedad de funciones igual a las que se han mencionado pero es escogida para el análisis o la comprobación de puertos con las direcciones ip que tiene su receptor a ser vulnerado, mientras que el programa AES CRYPT tiene como finalidad la encriptación de archivos en forma segura, utilizando este software los piratas informáticos respaldan sus datos o informaciones para que su víctima a la hora de atacar o en este caso de defenderse no distinga sus archivos tan fácilmente y mucho menos desencriptarlos. Es así como se ha podido contrastar estos programas que tienen las ciertas características similares, pero con distintas magnitudes altas al conocer detalles valiosos de una víctima [18].

3 Resultados y Discusión

Un software o herramienta utilizado por un pirata informático, es declarable una amenaza a la hora de realizar un lanzamiento de penetración ya sea en un medio interno como externo, porque es difícil que una víctima resguarde información integral o confidencial. En el año 2016, con el rastreo y ataque de estos softwares se pudo ocasionar una máxima incidencia de malware con softwares en ese entonces de última generación, estableciendo las medidas y estadísticas de diferentes tipos de ataques, con solo una sentencia o manipulación de un código malicioso se puede generar un riesgo hacia la victima quien no podrá equiparar sus herramientas de ataque [18].

Por otra parte, en el año 2017 se realizó una evaluación técnica acerca del hacking o piratería volviéndose un servicio de diagnósticos en diferentes alojamientos de vulnerabilidades y que se pudo prestar con un periodo de tiempo diversificado, de esta manera el prolongando un diseño experimental se dio a cabo con un análisis de minucioso y estadístico al momento de penetrar un sistema. Las medidas ofensivas y defensivas de la seguridad informática llevan lugar a los sistemas informarles el estado en el que se encuentra un software en su estado de verificación [16].

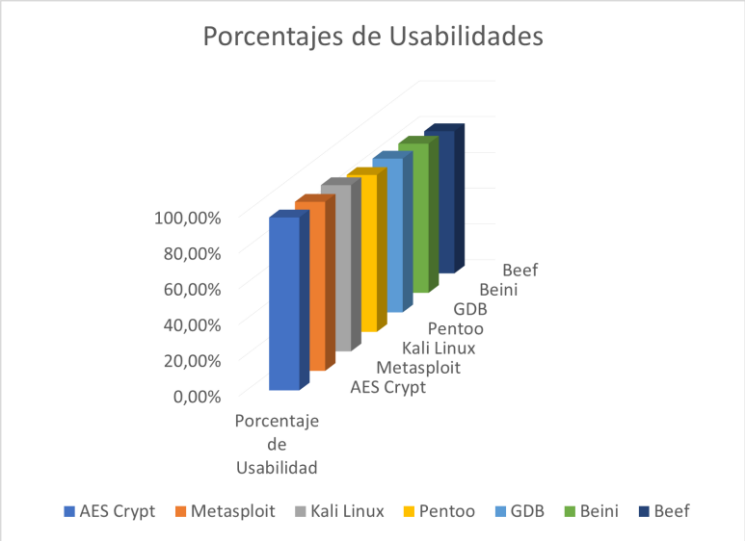

Fig. 1. Estadísticas de los Softwares más utilizados por los Piratas Informáticos.

La seguridad de TI refuerza protección ante todo delito informático, minimizando el desarrollo eficiente y mejorando el desarrollo eficaz, para dar como resultado una protección estricta y preventivas hacia nuevas amenazas. Al mismo tiempo, demostrando un promedio estadístico del 94 % de los hackers utilizan Metasploit para los lanzamientos delictivos de ataques informáticos. Un valor a ponderado del 86 % reportan ataques de phishing dándole a este resultado un nivel de peligrosidad destacable para las organizaciones [19].

Contrarrestando los malo hábitos de estos resultados, el 53 % de penetración en un sistema legal es perjudicado por el valor organizacional, promoviendo resultados de hackers infiltrados en sistemas patentes a auditorias simplificadas. La delincuencia informática maneja muchas estrategias de vulnerabilidades a penetrar en distintos escenarios dando continuidad al desarrollo investigativo tecnológico llegando al punto de no poder abogar o mitigar en relación con un ataque cibernético [17].

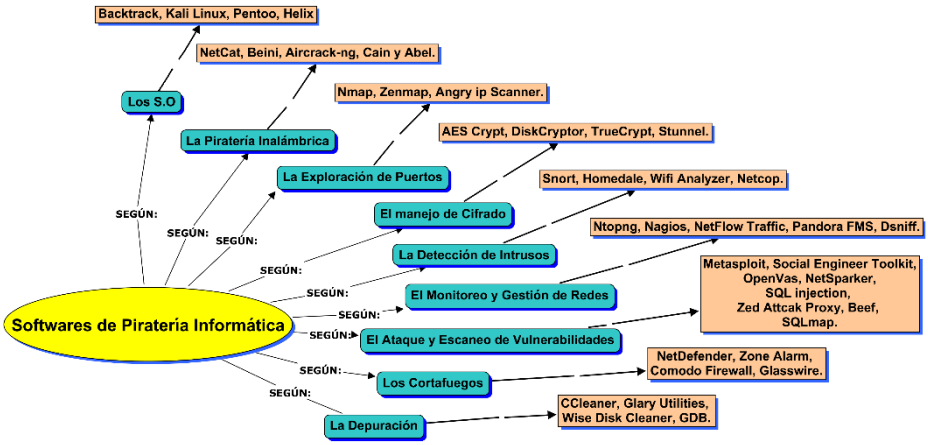

Fig. 2. Categorización de los Softwares de Piratería Informática más utilizados por los hackers, dentro de los años 2015-2020.

Llegando al procedimiento de argumentar o discutir la situación de estos softwares, se puede captar que existen manipulaciones en los códigos fuentes de cada programa, estos procedimientos consisten en tener los conocimientos técnicos en codificaciones de datos, para realizar lo más común que se conoce como Caballo de Troya. A un creador de softwares quien establece parámetros para combatir la piratería informática, se ve obligado a cumplir normas de vida útil para los programas que él ha desarrollado, que por lo general siempre los hackers se verán obligados a descifrar estos códigos fuentes para producirlos, clonarlos y venderlos al mercado[20]. De esta forma es como se discute el riesgo de un programa informático que estaría dispuesto a la ciberdelincuencia.

4 Conclusiones

Se analizaron varios trabajos científicos, que están en bases de datos de investigaciones y son reconocidas a nivel de investigadores en el campo científico, para poder clasificar y examinar los softwares más utilizados por los piratas informáticos.

Se mantuvieron organizadas y claras todas y cada una de las metodologías de ataques que se han venido utilizando por los piratas informáticos; las cuales se han podido identificar qué tipos de procedimiento se han logrado manejar para una penetración en sistemas de seguridad.

En el artículo académico, los softwares o herramientas de los hackers han sido contrastados gracias a la categorización que se pudo aplicar para la comprensión y conocimiento de estos programas que han poseído los piratas informáticos.

Finalmente, como vías futuras acerca de estos softwares de piratería ya examinados y estudiados, se investigará el desarrollo de un software, que vincule directamente desde un BIG DATA relacionado a la seguridad, para la ayuda de encaminar los

diferentes tipos de categorizaciones e ir simplificando los resultados de ataques, utilizándose bajo la responsabilidad de la ciberseguridad ética.

Referencias

[1] C. Ulaş, U. Aşik, and C. Karadeniz, "Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines," *Comput. Secur.*, vol. 58, pp. 250–267, 2016, doi: 10.1016/j.cose.2016.02.001.

[2] X. Zhou and J. Pang, "Expdf: Exploits detection system based on machine-learning," *Int. J. Comput. Intell. Syst.*, vol. 12, no. 2, pp. 1019–1028, 2019, doi: 10.2991/ijcis.d.190905.001.

[3] M. C. Ghanem and T. M. Chen, "Reinforcement learning for efficient network penetration testing," *Inf.*, vol. 11, no. 1, pp. 1–23, 2020, doi: 10.3390/info11010006.

[4] F. Abazari, M. Analoui, and H. Takabi, "Effect of anti-malware software on infectious nodes in cloud environment," *Comput. Secur.*, vol. 58, pp. 139–148, 2016, doi: 10.1016/j.cose.2015.12.002.

[5] T. Nagai, M. Kamizono, Y. Shiraishi, and S. Member, "A Malicious Web Site Identification Technique Using Web Structure Clustering," no. 9, pp. 1665–1672, 2019.

[6] H. Aldawood and G. Skinner, "Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions," *IEEE Access*, vol. 8, pp. 67321–67329, 2020, doi: 10.1109/ACCESS.2020.2983280.

[7] M. Luck, "Entrapment behind the firewall: the ethics of internal cyber-stings," *Australas. J. Inf. Syst.*, vol. 23, pp. 1–15, 2019, doi: 10.3127/ajis.v23i0.1886.

[8] S. Keshishzadeh and A. J. Mooij, "Formalizing and testing the consistency of DSL transformations," in *Formal Aspects of Computing*, 2016, vol. 28, no. 2, pp. 181–206, doi: 10.1007/s00165-016-0359-1.

[9] G. Falco, A. Viswanathan, C. Caldera, and H. Shrobe, "A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities," *IEEE Access*, vol. 6, pp. 48360–48373, 2018, doi: 10.1109/ACCESS.2018.2867556.

[10] S. S. Malladi and H. C. Subramanian, "Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations," *IEEE Softw.*, vol. 37, no. 1, pp. 31–39, 2020, doi: 10.1109/MS.2018.2880508.

[11] R. Zhang, X. Chen, S. Wen, X. Zheng, and Y. Ding, "Using AI to Attack VA: A stealthy spyware against voice assistances in smart phones," *IEEE Access*, vol. 7, pp. 153542–153554, 2019, doi: 10.1109/ACCESS.2019.2945791.

[12] H. Wang, W. Yue, Q. Song, J. Liu, and G. Situ, "A hybrid Gerchberg–Saxton-like algorithm for DOE and CGH calculation," in *Optics and Lasers in Engineering*, 2016, vol. 89, pp. 109–115, doi: 10.1016/j.optlaseng.2016.04.005.

[13] D. Javaheri, M. Hosseinzadeh, and A. M. Rahmani, "Detection and elimination of spyware and ransomware by intercepting kernel-level system routines," *IEEE Access*, vol. 6, pp. 78321–78332, 2018, doi: 10.1109/ACCESS.2018.2884964.

[14] J. E. Martínez-Lozano and P. S. Atencio-Ortiz, "Creation of a DDOS attack using HTTP-GET Flood with the Cyber Kill Chain methodology," *Iteckne*, vol. 16, no. 1, pp. 41–47, 2019, doi: 10.15332/iteckne.v16i1.2160.

[15] H. Zhang, D. Yao, N. Ramakrishnan, and Z. Zhang, "Causality reasoning about network events for detecting stealthy malware activities," *Comput. Secur.*, vol. 58, no. May 2012, pp. 180–198, 2016, doi: 10.1016/j.cose.2016.01.002.

[16] D. Nikolopoulos, G. Moraitis, D. Bouziotas, A. Lykou, G. Karavokiros, and C. Makropoulos, "Cyber-Physical Stress-Testing Platform for Water Distribution Networks," *J. Environ. Eng. (United States)*, vol. 146, no. 7, pp. 1–21, 2020, doi: 10.1061/(ASCE)EE.1943-7870.0001722.

[17] C. Trippel, D. Lustig, and M. Martonosi, "Security Verification via Automatic Hardware-Aware Exploit Synthesis: The CheckMate Approach," *IEEE Micro*, vol. 39, no. 3, pp. 84–93, 2019, doi: 10.1109/MM.2019.2910010.

[18] D. Bowes, T. Hall, and J. Petrić, "Software defect prediction: do different classifiers find the same defects?," in *Software Quality Journal*, 2018, vol. 26, no. 2, pp. 525–552, doi: 10.1007/s11219-016-9353-3.

[19] J. W. Park and S. J. Lee, "Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants," *Nucl. Eng. Technol.*, vol. 51, no. 1, pp. 138–145, 2019, doi: 10.1016/j.net.2018.09.009.

[20] W. Li, L. Xie, Z. Deng, and Z. Wang, "False sequential logic attack on SCADA system and its physical impact analysis," *Comput. Secur.*, vol. 58, pp. 149–159, 2016, doi: 10.1016/j.cose.2016.01.001.