Revista NEYART
ISSN: 2992-7161

DETECCIONES DE VULNERABILIDADES WEB ATRAVÉS DE LA EVALUACIÓN DE PRUEBAS DE PENETRACIÓN

DETECTIONS OF WEB VULNERABILITIES THROUGH THE EVALUATION OF PENETRATION TESTS

Bernal Ontiveros Juan Manuel
Tecnológico Nacional de México/I. T. De Ciudad Juárez
https://orcid.org/0000-0002-3819-5750
jbernal@itcj.edu.mx

Bailón Estrada Margarita
Tecnológico Nacional de México/I. T. De Ciudad Juárez
https://orcid.org/0000-0003-2830-5829
mbailon@itcj.edu.mx

Flores Regalado Anilu
Tecnológico Nacional de México/I. T. De Ciudad Juárez
https://orcid.org/0000-0003-4352-259X
anilu.fr@cdjuarez.tecnm.mx

Benítez Guadarrama Juan Pedro
Universidad autónoma del Estado de México/UAEM
https://orcid.org/0000-0002-2826-6359
jpbenitezg@uaemex.mx

Cervantes Cardenas Susan Alexandra
Tecnológico Nacional de México/I. T. De Ciudad Juárez
https://orcid.org/0009-0008-6125-3657
L21111089@itcj.edu.mx

DOI: https://doi.org/10.61273/neyart.v1i2.49 **| Recibido: 25/01/2024 | Aceptado: 14/03/2024 | Publicado: 15/04/2024**

Resumen: A través de los últimos años los administradores de seguridad han influido en los desarrolladores de software para que diseñen software más resistente ante ataques de software mal intencionados, pero también en las metodologías y técnicas de seguridad que dan apoyo para detectar vulnerabilidades en la infraestructura de la información de una empresa, basado en el surgimiento de fraudes y robos de información que sufren organizaciones, emerge la práctica pentesting (Prueba de penetración), que es una de las técnicas más novedosas en cuanto a lo que a Seguridad Informática se refiere.

Esta técnica es una forma de detectar vulnerabilidades tras implementarse, en beneficio de una empresa para reforzar aquellas fallas que pudiesen explotar los atacantes, es por ello que la meta principal es encontrar vulnerabilidades en las aplicaciones web. Con el pentesting se llevará a cabo una rastreabilidad exhaustiva de todas las vulnerabilidades que puedan ser encontradas. Los impactos y la probabilidad de explotación de cada vulnerabilidad encontrada también será calificada según el esquema estándar de puntuación de vulnerabilidad basándose en la metodología OWASP.

Además, las vulnerabilidades se clasificarán según las consecuencias de la explotación identificadas a través de los hallazgos. Por lo que se proporcionará un informe con la recomendación para cada vulnerabilidad para atenuar o detener la amenaza. La rastreabilidad de vulnerabilidades se basará en procesos de trabajo y formas innovadoras de proteger toda aplicación web de las amenazas. Este reporte apoyaría a los desarrolladores, proveedores y usuarios de aplicaciones web a comprender mejor los posibles problemas de seguridad relacionados con las aplicaciones web y cómo deben ser tratados.

Una manera de probar la robustez de un sitio es realizando una prueba de manera que se pueda atacar, esta técnica llamada prueba de penetración (Pentesting en inglés). Antes de lanzar un sitio, la seguridad de la red y de la aplicación web debe ser completamente segura y probada. Este estudio tiene como objetivo encontrar debilidades y fallas en las aplicaciones web. La prueba de penetración recopilará información sobre la fortaleza de las redes, los agujeros de seguridad y el acceso. El resultado del reporte es indicar las recomendaciones para mejorar la seguridad de una infraestructura de una organización. En cuanto a los resultados de las pruebas de penetración, la organización o empresa interesada puede corregir las vulnerabilidades que existen en el sitio web.

La importancia de tener un sistema fuerte ante ataques e infiltraciones es el de evitar las vulnerabilidades, que son explotadas por un atacante malintencionado (atacante/hacker), por lo que puede afectar la confidencialidad, integridad y disponibilidad de una aplicación web o información distribuida.

Palabras Clave: Vulnerabilidades, Infiltración, Seguridad, Prueba de Penetración, Pentesting.

Abstract: Over the last few years, security administrators have influenced software developers to design software that is more resistant to malicious software attacks, but also in the security methodologies and techniques that support detecting vulnerabilities in the infrastructure of a company's information, based on the emergence of fraud and theft of information suffered by organizations, the practice of Pentesting (Penetration Testing) emerges, which is one of the most innovative techniques in terms of Computer Security.

This technique is a way to detect vulnerabilities after being implemented, for the benefit of a company to reinforce those flaws that attackers could exploit, which is why the main goal is to find vulnerabilities in web applications. With pentesting, exhaustive traceability of all vulnerabilities that may be found will be carried out. The impacts and probability of exploitation of each vulnerability found will also be scored according to the standard vulnerability scoring scheme based on the OWASP methodology.

Additionally, vulnerabilities will be classified based on the consequences of exploitation identified through the findings. Therefore, a report will be provided with the recommendation for each vulnerability to mitigate or stop the threat. Vulnerability traceability will be based on work processes and innovative ways to protect every web application from threats. This report would support web application developers, providers and users to better understand the potential security issues related to web applications and how they should be addressed.

One way to test the robustness of a site is to perform a test so that it can be attacked, this technique is called penetration testing (Pentesting in English). Before launching a site, the network and web application security must be completely secure and tested. This study aims to find weaknesses and flaws in web applications. Penetration testing will collect information on network strength, security holes, and access. The result of the report is to indicate recommendations to improve the security of an organization's infrastructure. Looking at the results of the penetration tests, the interested organization or company can correct the vulnerabilities that exist on the website. The importance of having a strong system against attacks and infiltrations is to avoid vulnerabilities, which are exploited by a malicious attacker (attacker/hacker), which can affect the confidentiality, integrity and availability of a web application or information distributed.

Keywords: Vulnerabilities, Infiltration, Security, Penetration Testing, Pentesting.

INTRODUCCIÓN

Conforme la tecnología avanza a pasos agigantados, la información viene ser requerida como recurso muy valorado, que implícitamente contiene datos confidenciales y valiosos para las organizaciones o instituciones que deben ser protegidos contra ataques no deseados por infiltraciones externas a su entorno. Por medio de la web, la tecnología de la información está creciendo muy rápidamente, de manera que se puede acceder y recuperar fácilmente la información. La utilización de la información es absolutamente necesaria para aumentar el valor agregado de las empresas y organizaciones proporcionando un excelente servicio a los usuarios que la utilizan para ser competitivos. Por otro lado se tiene la amenaza de ataques y fugas de datos por las infiltraciones ilegales por parte de atacantes malintencionados. Es debido a esto que se ha incrementado el número de delitos informáticos relacionados con los sistemas de información en la web. Cada sistema que está conectado a la web es un blanco potencial a los ataques maliciosos, entre tanto el nivel de ataque también se incrementa (Hariyanto y Siahaan 2016).

Si definimos el pentesting o penetration test (prueba de penetración) podemos decir que es un ciberataque simulado que ataca al sistema informático de una organización o empresa para comprobar si existen vulnerabilidades que puedan ser explotables. Es, por tanto, una de las pruebas habituales para aumentar el cortafuegos de aplicaciones.

Conforme aumenta el uso de aplicaciones web para diferentes categorías de servicio o trabajo apoyando el manejo de la información, muchas empresas recurren a estas aplicaciones en línea para promocionar sus servicios, por tanto se ven grandes ventajas de las aplicaciones web entre las que destacan la comodidad, bajos costos y poca necesidad de configuración adicional de hardware o software. Mientras tanto, las amenazas o ataques contra las aplicaciones web se están incrementando por lo que el atacante no necesita mucha experiencia o conocimiento para atacar e infiltrarse en una aplicación web que tiene una protección muy débil o casi nula. Si bien los ataques comunes, como los scripts entre sitios y la inyección SQL tiene mucho tiempo de existencia, también se siguen descubriendo constantemente nuevos *exploits* (software que ataca una vulnerabilidad) que hacen que las empresas necesiten una mayor seguridad (Bitdefender, 2023).

Las pruebas de penetración son un método utilizado para medir la seguridad de una infraestructura de datos o sistema informático, ya sea de una red o aplicación web. Su principal objetivo es descubrir las posibles vulnerabilidades o fallas que podrían ser explotadas a través de una infiltración llevada a cabo

por un atacante malicioso y sugiriendo soluciones al problema a las vulnerabilidades encontradas. Con las correcciones de seguridad adecuadas, un sistema de una organización puede pasar de ser una amenaza a tener datos confidenciales en una plataforma segura y funcional con tan solo los ajustes necesarios.

DESARROLLO

Descripción del Problema

Una aplicación web debe garantizar seguridad a quien la utilice, para la realizar cualquier transacción, esto con el fin de evitar problemas de seguridad, por ende una aplicación debe garantizar que todos los receptores que sean sensibles reciban argumentos que están bien fundamentados en los niveles de seguridad. Debido a que los intentos de atacantes o usuarios potencialmente malintencionados puedan infiltrarse para infiltrar valores arbitrarios, por lo que la aplicación web tiene que validar adecuadamente cada entrada de información, es por esto que la aplicación debe verificar cada entrada de datos en busca de valores que violan las especificaciones. Cuando se encuentran problemas como cuando se intenta introducir valores no válidos se tiene dos opciones (Sreenivasa y Kumar 2012).

- La primera opción es la cancelación del procesamiento posterior a la solicitud de acceso, por lo que la aplicación se detiene para manejar la solicitud y devuelve un código de error para señalar que existe una entrada incorrecta.
- La segunda opción es la transformación del valor que se introduce de entrada tal que cuando este valor alterado sea denegado su acceso en base a la especificación de entrada y ya no represente una amenaza.

Se puede denotar el proceso de transformación de una entrada como una representación que ya no es peligrosa por lo que se conoce como un proceso seguro. Normalmente, la desinfección implica la eliminación de amenazas.

Las violaciones de seguridad han dominado a través del tiempo, poniendo en riesgo a un número cada vez mayor de empresas u organizaciones. Los atacantes informáticos malintencionados siguen desarrollando a diario formas de ataques complejas y sofisticadas (Mendhurwar y Mishra, 2021). La instalación de medidas de seguridad como cortafuegos y antivirus en el sistema ya no garantiza la seguridad de las empresas. Las operaciones corporativas modernas necesitan un enfoque avanzado para proteger sus sistemas. Por lo tanto, las organizaciones deben comprobar el nivel de seguridad, mediante pruebas de

penetración, a sus sistemas e información para que se desarrollen mecanismos de defensa fuertes y eficaces contra las infiltraciones delincuenciales que sean identificadas en el sistema de una corporación.

Justificación

Durante el desarrollo de estrategias o procesos de seguridad, las pruebas de penetración se han convertido en una técnica muy importante en la evaluación de la fortaleza de los sistemas de un corporativo evaluando sus procesos y mecanismos de seguridad para identificar la fragilidad de los sistemas de seguridad e incluso justificando la agregación de nuevas herramientas y procesos en el área para combatir infiltraciones no deseadas. Por lo tanto, es una manera de rastrear y reconocer las debilidades y vulnerabilidades de seguridad, permitiendo blindar y fortalecer las capas de seguridad implementadas en su infraestructura. Este tipo de pruebas de penetración son recomendables como una auditoria y que se puedan llevar a cabo al menos una vez al año, permitiendo una mejora continua en procesos y mecanismos de seguridad informática, y por supuesto que las pruebas de penetración las realicen personal certificado y calificado para realizar este trabajo.

Objetivo

Las pruebas de penetración tienen como función principal el de aplicar un ejercicio de seguridad en el cual un personal certificado y calificado intenta rastrear e identificar las vulnerabilidades de un sistema informático para sugerir mejoras a un sistema, fortaleciendo la estructura de una organización con respecto a la información. El objetivo de este ataque simulado es identificar cualquier vulnerabilidad potencial en las defensas de una infraestructura informática, y que los atacantes podrían aprovechar en los sistemas y estructuras de redes en una organización, y por medio de herramientas especializadas intentar lograr una infiltración del lado de un atacante, permitiendo medir el nivel de alcance e impacto del ataque que se pudiera dar al realizarse de forma real.

Metodología

Las Pruebas de Penetración son una técnica que las organizaciones o corporativos utilizan para evaluar los sistemas e infraestructuras internos, en busca de vulnerabilidades. Se lleva a cabo atacando todas las áreas en busca de debilidades en contra de infiltraciones de ataques maliciosos, por supuesto que este ataque debe tener la autorización debida de la dirección de la organización. El objetivo es simular los ataques a la empresa como si fuesen reales, esto se realiza con el motivo de identificar cualquier vulnerabilidad en los sistemas y la infraestructura, (Montero, 2005).

Antes de continuar en este apartado es necesario definir lo que es un Pentester: Es un profesional de ciberseguridad que se especializa en la evaluación de la seguridad de sistemas, redes y aplicaciones informáticas (KeepCoding, 2023)

Entre las actividades que realiza un pentester se destacan las siguientes:

- Análisis de vulnerabilidades.
- Pruebas de penetración.
- Evaluación de seguridad.
- Informe de resultados.
- Pruebas de redes y sistemas.
- Pruebas de aplicaciones web.
- Simulaciones de ataques.
- Formación y concientización.

Por lo que se muestra, el trabajo de un pentester es esencial y debe garantizar la seguridad de la información y proteger los activos digitales de una organización contra amenazas cibernéticas.

Las Pruebas de Penetración pueden clasificarse en 3 modos (Ortega 2022):

- *White Box (Caja Blanca):* El Pentester debe de tener pleno conocimiento del objetivo a atacar, y es necesario que el administrador de Seguridad de TI pueda compartir esta información con el Tester. El administrador tendrá un conocimiento sobre el tipo de prueba a realizar y en qué momentos se llevarán a cabo.
- *Black Box (Caja Negra):* El Pentester no cuenta con ningún tipo de información del objetivo, simulando un atacante externo a la organización, por lo que el pentester se encargaría de realizar la debida investigación por sus propios medios, ya sea por medio de ingeniería social, escaneos de puertos, escaneos de vulnerabilidades, etc. Dichas pruebas de penetración pueden ser realizadas desde localidades remotas o incluso dentro de las oficinas de la organización
- *Gray Box (Caja Gris):* El Pentester cuenta con determinada cantidad de información del objetivo, por lo que se trata de una combinación entre White y Black Box.

Tipos de Pruebas de Penetración

Es importante mencionar las siguientes categorías en las que se realizan las pruebas de penetración, conocida también como prueba de seguridad o de penetración, estas son utilizadas por los conocedores

llamados hackers éticos, y estos pueden aplicar uno o más tipos de pruebas a los sistemas de las organizaciones. A continuación se mencionan las clasificaciones:

- *Pruebas de Ingeniería Social:* este tipo de ataque se ejecuta para engañar a las personas para que revelen información confidencial acerca de ellos mismos o de su organización. Por lo tanto, los humanos pueden ser el eslabón más débil en un sistema de seguridad, (Tori, 2008).
- *Pruebas de Aplicaciones Web:* utilizan varias herramientas de software para probar qué tan seguro es el código de una aplicación web. Se prueba el código para detectar cualquier vulnerabilidad, y encontrar una manera de corregirla para evitar cualquier ataque.
- *Pruebas de Penetración Física:* los dispositivos físicos en una organización, deben asegurarse de que el acceso a ellos sea solo de personal autorizado. Todos los dispositivos físicos son probados en busca de cualquier vulnerabilidad.
- *Pruebas de Firmware de Red:* se realizan pruebas en todos los puntos de entrada de una red, y dichas pruebas verifican el tráfico que entrada y salida. La prueba se aplica tanto de forma local como remota.
- *Pruebas del Lado del Cliente:* son pruebas que se llevan a cabo sobre el software de la organización para identificar cualquier vulnerabilidad en la infraestructura.
- *Pruebas de Red Inalámbrica:* esta prueba escanea todos los puntos de acceso wi-fi en una organización en busca de vulnerabilidades.

Fases de una Prueba de Penetración (Pentesting)

- **Reconocimiento:** En esta fase se trabaja con la recopilación de toda información posible, utilizando diferentes técnicas tales como:
  - Recopilación de dominios/IPs/puertos/servicios
  - Recopilación de metadatos
  - Uso de Google Dorks: Google Dorks o Dorking, también conocido como Google Hacking es una técnica que en realidad es una búsqueda avanzada através de Google, la que encuentra información concreta en la web, elaborando un filtrado de resultados usando operadores que son conocidos como Dorks, que en realidad son símbolos que especifican una condición. Ejemplo de ello, si escribimos un texto en la búsqueda entre dobles comillas (“texto”), entonces actuará buscando la coincidencia que sea exacta del escrito con lo que se puso entre comillas dobles, o sea la palabra texto. Es

decir, si buscamos “OSI”, devolverá el contenido que encaje y sea exacto con ese término (Incibe, 2023).

- Recopilación de información gracias a servicios de terceros.

- **Análisis de vulnerabilidades:** En esta fase se analiza los datos coleccionados obtenidos en la fase anterior y el rastreo de las vulnerabilidades encontradas. Con la información obtenida se intenta la búsqueda de exposiciones y vulnerabilidades comunes (CVEs: Common Vulnerabilities and Exposures), ya conocidas y/o fáciles de ser explotadas.
- **Explotación:** La fase de explotación está basada en llevar acabo las acciones que comprometen al sistema de un corporativo que se está auditando, ya sea a los usuarios o la infraestructura de la información, la cual se maneja de manera interna. Y el principal punto es de que se compruebe que los ataques no se realicen, y se lista a continuación los tipos de ataque (Sánchez, 2018):
  - Inyección de código
  - Inclusión de ficheros locales o remotos
  - Evasión de autenticación
  - Carencia de controles de autorización
  - Ejecución de comandos en el lado del servidor
  - Ataques tipo Cross Site Request Forgery
  - Control de errores
  - Gestión de sesiones
  - Fugas de información
  - Secuestros de sesión
  - Comprobación de las condiciones para realizar una denegación de servicio
  - Carga de ficheros maliciosos

Se aclara que estos tipos de ataques se llevan a cabo de acuerdo a la naturaleza de cada ataque en desarrollo, las técnicas en uso y las últimas tecnologías disponibles adaptadas para conseguirlo.

- **Post explotación:** Cuando en la búsqueda de vulnerabilidades se encontrase una vulnerabilidad en el sistema auditado o en el entorno, se llevarán controles adiciones con el propósito de comprobar lo critico de esta debilidad. En función de la vulnerabilidad, se intentarán realizar las siguientes acciones de post-explotación (Pruebas):

- Evadir mecanismos de autenticación
- Realizar acciones del lado de un usuario
- Realizar acciones o ejecutar comandos en el servidor que aloja alguna aplicación
- Privilegios disponibles en el servidor, si se consigue acceso al mismo
- Otros sistemas o servicios accesibles desde la aplicación comprometida
- Posibilidad de infiltración impersonalizada de un usuario
- Realizar acciones sin el consentimiento o conocimiento de un usuario

La posibilidad de encadenar una o varias vulnerabilidades para conseguir una infiltración de acceso a un mayor nivel o en la infiltración para evadir los controles de seguridad, que también serán panoramas evaluados para valorar el análisis de riesgos a la hora de ser realizado.

- **Informes**: Esta es la última parte de una prueba de penetración en la que se realizará un reporte final (esto es un informe del estado de cómo se encontró la prueba de penetración) donde se deberá incluir todas las vulnerabilidades encontradas y las explotaciones de las áreas débiles en las que los atacantes podrían infiltrarse. Se debe describir en este documento todo lo obtenido en la prueba de penetración. Además de la información contenida en el reporte final, debe constar, si se ha pactado con anterioridad, contramedidas para resolver (o mitigar) en medida de lo posible estos problemas.

Herramientas de las Pruebas de Penetración (Pentesting)

KALI es una distribución GNU/Linux pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática y hacking ético en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática. Incluye una larga lista de herramientas de seguridad y de hacking listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, bases de datos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless, entre otras orientas a pruebas de Hacking Ético en todas sus fases.

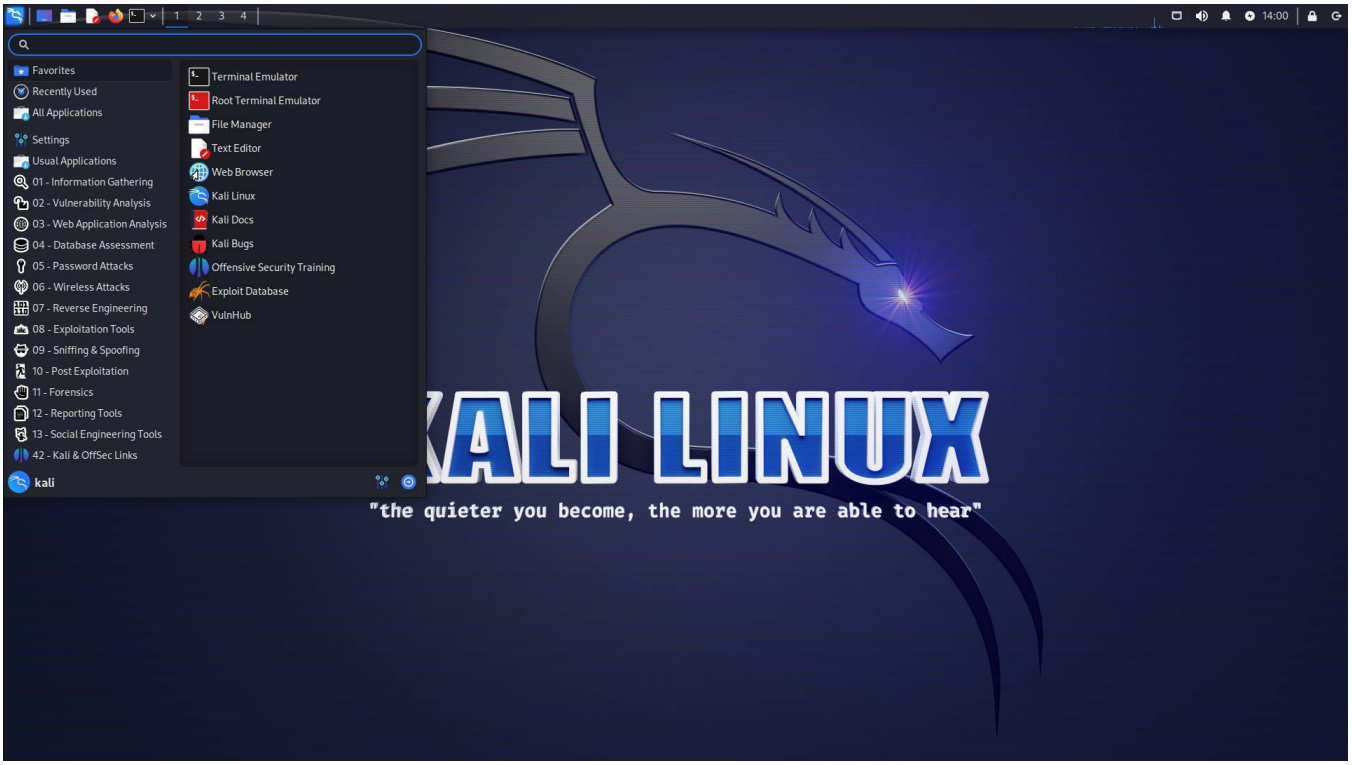

Figura 1. Herramientas Kali.
Fuente: Imagen descargada de http://www.kali.org

ANÁLISIS DE RESULTADOS

De las herramientas que contiene Kali Linux, para llevar a cabo las pruebas de penetración se encuentra *John The Ripper*, es una aplicación de código abierto que viene instalada por defecto en el sistema operativo Kali Linux, la cual tiene como función para descifrar contraseñas de usuarios a partir de sus códigos hash. Las funciones hash son irreversibles por definición, por lo que *John The Ripper* genera los códigos hash de miles de palabras incluidas en un archivo de texto plano conocido como diccionario. A este tipo de operación se le conoce como ataque de diccionario, además es el programa que comúnmente es más utilizado para ejecutar uno (KeepCoding, 2023). El método de uso del modo diccionario de *John The Ripper* involucra que sea usada una lista de palabras que son predeterminadas para adquirir de formas diferentes. Y para muestra, hay una existencia de diccionarios que son renombrados como el ejemplo *RockYou.txt*, entre tanto, asimismo, se pueden crear listas de palabras propias a partir de bases de datos filtradas, lo cual es común en los ciberataques.

1. Primero, puedes indicarle a John cuál es el tipo de hash que estás intentando romper. Si no, el programa puede identificarlo por sí solo. No obstante, especificar este dato agilizará el funcionamiento de la aplicación. Por ejemplo (para un hash en formato MD5): –format=rawmd5.
2. Luego, debes escoger la ruta del diccionario. Por ejemplo: wordlist=/usr/share/wordlists/rockyou.txt.
3. Finalmente, debes indicar el nombre del archivo de texto que contiene el código hash a romper. Por ejemplo: hashEjemplo.txt.

A partir de este ejemplo, la línea de código en la consola se vería de la siguiente manera para el aprendizaje de *John The Ripper*:

```
john --format=rawmd5 --wordlist=/usr/share/wordlists/rockyou.txt hashEjemplo.txt
```

Realizará que el programa genere las funciones *hash MD5* de cada una de las palabras del diccionario y sean comparadas contra el con el código hash del archivo de texto «hashEjemplo.txt» hasta que sea encontrada una coincidencia (KeepCoding, 2023).

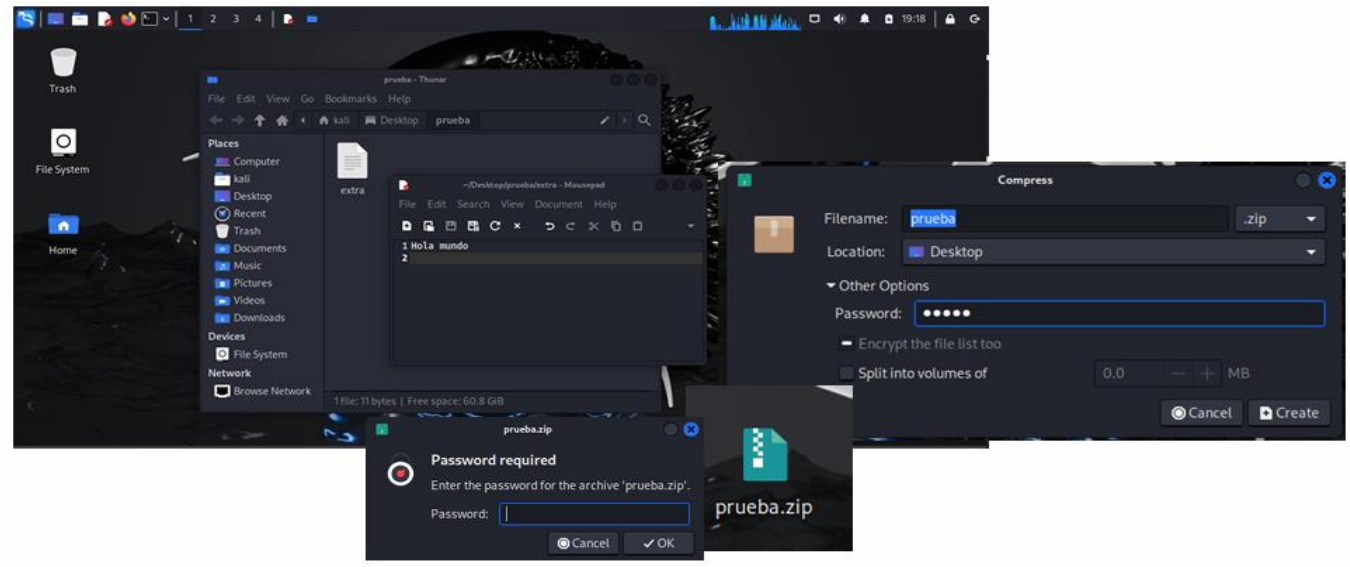

Figura 2. John The Ripper (Contraseña).

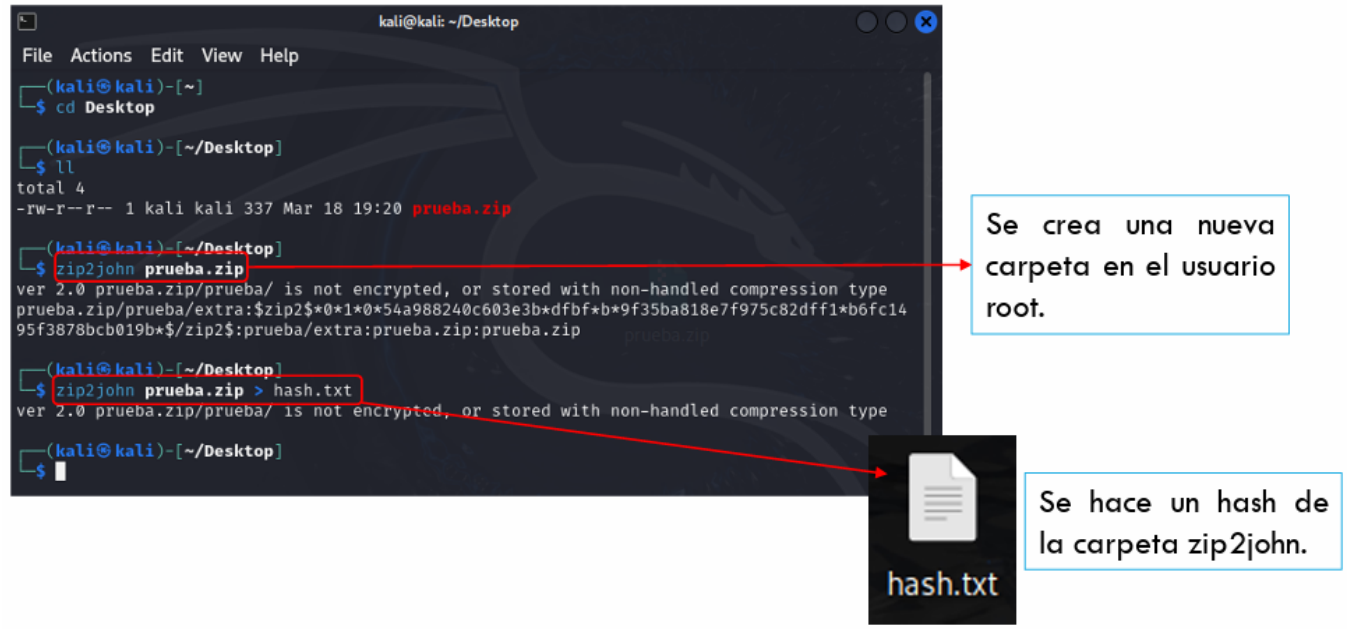

Figura 3. John The Ripper (Creación de Hash).

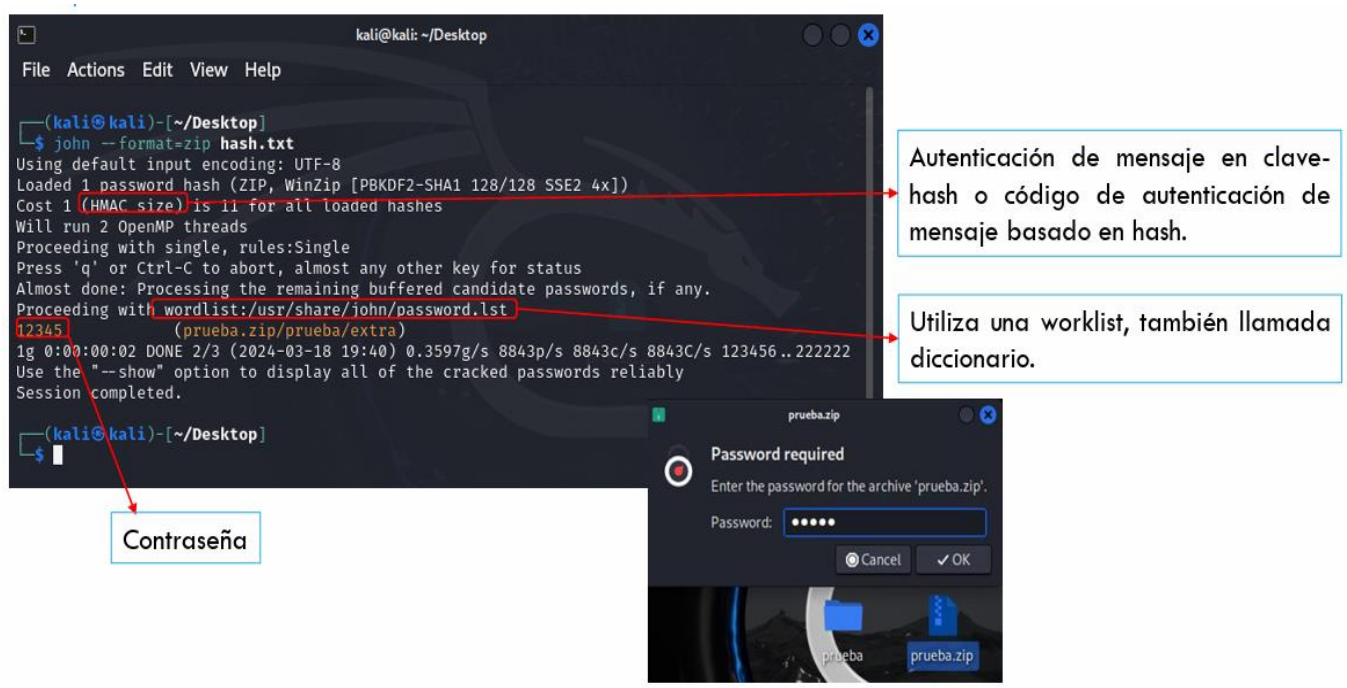

Figura 4. John The Ripper (Desencriptación).

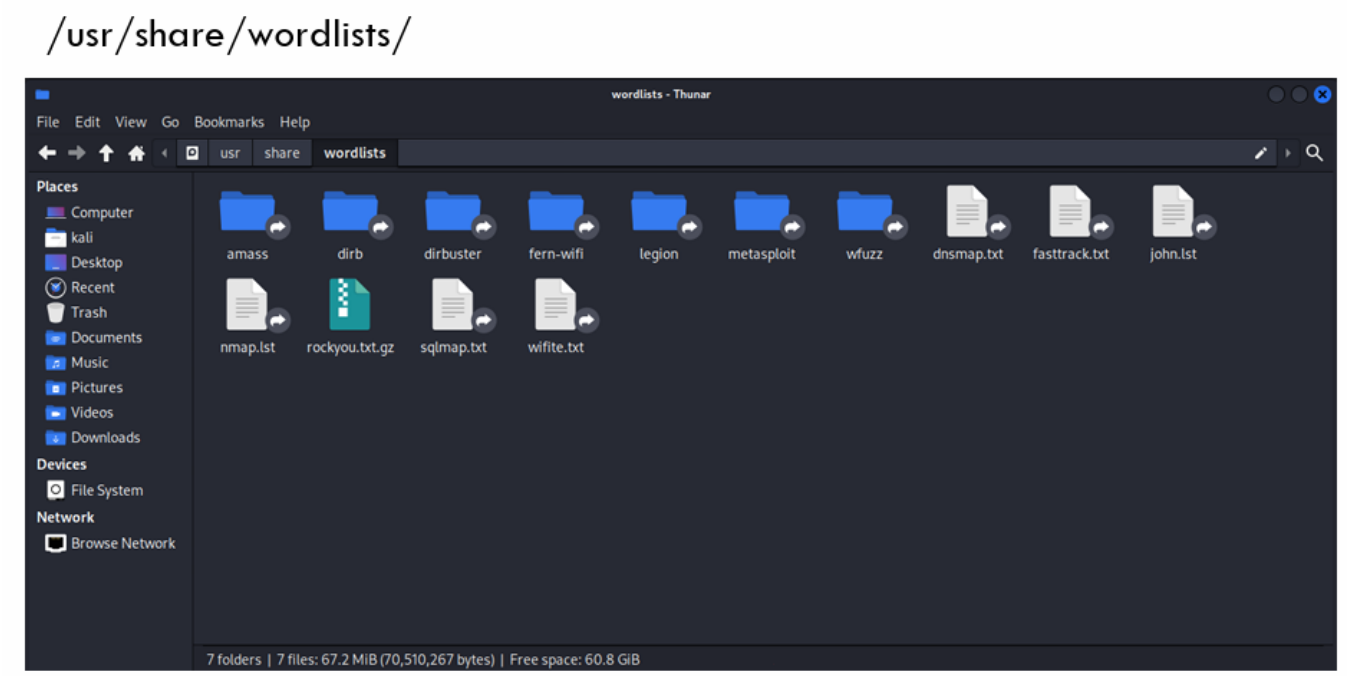

Figura 5. John The Ripper (Diccionario).

CONCLUSIONES

Por todo es sabido que la vulnerabilidad está directamente indexada a la complejidad de las nuevas tecnologías, Hernández (2015), es claro que se puede prevenir estos ataques informáticos, y la manera de de hacerlo es tomar la acción de anticipar detectando las vulnerabilidades que pueden ser potenciales, y que pueden ser infiltradas por los atacantes. Es por esta razón que se disminuye la probabilidad de infiltración, y así se reduce el éxito que puedan tener los atacantes.

Aunque existen muchas vulnerabilidades, algunas definitivamente son más importantes que otras, de aquí que el diseño y desarrollo de herramientas para detectarlas y corregirlas, debe ser eficiente, Campderrós Vilà (2019). Debemos de tener en cuenta que la seguridad es de suma importancia en las aplicaciones web, y el medio para implementarla es el de realizar pruebas de penetración, para qué a través de ellas, se pueda rastrear las vulnerabilidades en el sistema de una infraestructura de cualquier organización, institución o empresa. Al detectar las fallas o vulnerabilidades, sea entregado a la alta dirección o gerencia un reporte del mapeado por las diversas técnicas aplicadas y herramientas aplicadas en el pentesting, sugiriendo las prevenciones o acciones correctivas que se deben establecer para dar solución a dichos problemas.

Las pruebas de penetración tienen como finalidad el rastreo de lograr descubrir fallas de infiltraciones indebidas convertidas en ataques a los sistemas internos de las organizaciones o empresas, esto es con el objetivo de reparar las debilidades encontradas a través de huecos y que por medio de acciones de prevención o correcciones ante un ataque sin autorización a un sistema de un corporativo, para evitar el robo, fraude o alteración no autorizada de la información confidencial.

La prueba de penetración conocida también como *pentesting* dentro del concepto de *hacking ético*, es la evaluación de la infraestructura interna de una empresa, que prueba y determina si los mecanismos de defensa que se utilizan son fuertes para contrarrestar cualquier ataque. Al final de la prueba de penetración se realiza un reporte con todos los detalles de la auditoría, proponiendo a la alta dirección o gerencia de una organización las acciones que deben ser aplicadas para evitar o corregir cualquier infiltración de un ataque.

Las pruebas de penetración son el método que se permite como el único medio que es legal para para ser aplicado internamente en un sistema de una organización y todo esto es con el fin de identificar los riesgos después de que se haya probado la rastreabilidad de vulnerabilidades al aplicar las herramientas de apoyo, y que con esto sean minimizadas las amenazas. Para aprovechar al máximo las pruebas de penetración es necesario priorizar el esfuerzo entre la organización y el experto en pruebas de penetración (*pentester*) para llevar a cabo esta auditoría. Las pruebas de penetración deben tener un alcance adecuado, por lo que se debe aprovechar el conocimiento que la organización como cliente tiene, sobre las explotaciones de las fallas que se han encontrado dentro de la misma organización. Además esta información debe ser combinada con la experiencia y el conocimiento de la empresa a través de pruebas de penetración históricas.

RECOMENDACIONES

Se deben seguir los protocolos, reglas y políticas recomendadas por las fundaciones OWASP y la metodología abierta de Prueba de Seguridad (OSSTMM), para lograr tener un sistema interno seguro de una organización a prueba de infiltraciones, aplicando pruebas de penetración periódicas que incluyan el círculo de la seguridad informática, puesto que en las sombras ocultamente siempre habrá delincuentes informáticos que quieran violentar la seguridad implementada en los sistemas internos de las organizaciones o empresas protegidas.

Otra de las recomendaciones es la de implementar políticas de seguridad en base a las necesidades y exigencias de los de las altas direcciones de una empresa. Además se debe brindar capacitaciones en seguridad de la información a todos los involucrados. Debe de existir una restricción del uso de dispositivos de almacenamiento extraíbles que se conectan a través de puertos USB, como medida de prevención para evitar la propagación de virus o códigos maliciosos, implementando el uso de antivirus licenciado para contrarrestar la propagación de códigos maliciosos o malware.

REFERENCIAS BIBLIOGRÁFICAS

Bitdefender. (2023). *¿Qué es un Exploit? Prevención de Exploits*. Consumer Support. https://www.bitdefender.es/consumer/support/answer/22884/

Campderrós Vilà, Jaume (2019), *Ataques y vulnerabilidades web.* Dipòsit Digital de la Universitat de Barcelona. http://hdl.handle.net/2445/143419

Gómez González, I.C. (2012), *Diseño de Metodología para Verificar la Seguridad en Aplicaciones Web Contra Inyecciones SQL*. Universidad Militar Nueva Granada, Bogotá Colombia.

Hernández, M. (2022). *Pentesting con OWASP: fases y metodología*. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Incibe (Instituto Nacional de Ciberseguridad)(2023). *Google Dorks te ayuda a encontrar información sobre ti en la Red. Oficina de seguridad del internauta.* https://www.incibe.es/ciudadania/blog/google-dorks-te-ayuda-encontrar-informacion-sobre-ti-en-la-red.

Keep Coding. (2023). *¿Qué hace un pentester?. KeepCoding Tech School*. https://keepcoding.io/blog/que-hace-un-pentester/

Mendhurwar, S., y Mishra, R. (2021). *Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges*. Enterprise Information System.

Montero, V.H. (2005). *Técnicas de Penetration Testing*. CYBSEC Security System, Buenos Aires Argentina.

Ortega, K. (2022). *¿Qué tipos de pentesting existen?*. Saint Leo University, https://worldcampus.saintleo.edu/noticias/que-tipos-de-pruebas-de-penetracion-existen-en-seguridad-informatica

OSSTMM (Open Source Security Testing Methodology Manual). (2023). *Manual de la Metodología de Pruebas de Seguridad de Recurso Abierto (Open Source)*. https://www.ciberseguridad.eus/ciberpedia/vulnerabilidades/open-source-security-testing-methodology-manual-osstmm

OWASP (Open Web Application Security Project). (2017). *Estándar de Verificación de Seguridad en Aplicaciones 3.0.1*. OWASP. https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf

OWASP (Open Web Application Security Project). (2021). *Introducción: OWASP Top 10:2021*. OWASP. https://owasp.org/Top10/es/A00_2021_Introduction/

Sánchez Cano, G. (2018). *Seguridad Cibernética: Hackeo Ético y Programación defensiva*. Alfaomega Grupo Editor.

Saucedo, A.L.H., y Miranda, J.M. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica*, (1), 1-12.

Siahaan, A. P. U. (2016). Intrusion Detection System in Network Forensic Analysis and Investigation. *Journal of Computer Engineering*, 11(5), 1-18.

Sreenivasa Rao B., y Kumar N. (2012). Web Application Vulnerability Detection Using Dynamic Analysis With Peneteration Testing. *International Journal of Computer Science and Security*, (6), 1-12.

Tori, C. (2008). *Hacking Ético*. Mastroianni Impresiones.

Vañó Chic, J. (2014). *Exploits*. Universitat Oberta de Catalunya.

TABLA DE TRABAJO COLABORATIVO

Rol	Autor (es)
Conceptualización	Juan Manuel Bernal Ontiveros
Metodología	Margarita Bailón Estrada y Susan Alexandra Cervantes Cardenas, Anilu Flores Regalado
Software	No aplica

Validación	Juan Pedro Benítez Guadarrama y Susan Alexandra Cervantes Cardenas, Anilu Flores Regalado
Análisis Formal	Juan Manuel Bernal Ontiveros
Investigación	Juan Manuel Bernal Ontiveros y Margarita Bailón Estrada
Recursos	No aplica
Curación de datos	Juan Pedro Benítez Guadarrama y Susan Alexandra Cervantes Cardenas
Escritura - Preparación del borrador original	Juan Manuel Bernal Ontiveros, Margarita Bailón Estrada, Anilu Flores Regalado
Escritura - Revisión y edición	Juan Manuel Bernal Ontiveros y Juan Pedro Benítez Guadarrama