



UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

UTILIZACIÓN DE HERRAMIENTAS PARA
PRUEBAS DE PENETRACIÓN EN AUDITORÍAS
INFORMÁTICAS

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE
INGENIERA EN REDES

PRESENTA

MARIANA INÉS TORRES POZOS



SUPERVISORES

M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA
M.S.I. LAURA YÉSICA DÁVALOS CASTILLA
M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE
DR. JAIME SILVERIO ORTEGÓN AGUILAR
M.T.I. MELISSA BLANQUETO ESTRADA



CHETUMAL QUINTANA ROO, MÉXICO, JULIO DE 2019



UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO MONOGRÁFICO TITULADO
"UTILIZACIÓN DE HERRAMIENTAS PARA PRUEBAS DE PENETRACIÓN EN
AUDITORÍAS INFORMÁTICAS"

ELABORADO POR

MARIANA INÉS TORRES POZOS

BAJO SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y
APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:
INGENIERA EN REDES

COMITÉ SUPERVISOR

SUPERVISOR:


M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA

SUPERVISORA:


M.S.I. LAURA YESICA DÁVALOS-CASTILLA

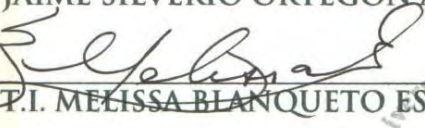
SUPERVISOR:


M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE

SUPERVISOR SUPLENTE:


DR. JAIME SILVERIO ORTEGÓN AGUILAR

SUPERVISORA SUPLENTE:


M.T.I. MELISSA BLANQUETO ESTRADA



RESUMEN.

Debido al incremento de ataques informáticos hacia sistemas, servidores, redes y sitios web, la capacitación en temas de seguridad va ganando relevancia con el fin de asegurar la integridad, disponibilidad y confidencialidad de los datos. La auditoría de seguridad informática nace con la finalidad de precautelar y poner a prueba las medidas de seguridad implementadas tanto en software como hardware. Esto trae retos al personal tanto del área de sistemas como de redes de una organización, por lo que se ven obligados a recibir capacitación oportuna en el campo para salvaguardar el activo más importante de la organización, la información.

Sin embargo, no solo es necesario estar al día en nuevas técnicas preventivas y correctivas de seguridad, sino que se requiere también la capacidad de pensar como el atacante, es aquí donde nace el hacking ético. Existe una distribución muy amplia de herramientas que permiten la capacitación formal de un experto en seguridad, mismo que al terminar su formación será llamado hacker ético.

El presente proyecto trata acerca de las herramientas que se emplean al momento de llegar a la etapa de una auditoría informática en la que se tendrá que aplicar diversas herramientas de penetración, ya sean de licencia gratuitas o de pago, con el fin de identificar los puntos débiles que un sistema o red empresarial pueda tener y de esa manera poder fortalecerlos. Este proyecto ha sido diseñado de tal forma que pueda guiar en el proceso de una auditoría industrial estándar, mostrando un buen listado de herramientas que puedan ser empleadas y sus funciones brindando un análisis detallado de un subconjunto de herramientas destacadas con la finalidad de ofrecer no solo una guía sino también un criterio formal del alcance de cada herramienta de software presentada.

Además, se lleva a cabo una recopilación de algunas herramientas, juntando la información general que se puede obtener de ellas, tal como lo es la forma de usarse, sus orígenes y sus licencias, otorgando de esta manera un análisis más detallado de algunas de las herramientas que se toman a consideración en el presente proyecto. Cabe recalcar que los procedimientos y características presentadas en la investigación son expuestos únicamente con propósitos educativos.

AGRADECIMIENTOS.

En esta vida todo tiene un principio y su fin, hoy es el fin de una meta, una meta que parecía muy lejana, pero con esfuerzo y perseverancia hoy ha culminado, tengo tanto que agradecer pues me siento muy afortunada de poder estar aquí y compartir este momento con seres tan valiosos, es por ello que debo agradecer principalmente a Dios por todas las bendiciones recibidas, a mi familia por el apoyo brindando, por las palabras de aliento, y por estar siempre presentes, inclusive a pesar de la distancia.

Agradezco al profesor Vladimir Cabañas, director de monografía por el apoyo brindando durante esta investigación.

En general a todas las personas especiales que han estado en mi vida.

DEDICATORIA.

Con todo mi cariño y orgullo dedico este trabajo a todas aquellas personas que estuvieron a mi lado y me supieron apoyar para la consecución de esta meta, en especial a:

Mis padres Alberta María Pozos y José Humberto Torres por su incesable lucha por darme lo mejor, por sus consejos, por todo su apoyo y en general por ser todo para mí.

CONTENIDO.

Índice de Tablas	v
Índice de Figuras	v
CAPÍTULO 1	1
1.1 Introducción	1
1.2 Objetivo general.....	2
1.3 Objetivos particulares	2
CAPÍTULO 2 MARCO DE REFERENCIA.	3
2.1 Pruebas de Penetración (<i>Pentesting</i>)	3
2.2 ¿Quién realiza las pruebas de Penetración?	3
2.3 Metodologías para la realización de las pruebas de Penetración.....	4
2.3.1 Information System Security Assessment Framework (ISSAF)	4
2.3.2 Open Source Security Testing Metodology Manual (OSSTMM).....	6
2.3.3 <i>Open Web Application Security Project</i> (OWASP)	7
2.4 Fases del Hacking Ético.	7
2.4.1 Reconocimiento (<i>Footprinting</i>)	8
2.3.2 Escaneo.....	9
2.3.3 Obtención de Acceso.	9
2.3.4 Elaboración de Informe.	9
2.3.5 Presentación del Informe.	10
2.4 Herramientas por categoría.	10
2.5 Descripción de algunas herramientas de penetración.....	13
Netsparker.	13
Metasploit.	14
Wireshark.	15

Kali Linux.....	15
Nessus.....	16
Burp suite.....	16
Cain & Abel.....	17
Zed Attack Proxy(ZAP).....	17
John the Ripper.....	19
Sqlmap.....	20
<i>Social Engineer Toolkit</i>	20
<i>Network Mapper (Nmap)</i>	20
Capítulo 3 DESARROLLO.....	22
3.1 Descripción.....	22
3.2 Análisis de herramientas destacadas.....	22
3.2.1 Etapa de Reconocimiento.....	22
3.2.2 Etapa de Escaneo.....	26
3.2.3 Etapa de Explotación.....	38
Capítulo 4 CONCLUSIONES.....	47
Referencias.....	50

Índice de Tablas

Tabla 1 Listado de herramientas por categoría.....	12
Tabla 2 Cantidad de herramientas por categoría.....	13
Tabla 3 Estados de Puertos en Nmap.....	28

Índice de Figuras

Figura 1 Usando Wireshark para capturar paquetes.....	23
Figura 2 Mostrando los paquetes que aparecen en tiempo real.....	24

Figura 3 Mostrando el tráfico en Wireshark.....	24
Figura 4 Los controles de Wireshark, enumerando desde del 1 al 15.	25
Figura 5 Submenú Opción 1 de SET.	41

CAPÍTULO 1

1.1 Introducción

El presente proyecto consiste en una investigación documental sobre las herramientas informáticas conocidas comúnmente como de hacking y que se utilizan de manera recurrente en los procesos de auditoría informática.

La información que las organizaciones poseen, administran, generan, almacenan o cualquier otro tratamiento que le den, es de gran valor tanto para la misma organización, como para los que participan directa o indirectamente con ella tales como clientes, proveedores y usuarios. Es por ello por lo que la protección de la información en las redes y sistemas de las grandes corporaciones es tan importante, ya que dichas empresas almacenan datos determinantes que pudieran definir el rumbo de su desarrollo y se encuentran en peligro por la ciberdelincuencia. El Reporte Anual de Ciberseguridad (Cisco, 2018), describe el aumento de binarios maliciosos aprovechando el uso de algunas comunicaciones de red, pasando de un 20% en noviembre del 2016, a un 80% en octubre del 2017.

Una auditoría informática consiste en llevar un control, de forma periódica, acerca de la seguridad con el que un sistema o una red cuentan, por lo que sólo puede ser realizado por profesionales formados para ello de manera específica. La función de dichos profesionales consiste en averiguar las vulnerabilidades de un sistema y en reforzar su seguridad a partir de los resultados que se obtengan de la auditoría.

El proceso de una auditoría informática requiere, además de ser realizada por un profesional en la materia, de la implementación de herramientas que ayuden al profesional a lograr el objetivo de averiguar las vulnerabilidades de un sistema, de esta forma, con las herramientas necesarias se puede implementar una solución y reforzar la seguridad.

Un tipo de las herramientas que se usan para las auditorías informáticas son las Herramientas de Pentesting, mismas que consisten en atacar diversos entornos con la intención de descubrir

fallos o vulnerabilidades de seguridad en los sistemas informáticos, para que se pueda prevenir ataques externos hacia los equipos o sistemas inspeccionados.

1.2 Objetivo general

Revisión y análisis documental sobre tipos de herramientas de *Pentesting* y su eficiencia utilizadas actualmente en los procesos de auditoría de seguridad informática.

1.3 Objetivos particulares

- i. Describir el proceso general de una auditoría en seguridad informática.
- ii. Determinar el objetivo de realizar *pentesting* en una auditoría de seguridad informática.
- iii. Identificar y determinar algunas de las principales herramientas para realizar *pentesting* dentro del proceso de auditoría en seguridad informática
- iv. Documentar una metodología de auditoría en seguridad informática describiendo el funcionamiento de las herramientas de *pentesting* seleccionadas.
- v. Comparar las herramientas descritas y asociarlas a sus usos más adecuados dentro del proceso de auditoría informática.

1.4 Alcance

La investigación documental abarca las principales herramientas utilizadas en las diferentes etapas del proceso de *pentesting* que se utiliza en las auditorías de seguridad informática. Las herramientas serán seleccionadas de un conjunto de recursos públicos que gozan de prestigio internacional

CAPÍTULO 2 MARCO DE REFERENCIA.

2.1 Pruebas de Penetración (*Pentesting*)

Las pruebas de penetración o *pentesting*, de acuerdo con la definición del libro *Penetration Testing, A Hands-On Introduction to Hacking* (Weidman, 2014), es una práctica para poder poner a prueba un sistema informático, una red o aplicación web para poder encontrar vulnerabilidades que un atacante podría explotar.

El principal objetivo de las pruebas de penetración consiste en determinar las debilidades de seguridad. Una prueba de penetración también puede ser utilizado para probar el cumplimiento de la política de seguridad de una organización, la conciencia de seguridad de sus empleados y la capacidad de la organización para identificar y responder a los incidentes de seguridad.

2.2 ¿Quién realiza las pruebas de Penetración?

Las pruebas de penetración pueden ser realizadas por un recurso interno calificado o un tercero calificado, es decir, debe ser un experto en sistemas informáticos y estar muy familiarizado con la programación informática, la creación de redes y sistemas operativos. Otro requisito es el conocimiento profundo orientado a plataformas como Windows y Unix. Además, debe poseer cualidades como la paciencia, la persistencia y la perseverancia debido a la cantidad de tiempo y el nivel de concentración necesario que requieren para realizar la mayoría de los ataques, comprometer los sistemas y obtener sus resultados.

Si se están utilizando los recursos internos para llevar a cabo pruebas de penetración, esos recursos deben ser *pentesters* experimentados. Los individuos que realizan pruebas de penetración deben estar separados del ambiente que está siendo testeado.

La mayoría de los encargados de realizar las pruebas de penetración son los hackers éticos que con su conocimiento de las áreas de seguridad o relacionadas a ella, están motivados en determinar lo que un atacante malicioso puede ver en el sistema o en la red, hay que recalcar

que un hacker ético no necesariamente tiene un fuerte control sobre las contramedidas que pueden prevenir los ataques.

2.3 Metodologías para la realización de las pruebas de Penetración.

Las metodologías para la realización de pruebas de Penetración en Auditorías Informáticas, de acuerdo a lo referenciado en la tesis "Análisis de las herramientas para el proceso de auditoría de seguridad informática utilizando Kali Linux" (Cedeño, 2015) son aquellos conjuntos de métodos, pasos y guías a seguir, con el fin de que se realice una correcta aplicación de las herramientas a utilizar en la Auditoría.

Existen varias metodologías que el auditor informático puede seguir, mismas que aseguran la obtención de los objetivos planteados a fin de conocer las vulnerabilidades del sistema. Estas metodologías engloban un conjunto de áreas y pasos que hacen que un hacker ético pueda prestar sus servicios, asegurando la reputación profesional y personal, tanto del hacker como la de la compañía a la que representa.

Existen tres metodologías generales que sirven y funcionan para el procedimiento necesario al momento de realizar las Pruebas de Penetración en Auditorías Informáticas, mismas que se detallan a continuación:

2.3.1 Information System Security Assessment Framework (ISSAF)

Esta metodología fue desarrollada por oissgroup.com (Oisssg, s.f.) y se enfoca en la evaluación de la seguridad de redes, sistemas y aplicaciones de control. Está compuesta por tres áreas de enfoque y define 9 pasos como parte de su ciclo, tal como se define a continuación:

- a) **Planeación y Preparación.** En esta fase se inicia con la Metodología, identificando los usuarios, determinar el alcance y enfoque del método y definir casos específicos de actuación con vías de escalada.
- b) **Evaluación.** En esta fase se llevan a cabo 9 pasos en concreto:
 1. Recopilación de Información.
 2. Mapeo de Red.
 3. Identificación de Vulnerabilidades.

4. Penetración.
 5. Obtención de accesos y privilegios.
 6. Detalles adicionales.
 7. Comprometer a usuarios y sitios remotos.
 8. Acceso para mantenimiento.
 9. Canales encubiertos.
- c) **Reporte, limpieza y destrucción de artefactos.** Al finalizar la fase de Evaluación se debe levantar un reporte que, como mínimo, debe contener:
1. Sumario.
 2. Alcance del proyecto.
 3. Herramientas usadas.
 4. Fechas y tiempo de las pruebas realizadas al sistema.
 5. Cada salida individual de las pruebas realizadas.
 6. Una lista de las vulnerabilidades identificadas, incluyendo sus recomendaciones para solventarlas.
 7. Una lista de acciones para tomar.

De igual forma, toda la información creada o almacenada en el sistema debe ser removida, sin embargo, si esta, por alguna razón no puede ser eliminada, debe mencionarse en el reporte, incluyendo su localización.

Como se puede observar, esta metodología posee puntos a favor y puntos en contra. Entre las ventajas tenemos el hecho de que los pasos establecidos le permiten al auditor informático tener una guía consecutiva de las pruebas que debe realizar y el orden en que debe hacerlas, para evitar obviarlas o repetirlas.

Sin embargo, entre las desventajas se encuentra que la última fase no posee todo el detalle requerido y las sugerencias no están actualizadas, debido a que la eliminación de los artefactos útiles para la prueba no forma parte de las nuevas prácticas de seguridad, las cuales indican que las mismas deben quedarse alojadas en los sistemas de pruebas, además la línea de flujo en un solo sentido no permite retroalimentación o readecuación de objetivos dada la detección de alguna vulnerabilidad.

A criterio personal, la fase de destrucción de pruebas puede quedar a consideración de las políticas de seguridad de la compañía auditada, con lo cual podrían destruirse.

2.3.2 Open Source Security Testing Methodology Manual (OSSTMM)

Esta metodología es considerada como un estándar para los auditores informáticos, ya que su procedimiento es muy completo y contiene un buen conjunto de pruebas que ofrecen un vasto número de herramientas para la elaboración de reportes.

Es un estándar profesional para el testeo de seguridad en cualquier entorno desde el exterior al interior. Como cualquier estándar profesional, incluye los lineamientos de acción la ética del pentester profesional, la legislación sobre testeo de seguridad y conjunto integral de pruebas.

El objetivo de este manual es crear un método aceptado para ejecutar una prueba de seguridad minucioso y completo.

Lo más importante en esta metodología es que los diferentes pruebas son evaluados y ejecutados donde sean aplicables, hasta arribar a los resultados esperados dentro de un período de tiempo determinado. Solo de esa manera el aplicador, habrá ejecutado la prueba en conformidad con el modelo OSSTMM, y por ello, el informe podrá ser considerado mínimamente exhaustivo.

El OSSTMM debe cumplir con las reglas establecidas en las diferentes leyes tanto Internacionales, Federales, Locales, Industriales y Políticas establecidas en la organización.

Cada una de las acciones debe proveer no violar alguna ley, reglamento o política y cada una de las actividades debe ser coordinadas con la organización que requiere la implementación de este tipo de pruebas a su seguridad.

También contempla el cumplimiento de normas y mejores prácticas como las establecidas en el NIST, ISO 27001-27002 e ITIL entre otras. Lo que hace de este manual uno de los más completos en cuanto a la aplicación de pruebas a la seguridad de la información de las organizaciones.

2.3.3 Open Web Application Security Project (OWASP)

El proyecto de seguridad de aplicaciones Web abierta (OWASP) es una comunidad conformada por voluntarios, permite a las organizaciones desarrollar, comprar y mantener aplicaciones que pueden ser confiables. Todas las herramientas OWASP, documentos, foros y capítulos son gratuitas y abiertas a cualquier persona interesada en la mejora de la seguridad de aplicaciones.

OWASP es un nuevo tipo de organización sin fines de lucro que brinda información imparcial, práctica y rentable sobre seguridad en aplicaciones. Al igual que muchos proyectos de software de código abierto, OWASP produce muchos tipos de materiales en una manera abierta y colaborativa.

OWASP en particular, se encuentra enfocado en ayudar a las personas a comprender: ¿Qué?, ¿Por qué?, ¿Cuándo?, ¿Dónde? Y ¿cómo? Testear sus aplicaciones Web y no sólo proporciona una lista de control simple o prescripción que deben abordarse. El resultado de este proyecto es un marco de pruebas completa, de la que otros puedan construir sus propios programas de pruebas o calificar los procesos de otras personas.

Muchos expertos de la industria y los responsables de la seguridad del software en algunas de las empresas más grandes del mundo están validando el marco de pruebas. Este marco ayuda a las organizaciones a probar sus aplicaciones web con el fin de construir software fiable y seguro, en lugar de simplemente poner de relieve las áreas de debilidad, aunque este último es ciertamente un subproducto de muchos de los guías y listas de control de OWASP.

En muchas ocasiones, una metodología requiere ser acompañada de documentos que sustenten en pasos prácticos y concretos, parte del contenido de la misma, haciendo de estos una referencia obligada a la hora de realizar un testeado de seguridad.

2.4 Fases del Hacking Ético.

Si bien existen metodologías que se pueden seguir, en caso de no seleccionarlas se han definido, de forma general en el hacking ético, cinco fases para realizar este proceso, las cuales se describen a continuación:

2.4.1 Reconocimiento (*Footprinting*)

Se trata de la fase de recopilación de información, tanto a través de datos obtenidos con una interacción directa con el sistema objetivo, llamada reconocimiento activo; o la revisión de documentación externa pública sin interactuar directamente con el sistema (esto se conoce con el nombre de reconocimiento pasivo).

En esta etapa se realizan las siguientes pruebas:

Reconocimiento Activo.

- Técnicas de Ingeniería social a los empleados de la compañía, como intimidación, *name-dropping*.
- Barridos de Ping.
- Mapeo de Red para determinar la existencia dispositivos de borde.
- *Banner Grabbing*, conexión a un puerto específico de una aplicación para obtener información del sistema operativo y otros servicios corriendo sobre la computadora.

Reconocimiento Pasivo.

- Recuperación de Información desde la basura (*dumpster diving*).
- Recuperación de Información disponible desde Internet como blogs, revistas, redes sociales (Facebook, Twitter, LinkedIn, Google plus, etc.), página web principal de la institución y utilizando la información obtenida de motores de búsqueda como Google.
- Consulta de Directorios en internet (DNS y bases de datos *Who-is*).

Ahora bien, no importa el tipo de información que se debe recopilar en esta etapa, ya que debe ser toda aquella que sea posible. Esta es la fase en donde se conoce al que se encuentra al otro lado del sistema y cualquier información relacionada puede ser de utilidad.

Para continuar con la presente etapa, lo siguiente es una lista en que debemos conseguir como objetivo:

- Estructura de la organización, incluyendo detalles de alto nivel, departamentales y tablas de organización jerárquica (directores, jefes, líderes de proyectos, etc.).
- Infraestructura organizacional, incluyendo rango de direcciones IP y topología de red.
- Tecnología utilizada, incluyendo plataforma de hardware y paquetes de software.
- Direcciones de correo electrónico de empleados.
- Auspiciantes, colaboradores y empresas afiliadas de la Organización.

- Ubicación física de la organización o de sus departamentos.
- Números de teléfono.

2.3.2 Escaneo.

En esta fase se procede a realizar el reconocimiento del host que se encuentran activos en las diferentes redes de la compañía, para luego comenzar a revisar los puertos y las aplicaciones que están escuchando por dichos puertos, identificar servicios y sistemas operativos para detectar vulnerabilidades de estos. Posterior a ello poder elaborar un diagrama de red y de equipos vulnerables.

Dentro de esta fase, aparece una sub-fase llamada enumeración, en donde el hacker ético se encarga de aprovechar las debilidades encontradas para obtener más información del cliente, como cuentas de usuarios, recursos compartidos, hashes de claves, entre otras. Algunos autores juntan esta fase con la de reconocimiento activo, debido a que se trabaja directamente con conexiones vinculadas al sistema objetivo.

2.3.3 Obtención de Acceso.

En esta fase, que también es conocida como "explotación" o "hacking", es donde se ejecutan *exploits* que buscan aprovechar la vulnerabilidad de un sistema para conseguir un comportamiento o lograr acceder a más información. Es en esta fase es donde se utilizan los *frameworks* de explotación.

2.3.4 Elaboración de Informe.

El hacker ético se encarga de elaborar un documento final con los hallazgos encontrados debido a una baja o nula seguridad en los sistemas, indicando sugerencias para la corrección de las debilidades encontradas. Además del informe detallado y técnico, se elabora un resumen ejecutivo completo donde se especifican las vulnerabilidades encontradas de forma general.

La parte más difícil del período de auditoría es el Informe Final, por el éxtasis de las pruebas y la obtención de resultados que pueden hacernos recopilar información de forma desordenada. Es por ello por lo que es recomendable realizar lo siguiente:

- Crear un solo repositorio para el proyecto de auditoría y dentro de esta carpeta superior, crear una carpeta con cada fase de la auditoría.
- Llevar una bitácora o registro de las pruebas realizadas con fecha.

- Capturar imágenes y/o video, de las pruebas que se realizan o los comandos que se aplican.
- Llevar un registro de los hallazgos, distinto a la bitácora, ya que aquí solo se detallará las pruebas que hallamos realizado y hayan detectado alguna vulnerabilidad.
- Usar herramientas de documentación.
- Usar una plantilla para realizar el informe.

2.3.5 Presentación del Informe.

Como última fase, se debe presentar y entregar los documentos elaborados, de acuerdo con el protocolo burocrático de la compañía cliente y de la que está realizando el hacking ético.

Existe una variación cuando se sigue el proceso de hacking, se trata de una etapa llamada en algunos libros como "Mantener acceso" o "Post Explotación", ésta se ubica después de la fase de explotación, sin embargo, como podemos percatarnos no forma parte del ciclo de vida del hacking ético.

Para llevar a cabo las primeras fases el hacker ético debe valerse de herramientas de software que le permitan la detección de vulnerabilidades en el sistema, es decir, herramientas de penetración, de las cuales más adelante realizaré una descripción a algunas de las más utilizadas generalmente por los profesionales.

2.4 Herramientas por categoría.

Las Herramientas de Penetración usadas en la Auditoría Informática pueden ser clasificadas por categoría, de tal forma que se identifique las características que varían entre las diferentes herramientas y puedan clasificarse el objetivo o función de cada una de ellas. A continuación, describiré las diferentes categorías en las que pueden clasificarse las herramientas:

- **Recopilación de Información (*Information Gathering*).** Contiene un conjunto de herramientas que permiten la detección de información relacionada con lo siguiente:
 - ✓ Servidores de Nombres de Dominio (DNS).
 - ✓ Sistema de detección y prevención de Intrusos (IDS/IPS)
 - ✓ Escáner de red.
 - ✓ Escáner de sistema operativo.
 - ✓ Ruteo.
 - ✓ *Secure Socket Layer (SSL)*, protocolo que provee de

- ✓ seguridad a la comunicación en una red de computadoras.
 - ✓ SMB, protocolo de la capa de aplicación que permite compartir archivos y recursos.
 - ✓ VPN o Red Privada Virtual.
 - ✓ VoIP.
 - ✓ SNMP.
 - ✓ Correo electrónico.
- **Análisis de Vulnerabilidades (*Vulnerability Analysis*)**. Provee de herramientas para la evaluación de vulnerabilidades sobre un sistema, así como herramientas para evaluar redes Cisco y evaluar vulnerabilidades de servidores de base de datos.
 - **Husmeando & envenenando (*Sniffing & Spoofing*)**. Incluye herramientas para el rastreo de red, tráfico web y herramientas para la suplantación de identidad en la red.
 - **Decodificación de Contraseñas (*Password Attacks*)**. Provee herramientas para el descifrado de contraseñas con conexión y sin conexión.
 - **Aplicaciones Web (*Web Applications*)**. Contiene software como escáner de gestión de contenido, intrusión a base de datos, fuzzers de aplicaciones web y otros escáneres de vulnerabilidades web.
 - **Herramientas de Explotación (*Exploitation Tools*)**. Provee programas que permiten realizar la intrusión hacia redes, servidores web, base de datos, entre otros.
 - **Herramientas para la elaboración de reportes (*Reporting tools*)**. Dispone de las herramientas que agilitan y permiten almacenar los resultados de las pruebas de intrusión realizadas.

Existen algunas herramientas que coinciden en varias categorías, debido a su amplio alcance, por lo que no debe ser extraño encontrarnos con algunas herramientas de penetración que cuentan con dos o más de las categorías descritas anteriormente. Por supuesto que esto

puede representar una ventaja sobre otras herramientas, debido al mayor alcance que abarca, sin embargo, en ocasiones el alcance máximo no es necesario, dependerá de las necesidades y los objetivos que el Hacker Ético profesional quiera alcanzar. En la siguiente tabla, podemos visualizar el número de herramientas y a que categoría corresponden siguiendo la numeración anterior:

Tabla 1 Listado de herramientas por categoría.

Herramientas	1	2	3	4	5	6
1. Netsparker		X				
2. Metasploit						X
3. Wireshark	X		X			
4. Kali Linux	X	X	X	X		X
5. Burp Suite			X	X	X	
6. Cain & Abel			X	X		
7. Zed Attack Proxy		X			X	
8. John The Ripper				X		
9. Sqlmap		X			X	X
10. Nessus		X				X
11. Social Engineer Toolkit	X					
12. Nmap	X	X				

Derivado de los resultados obtenidos en la tabla de comparación, podemos determinar el número de herramientas que desarrollan las diversas fases de procedimientos, mismos resultados que podemos ver de la siguiente manera:

Tabla 2 Cantidad de herramientas por categoría

Categoría	Cantidad de Herramientas
1. Recopilación de Información	4
2. Análisis de Vulnerabilidades	6
3. Sniffing & Spoofing	4
4. Decodificación de Contraseñas	4
5. Aplicaciones Web	3
6. Herramientas de Explotación	4

2.5 Descripción de algunas herramientas de penetración

Actualmente existe una gran variedad de Herramientas de Penetración que son usadas para la Auditoría Informática, mismas que contienen diferentes características y pueden alcanzar diversos objetivos, de acuerdo con las necesidades del Hacker Ético. A continuación, describiré algunas de las herramientas más comunes y generales que se aplican por los profesionales del hacker ético en las auditorías informáticas.

Netsparker.

Tal cómo podemos observar en la página web <https://www.netsparker.com/> (Shay Chen, 2019), esta herramienta trata de un escáner de seguridad de aplicaciones web, totalmente automatizado. Por su configuración se vuelve fácil de usar, además, implementa una tecnología avanzada a la que se le llama "*Proof Based Scanning*", misma que sirve para identificar la Inyección de SQL, Secuencias de Comandos entre Sitios (XSS), entre otras vulnerabilidades en aplicaciones web, servicios web y API web.

El escáner de vulnerabilidad web Netsparker también tiene herramientas integradas de pruebas de seguridad, generador de informes y se puede integrar fácilmente en el SDLC, *DevOps* y otros entornos.

El funcionamiento de Netsparker es independientemente de la plataforma y de la tecnología con la que están contruidos, por lo que puede encontrar e informar de las vulnerabilidades del sistema en diferentes entornos.

Además de informar de las vulnerabilidades encontradas, también produce una prueba de concepto que sirve para confirmar que no sean falsos positivos.

Metasploit.

Tal cómo podemos observar en la página web <https://openwebinars.net/blog/que-es-metasploit/> (Rizaldos, 2018), esta herramienta trata de un proyecto de ciberseguridad, de código abierto, que permite a los hackers éticos profesionales usar las diferentes herramientas de prueba de penetración para poder descubrir vulnerabilidades de software remotas. También funciona como una plataforma de desarrollo de módulos de exploit.

Además, con Metasploit se pueden realizar las siguientes fases:

- **Interacciones previas al objetivo:** Este paso define todas las actividades previas al objetivo y las definiciones de alcance, básicamente todo lo que necesita discutir con un cliente antes de que comience la prueba.
- **Recopilación de inteligencia:** En esta fase se recopila información sobre el objetivo sometido a prueba, al conectarse al objetivo directa o pasivamente, sin conectarse al objetivo en absoluto.
- **Modelado de amenazas:** Esta fase consiste en hacer coincidir la información descubierta con los activos para encontrar las áreas con el nivel de amenaza más alto.
- **Análisis de vulnerabilidad:** Esta fase implica encontrar e identificar vulnerabilidades conocidas y desconocidas y validarlas.
- **Explotación:** Esta fase funciona aprovechando las vulnerabilidades descubiertas en la fase anterior. Esto normalmente significa que estamos tratando de obtener acceso al objetivo.
- **Después de la explotación:** En esta fase se realizan las tareas reales que se deben realizar en el objetivo, mismas que implican descargar un archivo, apagar un sistema, crear una nueva cuenta de usuario en el destino, etc. Además, esta fase describe lo que necesita hacer después de la explotación.
- **Informes:** En esta fase se incluye un resumen de los resultados de la prueba en un archivo y las posibles sugerencias y recomendaciones para corregir las debilidades actuales en el objetivo.

Wireshark.

Tal cómo podemos observar en la página web <https://www.wireshark.org/> (Combs, 2019), esta herramienta se basa de código abierto para perfilar el tráfico de red y analizar paquetes. A esta herramienta se le suele denominar como "analizador de red", "analizador de protocolo de red" o "rastreador".

Esta herramienta es comúnmente utilizada para la solución de problemas en la red, la examinación de problemas de seguridad, implementaciones de protocolo de depuración y la memorización de protocolos de la red.

Además, con Wireshark se pueden examinar los detalles del tráfico en una variedad de niveles que van desde la información de nivel de conexión a los bits que forman un solo paquete. La captura de paquetes puede proporcionar al administrador de la red información sobre paquetes individuales, como el tiempo de transmisión, el origen, el destino, el tipo de protocolo y los datos del encabezado. Esta información puede ser útil para evaluar eventos de seguridad y solucionar problemas de dispositivos de seguridad de red.

Kali Linux.

Tal como podemos observar en la página web <https://www.kali.org> (N.A., Our Most Advanced Penetration Testing Distribution, Ever., 2019) esta herramienta trata de una herramienta basada en GNU/Linux Debian, destinada para auditorías de seguridad y pruebas de penetración avanzadas. En su plataforma se incluyen las funciones de análisis forense, ingeniería inversa y evaluación de vulnerabilidades.

Su objetivo es la búsqueda de los límites y fisuras en la seguridad de las redes y sistemas informáticos.

De igual forma sirve para tareas de análisis forense, con lo que se puede descubrir el lugar por el cual ha sido atacado un sistema informático, además de encontrar posibles rastros de su atacante.

Nessus.

Tal cómo podemos observar en la página web <https://www.tenable.com/products/nessus>, (N.A., The Nessus Family, 2019) esta herramienta trata de un escáner de vulnerabilidades de red de código abierto que utiliza la arquitectura de vulnerabilidades y exposiciones comunes para un fácil enlace entre las herramientas de seguridad compatibles. Nessus emplea el *Nessus Attack Scripting Language* (NASL), un lenguaje simple que describe amenazas individuales y posibles ataques.

La función de Nessus es realizar un estudio completo y eficaz, capaz de encontrar las vulnerabilidades que se encuentren a lo largo de todos los puertos que lleguen a tener las computadoras que formen parte del sistema.

Una diferencia, con la que cuenta Nessus de otras herramientas, es que no hace suposiciones sobre la configuración de su servidor, ya que no supone que, por ejemplo, el puerto 80 debe ser el único servidor web. De igual forma, proporciona un lenguaje de scripting para que escriba pruebas específicas de un sistema, una vez que se familiarice con la herramienta. También proporciona una interfaz de complemento, entre otros. Estos enchufes suelen ser específicos para detectar un virus o vulnerabilidad común.

Esta herramienta cuenta con Información actualizada sobre nuevas vulnerabilidades y ataques ya que su proveedor actualiza la lista de las vulnerabilidades que se deben verificar diariamente para minimizar la posibilidad de una vulnerabilidad que aparezca en ocasiones.

Burp suite.

Se trata de una plataforma integrada para la realización pruebas de seguridad en aplicaciones web. Cuenta con diversas herramientas que trabajan a fin de respaldar todo el proceso de prueba, desde el mapeo inicial y el análisis de la superficie de ataque de una aplicación, hasta encontrar y explotar vulnerabilidades de seguridad.

Esta herramienta se encuentra diseñada para un uso práctico, en el que el usuario controla las acciones que se realizan. Cuenta con un núcleo de flujo de trabajo, impulsado por el usuario de Burp, mismo que cuenta con la capacidad de pasar solicitudes HTTP entre las herramientas de Burp para realizar tareas específicas. Puede enviar mensajes desde la

pestaña Intercepción de proxy, el historial de Proxy, el mapa del sitio y en cualquier otro lugar de Burp, siempre y cuando se vean mensajes HTTP.

Cain & Abel.

Se trata de una herramienta usada para comprobar la seguridad de las redes y recuperar contraseñas, su función la realiza usando el diccionario, fuerza bruta, *sniffing*, ataques criptoanálisis, etc.

Esta herramienta permite la recuperación de varios tipos de contraseñas, mediante el rastreo de la red, descifrando contraseñas cifradas a través de ataques de Diccionario, fuerza bruta y criptoanálisis, grabando conversaciones VoIP, descodificando contraseñas codificadas, recuperando claves de red inalámbrica, revelando cuadros de contraseñas, descubriendo contraseñas almacenadas en caché y analizando el enrutamiento protocolos.

El programa no hace *exploit* de ninguna vulnerabilidad software, en cambio lo que hace es cubrir algunos aspectos de seguridad presentes en los protocolos estándares, métodos de autenticación y mecanismos de caché.

Zed Attack Proxy(ZAP).

Tal cómo podemos observar en la página web <https://www.zaproxy.org/> (GitHub, s.f.), esta herramienta trata de una herramienta elaborada por OWASP (*Open Web Application Security Project*), siendo una de las herramientas de seguridad gratuitas más populares del mundo, mantenida activamente por cientos de voluntarios internacionales. Es un escáner de seguridad de aplicaciones web de código abierto.

Esta herramienta puede ayudar a encontrar automáticamente vulnerabilidades de seguridad en sus aplicaciones web mientras desarrolla y prueba sus aplicaciones. También realiza *pentesters* experimentados, para usar en pruebas de seguridad manuales.

ZAP ofrece diferentes funcionalidades para analizar las vulnerabilidades de las aplicaciones, tales como spider, escaneos pasivos y activos, *fuzzer*, fuerza bruta, entre otros. A continuación, se describen algunas de dichas funcionalidades:

- **Escaneo Pasivo:** El análisis pasivo se puede usar para analizar aplicaciones web y permite evaluar la vulnerabilidad al detectar el tráfico de red normal y actuar como un proxy entre el servidor y el navegador.
La exploración pasiva no ataca ni interfiere con el cliente y el servidor, sino que analiza la solicitud - respuesta desde y hacia el servidor para identificar vulnerabilidades.
- **Spider:** Esta función explora y crea, automáticamente, la estructura de una aplicación web con la lista de todos los recursos URL encontrados. Para cada URL, ZAP crea una solicitud para obtener el recurso y luego analiza la respuesta, descubriendo hipervínculos. Para usar Spider es necesario especificar una URL inicial o un subgrupo de URLs.
- **Escaneo Activo:** El escaneo activo intenta encontrar agujeros de seguridad simulando ataques reales conocidos contra aplicaciones web de destino. El escaneo activo debe usarse solo con sus propias aplicaciones. Con ZAP es posible seleccionar una lista de recursos utilizados anteriormente y realizar ataques activos sobre ellos para estar al tanto de las vulnerabilidades conocidas.
La exploración activa proporciona una lista más amplia de vulnerabilidades y, combinada con Spider y la exploración pasiva, puede mostrar todas las vulnerabilidades que ZAP puede reconocer, incluidas las vulnerabilidades de alto riesgo.
- **Fuzzer:** Esta función permite enviar un rango de cadenas aleatorias no válidas e inesperadas para descubrir agujeros de seguridad en la aplicación de destino. ZAP permite eliminar cualquier solicitud utilizando cadenas de una lista de archivos de texto que contienen entradas. Los usuarios pueden agregar archivos manualmente o mediante la aplicación para ampliar el rango de cadenas disponibles.
- **Fuerza Bruta:** La función de Fuerza Bruta no se usa para ataques de fuerza bruta en campos de autenticación, sino que ayuda a encontrar archivos o directorios de la aplicación de destino. ZAP contiene archivos con listas de nombres y directorios, utilizándolos para intentar acceder a los recursos directamente, en lugar de confiar en encontrar enlaces a ellos. Un ataque de fuerza bruta solo requiere el conocimiento de la aplicación web de destino y el archivo asociado con la lista de nombres.

Otras funcionalidades son *HttpSession*, *Param*, *WebSockets*, entre otras.

John the Ripper.

Tal cómo podemos observar en la página web https://www.ecured.cu/John_The_Ripper (Acosta, N.A.), esta herramienta trata de una herramienta que permite crackear diferentes tipos de hashes para obtener contraseñas en base a distintos mecanismos de crackeo, incluyendo ataques por fuerza bruta mediante diccionario.

Esta herramienta se usa comúnmente en empresas para detectar contraseñas débiles que podrían poner en riesgo la seguridad de la red, así como otros fines administrativos. El software puede ejecutar una amplia variedad de técnicas de descifrado de contraseñas en las distintas cuentas de usuario en cada sistema operativo y puede ejecutarse mediante secuencias de comandos para ejecutarse local o remotamente.

Además, cuenta con otras funciones, entre las cuales se encuentran las siguientes:
Optimizado para muchos modelos de procesadores.

- Funcionamiento en diversas arquitecturas y sistemas operativos.
- Ataques de diccionario y por fuerza bruta.
- Se trata de un software de Código Abierto.
- Permite definir el rango de letras que se usará para construir las palabras y las longitudes.
- Permite parar el proceso y continuarlo más adelante.
- Permite incluir reglas en el diccionario para decir cómo han de hacerse las variaciones tipográficas.

Esta herramienta cuenta con un diccionario con palabras que pueden ser contraseñas típicas, y las va probando todas. Para cada palabra, la cifra y compara con el hash a descifrar. Si coinciden, es que la palabra era la correcta. Esto funciona bien porque la mayor parte de las contraseñas que usa la gente son palabras de diccionario. Sin embargo, John the Ripper también prueba con variaciones de estas palabras: les añade números, signos, mayúsculas y minúsculas, cambia letras, combina palabras, etc. Además, ofrece el típico sistema de fuerza bruta en el que se prueban todas las combinaciones posibles, sean palabras o no. Éste es el sistema más lento, y usado sólo en casos concretos, dado que los

sistemas anteriores (el ataque por diccionario) ya permiten descubrir muy rápidamente las contraseñas débiles.

Sqlmap.

Tal cómo podemos observar en la página web <https://www.solvetic.com/tutoriales/article/1615-sqlmap-herramienta-de-inyecci%C3%B3n-de-sql-y-ethical-hacking-de-bases-de-datos/> (Culoccioni, 2015), esta herramienta trata de una herramienta de prueba de penetración de código abierto que automatiza el proceso de detección y explotación de fallas de inyección SQL y toma de control de servidores de bases de datos. Tiene integrado un motor de detección, muchas funciones de nicho, para el mejoramiento a la hora de realizar pruebas en las aplicaciones web y una amplia gama de interruptores que van desde la toma de huellas dactilares de la base de datos, hasta el acceso al sistema de archivos subyacente y la ejecución de comandos en el sistema operativo a través de medios externos.

Social Engineer Toolkit.

Tal cómo podemos observar en la página web <https://www.computerweekly.com/tutorial/Social-Engineer-Toolkit-SET-tutorial-for-penetration-testers> (R, 2019), esta herramienta trata de un Kit de herramientas para ingenieros sociales que incorpora muchos ataques útiles de ingeniería social en una sola interfaz. El propósito principal de SET es automatizar y mejorar muchos de los ataques de ingeniería social que existen. Puede generar automáticamente páginas web o mensajes de correo electrónico que ocultan vulnerabilidades, y puede utilizar las cargas útiles Metasploit para, por ejemplo, conectarse de nuevo con un shell una vez que se abre la página.

Network Mapper (Nmap).

Tal cómo podemos observar en la página web <https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html> (Ferranti, 2018), esta herramienta trata de una herramienta de código abierto para el análisis de vulnerabilidades y el descubrimiento de redes. Generalmente se usa Nmap para identificar qué dispositivos se están ejecutando en un sistema, descubriendo los hosts disponibles y los servicios que ofrecen, encontrando puertos abiertos y detectando riesgos de seguridad.

Esta herramienta puede ser usada para monitorear hosts individuales, así como diversas redes que abarcan cientos de miles de dispositivos y multitudes de subredes.

Se considera que esta herramienta es extremadamente flexible, siendo esencialmente una herramienta de escaneo de puertos, misma que recopila información mediante el envío de paquetes sin procesar a los puertos del sistema. Escucha las respuestas y determina si los puertos están abiertos, cerrados o filtrados de alguna manera, por ejemplo, por un firewall. Otros términos utilizados para escanear puertos incluyen el descubrimiento o enumeración de puertos.

De igual forma, Nmap permite la aplicación de diversas funciones, mismas de las que se describen algunas a continuación:

- **Mapeo de red:** Identifica los dispositivos en una red, incluidos los servidores, enrutadores y conmutadores, y cómo están conectados físicamente.
- **Detección del sistema operativo:** Detecta los sistemas operativos que se ejecutan en dispositivos de red (también denominados huellas digitales del sistema operativo), proporcionando el nombre del proveedor, el sistema operativo subyacente, la versión del software y una estimación del tiempo de actividad de los dispositivos.
- **Detección de servicios:** Identifica si los hosts en la red actúan como servidores de correo, web o de nombres, y las aplicaciones y versiones particulares del software relacionado que están ejecutando.
- **Auditoría de seguridad:** Averigua qué versiones de sistemas operativos y aplicaciones se ejecutan en hosts de red y permite a los administradores de redes determinar su vulnerabilidad a fallas específicas. Si un administrador de red recibe una alerta sobre una vulnerabilidad en una versión particular de una aplicación, por ejemplo, puede escanear su red para identificar si esa versión de software se está ejecutando en la red y tomar medidas para parchear o actualizar los hosts relevantes. Los scripts también pueden automatizar tareas como la detección de vulnerabilidades específicas. (LINUX, 2014)

Capítulo 3 DESARROLLO

3.1 Descripción

Mediante esta investigación se tiene como objetivo describir de forma conjunta algunas de las herramientas revisadas en el capítulo anterior siguiendo el orden de las fases del hacking ético, simulando en un ambiente local controlado algunas de las características más comunes de una red de área local.

En esta sección se cubrirá los siguientes aspectos:

- Reconocimiento de información general de las herramientas.
- Descripción de la operación de las herramientas.
- Opiniones de usuarios experimentados en las herramientas.

3.2 Análisis de herramientas destacadas

3.2.1 Etapa de Reconocimiento

Wireshark

Esta aplicación es ejecutada por muchos expertos, algunas de las razones por las que la gente usa Wireshark son las siguientes:

- Los administradores de red lo utilizan para solucionar problemas de red.
- Los ingenieros de seguridad de redes lo utilizan para examinar problemas de seguridad.
- Los ingenieros de control de calidad lo utilizan para verificar las aplicaciones de red.
- Los desarrolladores lo utilizan para depurar implementaciones de protocolo.
- Personas lo utilizan para aprender de protocolo de red internos.

No obstante, éstas no son las únicas razones, ya que Wireshark también puede ser utilizado en otras situaciones (espionaje o robo de información)

Detalles generales

- Licencias: GPLv2, GPLv2 o posterior.
- Lenguaje de programación: C
- Desarrollador: Gerald Combs
- Último lanzamiento: 2.6.2 [2018-07-18]
- Sistemas operativos: Linux, Microsoft Windows.

Wireshark no es un sistema de detección de intrusos. No avisa cuando alguien hace cosas extrañas en la red que él/ella no se le permita hacer. Sin embargo, si cosas extrañas suceden, Wireshark puede ayudar a averiguar lo que realmente está pasando.

Cómo capturar paquetes con Wireshark

Wireshark se basa en su capacidad para capturar paquetes de red y mostrarlos en un formato que puede ser interpretado. Después de descargar e instalar Wireshark, puede iniciarse y utilizar el módulo con el nombre de una interfaz de red en Captura para comenzar a capturar paquetes. Por ejemplo, si se desea capturar el tráfico en su red inalámbrica, se selecciona dicha interfaz. (ver figura 1).

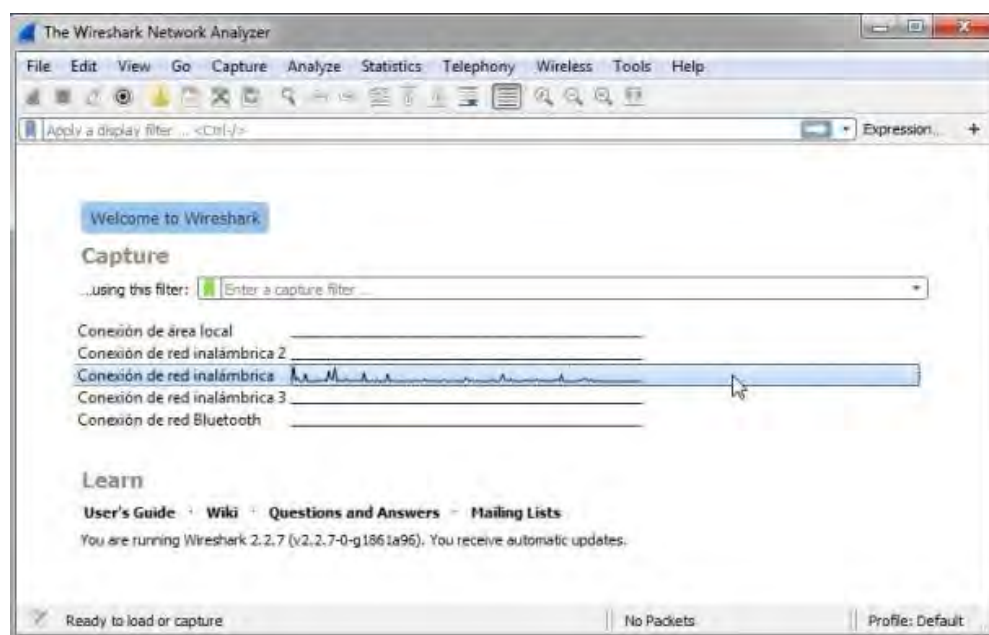


Figura 1 Usando Wireshark para capturar paquetes.

A continuación, se muestra un ejemplo de cómo los paquetes comienzan a aparecer en tiempo real. Wireshark captura cada paquete enviado hacia o desde un sistema.

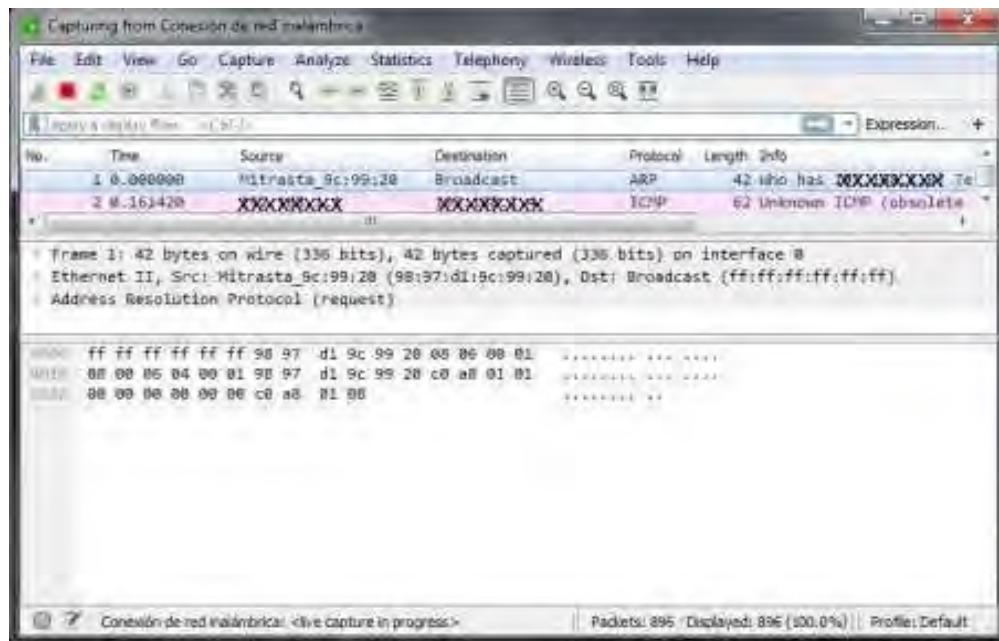


Figura 2 Mostrando los paquetes que aparecen en tiempo real.

La figura 3 muestra el botón rojo “Detener” cerca de la esquina superior izquierda de la ventana cuando se desea detener la captura de tráfico. (Perez, 2013)

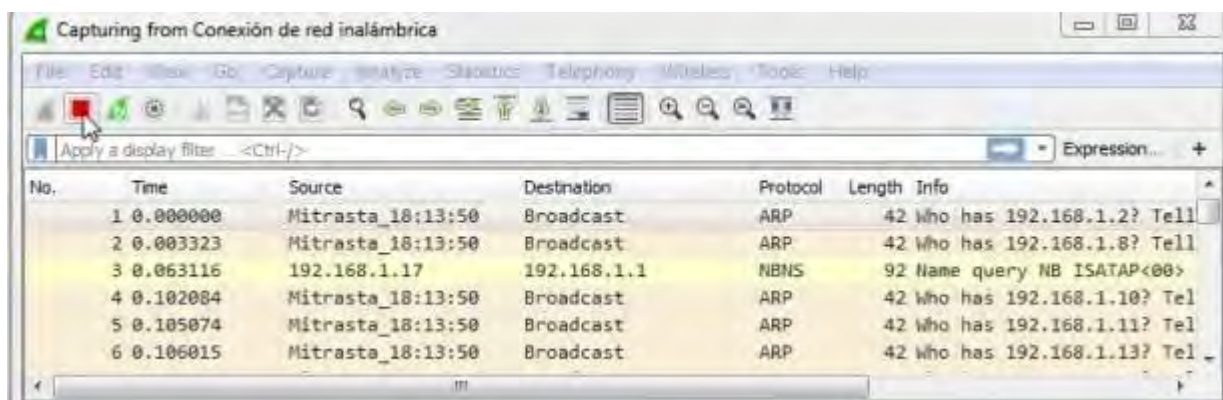


Figura 3 Mostrando el tráfico en Wireshark.

A continuación se muestra una pequeña guía de los controles de Wireshark, enumerando desde abajo hacia arriba del 1 al 15.

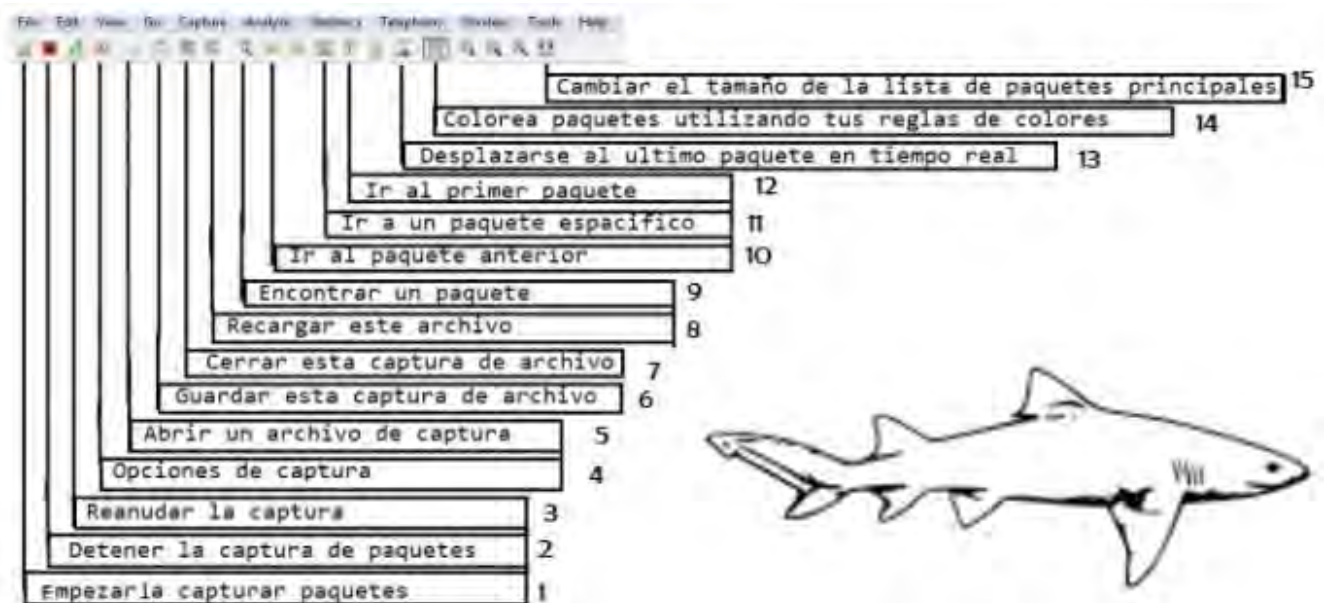


Figura 4 Los controles de Wireshark, enumerando desde del 1 al 15.

Wireshark es una herramienta muy útil, los profesionales de las redes lo utilizan para depurar las implementaciones de los protocolos de red, examinar los problemas de seguridad e inspeccionar las partes internas de los protocolos de red. (Terrill, 2019)

Opiniones

Respecto al uso de la herramienta Wireshark, podemos encontrar, en el sitio web <https://www.trustradius.com/products/wireshark/reviews> (N.A., Wireshark Reviews , 2019) , que el Director de Tecnología de la Información Matthew Frederickson, comenta que: *“Usamos Wireshark para solucionar problemas de red, tanto alámbricos como inalámbricos. No es raro obtener un ticket de un usuario que indique que la red es “lenta”. Como eso siempre es menos útil, generalmente iniciamos una captura de Wireshark más cercana al punto final con el problema. Invariablemente, siempre podemos encontrar el problema, ya sea relacionado con el punto final o el conmutador, o incluso si es algo posterior.*

Hemos logrado capacitar a algunos miembros del personal de TI sobre cómo realizar una captura, por lo que incluso si no entienden lo que están viendo, están familiarizados con el uso de un archivo pcap para nuestra revisión.”

De igual forma, en la página <https://www.trustradius.com/reviews/wireshark-2018-09-25-11-46-05> (N.A., Wireshark Reviews , 2019), el analista de sistemas Kenneth Hess dice que: *“Usamos Wireshark para capturar y analizar el tráfico de redes inalámbricas y por cable. Es una herramienta absolutamente necesaria para cualquier administrador del sistema o administrador de red. Todo nuestro departamento de TI lo utiliza. Wireshark es un software gratuito y de código abierto que, por lo que hace, nos ahorra mucho dinero.*

Esta herramienta gráfica es fácil de usar y hace que el análisis de paquetes de red sea mucho menos doloroso que si tuviéramos que confiar solo en la línea de comandos. Usando Wireshark, podemos analizar el tráfico de la red para un análisis más profundo por nosotros mismos o podemos capturarlo y enviarlo como un archivo pcap a un consultor de seguridad para una investigación adicional. Es una parte esencial de nuestra caja de herramientas administrativa.”

3.2.2 Etapa de Escaneo

En esta segunda etapa se analizarán las siguientes herramientas, cinco de ellas en el Top 10 de Kali Linux: Nmap, Burpsuite, owasp-zap, sqlmap, nessus.

Nmap

Las razones por las que se usa escáner de red Nmap son las siguientes:

- ✓ Detectar puertos abiertos y servicios
- ✓ Descubrir servicios junto con sus versiones.
- ✓ Adivinar el sistema operativo que se ejecuta en una máquina de destino
- ✓ Obtener rutas de paquetes precisas hasta la máquina objetivo
- ✓ Monitorear hosts

Detalles generales

- Licencias: GPLv2, Multi-licencia.
- Lenguaje de programación: C, C++, Lua, Python
- Desarrollador: Gordon Lyon
- Último lanzamiento: 7.70 [2018-03-20]
- Sistemas operativos: FreeBSD, Linux, macOS, Microsoft Windows y OpenBSD.

Permite utilizar diferentes técnicas de escaneo de puertos como:

- **Escaneo SYN o half open (-sS):** Utiliza el protocolo TCP el cual realiza el “three-way handshake” (apretón de manos de tres vías), sin embargo, este método no realiza el último paso de este procedimiento que es el enviar el mensaje ACK30 de confirmación de recepción del mensaje (SYN+ACK). De allí su nombre. Este método es conveniente ya que, al no completarse, no se registra en el log de eventos de red lo que hace que ni los IDS o los administradores del sistema detecten el escaneo. Si se recibe un SYN/ACK o un paquete SYN entonces el puerto está abierto, si se recibe un RST entonces el puerto está cerrado, si no se recibe respuesta o se recibe un paquete ICMP tipo 3 código 1, 2, 9, 10 ó 13 se marca como filtrado.
- **Escaneo Completo o TCP Connet Scan (-sT):** A diferencia del anterior, este completa los pasos del three-way handshake, con lo cual este escaneo si se registra en el log de eventos.
- **Escaneo UDP o UDP Scann (-sU):** Consiste en el envío de un paquete UDP a los puertos de host remoto, si este mensaje no devuelve ninguna contestación coloca el puerto como abierto|filtrado, si devuelve un paquete ICMP port-unreachable lo coloca como cerrado, si se recibe un paquete ICMP tipo 3 código 1, 2, 9, 10 ó 13 se marca como filtrado y por último si se recibe un segmento UDP entonces el puerto se clasifica como abierto.
- **Escaneo ACK (-sA):** Este tipo de escaneo se utiliza para conocer si un puerto está o no filtrado, se envía un segmento con la bandera ACK encendida, si la respuesta es un RCT o reset quiere decir que el puerto no está filtrado, mientras que, si no se recibe respuesta o se recibe un paquete ICMP tipo 3 código 1, 2, 9, 10 ó 13 se marca como filtrado.

Tabla 3 Estados de Puertos en Nmap

Estado	Descripción
Abierto	El puerto se encuentra disponible y receptando solicitudes para la conexión al servicio ofrecido a través de él.
Cerrado	El puerto es accesible pero no cuenta con una aplicación o servicio asociado que responda las solicitudes.
Filtrado	Existe un dispositivo filtrador de paquetes que impiden que las solicitudes enviadas para el escaneo de puerto se recepen.
No-Filtrado	El puerto es accesible pero no puede determinarse si está abierto o cerrado.
Abierto Filtrado	Estado ambiguo en el que el escáner no puede determinar si está abierto o filtrado y es posible de obtener cuando se utiliza una técnica de escaneo en el que un puerto abierto puede no responder.
Cerrado Filtrado	Estado ambiguo en el que no se puede determinar si el puerto está cerrado o filtrado.

Opiniones

Respecto al uso de la herramienta Nmap, podemos encontrar, en el sitio web <https://www.trustradius.com/reviews/nmap-2019-01-30-15-49-52> (N.A., Nmap Review, 2019), que el gerente de infraestructura de TI Demitri Pevzner, comenta que: *“El software es utilizado por mí personalmente. Actualmente, uso Nmap para barrer las LAN para determinar si hay algún dispositivo malicioso conectado. Además, cualquier elemento desconocido se puede escanear en el puerto y se pueden determinar los servicios actuales. De manera similar, para las pruebas de seguridad, las vulnerabilidades de máquinas virtuales específicas se pueden descubrir mediante scripts NSE.”*

De igual forma, en la página <https://www.trustradius.com/reviews/nmap-2019-01-30-17-52-53> (N.A., Nmap Review, 2019), el administrador de TI Roger Mialkowski, dice que: *“Usamos Nmap varias veces por semana para ayudar a los equipos de aplicaciones que no están familiarizados con un paquete de software nuevo / existente para el que tienen la tarea de admitir. Esto es necesario porque tenemos firewalls que requieren reglas explícitas para*

permitir que las aplicaciones se comuniquen en la red. A menudo, los equipos de aplicaciones no conocen el software que soportan en ese nivel intrincado. Nmap nos ayuda a determinar exactamente cómo habla la aplicación en la red.”

Burp Suite

Detalles generales

- Licencias: Burp Suite Free Edition Licence Agreement.
- Lenguaje de programación: Java
- Desarrollador: PortSwigger Ltd.
- Último lanzamiento: 7.70 [2018-03-20]
- Sistemas operativos: Linux, macOS, Microsoft Windows.

Burp Suite está compuesto por los siguientes elementos:

- **Burp Proxy:** Es una de las principales herramientas de Burp Suite, el cual permite interceptar, visualizar y modificar todas las solicitudes y respuestas entre un navegador y un servidor web.
- **Burp Spider:** Permite realizar un rastreo de sitio web utilizando técnicas de inteligencia que permiten generar un inventario de su contenido y funcionalidad.
- **Burp Repeater:** Esta herramienta permite manualmente generar peticiones HTTP y analizar la respuesta del aplicativo. Además, se pueden enviar solicitudes al repetidor desde otras herramientas como el proxy del mismo aplicativo para comenzar el análisis.
- **Burp Sequencer:** Es una herramienta de análisis de calidad de la aleatoriedad de los tokens de sesión³² que da la aplicación y de otros datos relevantes que podría pasar por desapercibida.
- **Burp Decoder:** es capaz de transformar datos codificados a su forma natural, así como codificar datos simples (texto o hexadecimal) en otra codificación (Base64, ASCII hexadecimal, hexadecimal, octal, binario, etc) o inclusive permite aplicar funciones de hash sobre el texto ingresado (MD2, MD5, SHA1, SHA-256, entre otras).
- **Burp Comparer:** Permite como su nombre lo indica realizar comparaciones entre dos textos (simples o hexadecimales), es sencillamente una ventana con dos cajas de texto

que permite comparar a nivel de palabras o de bytes, identificando a través de resaltadores de colores los datos modificados, añadidos y eliminados.

- **Burp Intruder:** Es una herramienta para la automatización personalizada de ataques a aplicaciones web que permite identificar y explotar todo tipo de vulnerabilidades de seguridad. Los resultados obtenidos con otras herramientas de Burpsuite pueden incorporarse para: fuzzing33, descifrar identificadores como números y usuarios utilizados dentro de la aplicación, ataques de fuerza bruta, explotación de fallos, entre otros. Esta herramienta viene como Demo, sin embargo, se puede encontrar en su versión completa en Burp Suite Pro.

Opiniones

Respecto al uso de la suite Burp, podemos encontrar, en el sitio web <https://www.trustradius.com/reviews/burp-suite-2018-08-24-12-43-34> (N.A., Burp Suite Reviews, 2019), que el Sr. Arquitecto de Sistemas y Seguridad Glenn Jones, comenta que: “*Burp Suite está siendo utilizado por el Equipo de Seguridad del Software Web. Es bastante fácil de usar y puede realizar gran parte de las pruebas de seguridad dinámica (DAST) en la empresa. Tenemos una política de la compañía de que todos los sitios web deben pasar por una revisión de seguridad antes de que puedan pasar a producción. Burp es una de las herramientas que utilizamos para ayudar en este proceso. Descubrí que Burp Suite generalmente puede hacer el trabajo requerido con bastante rapidez. También produce un informe que la mayoría de los desarrolladores pueden entender.*”

De igual forma, en la página <https://www.trustradius.com/reviews/g-suite-2018-06-11-22-23-20> (N.A., Burp Suite Reviews, 2019), el director de desarrollo de negocios Gagan Kanwar, dice que: “*Hemos estado utilizando Burp Suite durante aproximadamente 5 años, sin embargo, la organización lo ha estado utilizando durante más tiempo. Personalmente me lo presentaron hace unos 5 años, pero no antes de escucharlo. Desde que me convertí en un "pichón" en las pruebas de penetración web, no conozco a una sola persona que realice pruebas de penetración web que no dirían que Burp Suite es su principal herramienta.*”

Zed Attack Proxy

Detalles generales

- Licencias: Apache version 2.
- Lenguaje de programación: Java
- Desarrollador: Simon Bennetts
- Último lanzamiento: 2.7.0 [2017-11-28]
- Sistemas operativos: Linux, macOS, Microsoft Windows.

Lo que consiste la herramienta zed attack proxy:

- Intercepting Proxy: Permite visualizar las solicitudes y respuestas realizadas a través del navegador web, además es posible ver llamadas Ajax³⁷. Se puede inclusive establecer puntos de quiebre (modo depuración) para cambiar las solicitudes receptadas.
- Spiders tradicionales y Ajax: Esta herramienta es usada para automáticamente descubrir nuevos recursos (URL) de una página web.
- Ejecutar escaneos activos y pasivos para detectar vulnerabilidades del sitio objetivo, así como la configuración de determinados parámetros para cada tipo de escaneo (número de host analizados para el escaneo activo, entre otras y definir etiquetas en el escaneo pasivo).
- Descubrir directorios y archivos utilizando técnicas de búsqueda bajo mecanismos de fuerza bruta. A través de la ventana de opciones (Brute Force) permite establecer el número de ejecuciones por host, si se habilita recursividad en la búsqueda, permite añadir archivos personalizados que realicen mecanismos de fuerza bruta. Se encuentra basado en otra herramienta llamada OWASP Dirbuster Code (proyecto actualmente inactivo ya que fue incorporado a ZAP)
- Generar reportes en formato HTML y XML con los asuntos detectados, así como consejos y enlaces que podrían ayudar a la resolución de los mismos.
- Fuzzer: Zap permite aplicar técnicas de fuzzing utilizando una base de datos llamada Fuzzdb y las librerías de JBroFuzz, un proyecto inactivo actualmente de OWASP que

proveía de técnicas de fuzzing para solicitudes sobre HTTP y HTTPS a través de un aplicativo web.

- Certificado SSL Dinámicos: Es posible generar una única autoridad de certificación que sea reconocida como confiable para el navegador web, de tal forma que se pueda interceptar el tráfico HTTP.
- Soporte para tarjetas inteligentes y certificados digitales de clientes: Esta funcionalidad es útil si la aplicación evaluada usa tarjetas inteligentes o tokens para la autenticación.
- Capaz de interceptar y mostrar mensajes WebSocket, establecer un punto de quiebre en tipos específicos de mensajes WebSocket y enviar información inválida o inesperada al navegador o servidor a través de los mensajes WebSocket.
- Soporta una amplia gama de lenguajes script que soporten JSR 223 (Especificación de solicitudes Java) como ECMAScript, Zest, Groovy, Python, Ruby, entre otros.
- Soporte Plug-n-Hack38: Agrega un botón a la pestaña de inicio rápido que permite configurar rápida y fácilmente el navegador para trabajar con ZAP.
- Soporte para autenticación y sesiones: Permite comparar sesiones distintas si la aplicación evaluada lo permite. (Cedeño, 2015)

Opiniones

Respecto al uso de la herramienta Zed Attack Proxy, podemos encontrar, en el sitio web <https://www.itcentralstation.com/products/owasp-zap-reviews> (Station, 2019), que el Adam Sims, comenta que: *“ZAP es una buena herramienta, sin embargo, no tiene la misma facilidad de uso que Burp. A pesar de que ZAP es una herramienta gratuita y de código abierto y tiene mucho impacto, simplemente no es tan agradable de usar como Burp Suite. Estas son dos piezas de software fáciles de comparar e incluso la versión gratuita y limitada de Burp supera a la versión completa gratuita de Zap.”*

De igual forma, en la página <https://www.itcentralstation.com/products/owasp-zap-reviews> (Station, 2019), Tvsham Ghosh, dice que: *“He utilizado este ZAP para pruebas de seguridad en mi proyecto y esta es una muy buena opción si no tiene mucho presupuesto, ya que es una herramienta totalmente gratuita.”*

Puede probar casi toda la vulnerabilidad de OWASP top 10 con ZAP. También puede realizar pruebas de inyección SQL en API mediante el editor de solicitudes manual de ZAP. Lo he probado y es horrible.

Pero carece de la funcionalidad de informes como eructar, pero para la herramienta gratuita, eso está bien.”

Sqlmap

Detalles generales

- Licencias: GPLv2.
- Lenguaje de programación: Python
- Desarrollador: Bernado Damele A. G., Miroslav Stampar
- Último lanzamiento: 1.3.44[2019]
- Sistemas operativos: Linux Windows, Mac OS.

Lo que soporta sqlmap:

- Soporte completo para sistemas de administración de bases de datos MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, HSQLDB y Informix.
- Soporte completo para seis técnicas de inyección SQL: boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.
- Soporte para conectarse directamente a la base de datos sin pasar por una inyección SQL, proporcionando credenciales DBMS, dirección IP, puerto y nombre de la base de datos.
- Soporte para enumerar usuarios, password hashes, privilegios, roles, bases de datos, tablas y columnas.
- Reconocimiento automático de los formatos password hash y soporte para descifrarlos usando un dictionary-based attack.
- Soporte para vaciar completamente las tablas de la base de datos, un rango de entradas y opciones específicas según la elección del usuario. El usuario también puede elegir un solo rango de caracteres desde la entrada de cada columna.

- Soporte para buscar nombres de bases de datos específicos, tablas específicas en todas las bases de datos o columnas específicas en todas las tablas de las bases de datos. Esto es útil, por ejemplo, para identificar tablas que contienen credenciales de aplicaciones personalizadas donde los nombres de columnas relevantes contienen cadenas como nombre y pass.
- Soporte para descargar y cargar cualquier archivo del sistema de archivos subyacente del servidor de base de datos cuando el software de base de datos es MySQL, PostgreSQL o Microsoft SQL Server.
- Soporte para ejecutar comandos arbitrarios y recuperar su salida estándar en el sistema operativo subyacente del servidor de bases de datos cuando el software de base de datos es MySQL, PostgreSQL o Microsoft SQL Server.
- Soporte para establecer una conexión TCP con estado out-of-band entre la máquina atacante y el sistema operativo subyacente del servidor de base de datos. Este canal puede ser un símbolo del sistema interactivo, una sesión de Meterpreter o una sesión de interfaz gráfica de usuario (VNC) según la elección del usuario. (neoslab, 2018)

Opiniones

Respecto al uso de la herramienta sqlmap, podemos encontrar, en el sitio web <https://www.g2.com/products/sqlmap/reviews/sqlmap-review-1828212> (G2 Crowd, SQLmap, 2019), que la analista de seguridad de la información Medhavi W, comenta que: *“Facilidad de instalación y uso. Ejemplos y casos de uso. Casos de prueba, gran volumen de foros y ayudas. Libre de costo. Los tutoriales son fáciles de encontrar y muy extensos y cubren todos los casos de uso. Por lo tanto, cualquier desarrollador o probador que no conozca la base de datos puede aprender fácilmente e iniciar las pruebas de base de datos.”*

De igual forma, en la página <https://www.g2.com/products/sqlmap/reviews/sqlmap-review-2205376> (G2 Crowd, SQLmap, 2019), el ingeniero de software Lena C. dice que: *“El trabajo de mapas SQL con todas las bases de datos SQL, MSSQL y Oracle, esta herramienta es una herramienta útil para tomar volcados de información y acceder a bases de datos a través de escaladas privilegiadas victimización Inyección de comandos de victimización de comandos de SQLmap. Es una herramienta terriblemente poderosa para alterar las inyecciones de SQL para penetrar en los servidores de Internet y en los servidores de información de SQLmap.*

Los scripts de Python se utilizan para modificar estas tareas de forma rápida y sencilla. Conjuntamente, SQLmap puede ser una herramienta de fuente abierta y gratuita integrada con el sistema kali UNIX. Por lo tanto, cualquier persona lo usará sin más valor y si alguien desea opciones adicionales, también hay una versión profesional para comprar. Confíe en sus necesidades.”

Nessus

Detalles generales

- Licencias: GNU.
- Lenguaje de programación: NASL
- Desarrollador: Tenable, Inc.
- Último lanzamiento: 8.3.1[2019-03-29]
- Sistemas operativos: Microsoft Windows, Mac OS X, Linux, FreeBSD, GPG keys.

Nessus Professional ayuda a consultores y encargados de analizar intrusiones:

- Escanea el rango más amplio de dispositivos de red, sistemas operativos, bases de datos y aplicaciones
- Detecta amenazas como virus, malware, puertas traseras y servidores que se comunican con sistemas infectados con botnets;
- Informa y comunica problemas de seguridad en toda la organización mediante informes de solución.

Los escaneos integrales de Nessus incluyen:

- Escaneo de PCI;
- Escaneo de aplicaciones web;
- Escaneos activos;
- Escaneos autenticados;
- Evaluación de red;
- Descubrimiento de recursos;

- Manejo de parches;
- Política de BYOD y seguridad de dispositivos móviles. (Nessus, n.d.)

Opiniones:

Respecto al uso de la herramienta Nessus, podemos encontrar, en el sitio web <https://www.g2.com/products/nessus/reviews/nessus-review-2202331> (G2 Crowd, Nessus Reviews , 2019), que Sergio M., comenta que: *“Lo que más me gusta de Nessus es que nos permite hacer descubrimientos sobre el equipo que coexiste en nuestra red, esto es muy beneficioso porque nos permite reforzar la seguridad dentro de ella y a menudo se ve que las computadoras aparecen en la red de las cuales no teníamos ni idea y no sabemos qué actividad tienen, podría ser un atacante, luego con nessus podemos detectar estos equipos para luego excluirlos y mantener nuestra red segura en todo momento.”*

De igual forma, en la página <https://www.g2.com/products/nessus/reviews/nessus-review-2139524> (G2 Crowd, Nessus Reviews , 2019), Victor M., dice que: *“Actualmente existen muchas herramientas para analizar vulnerabilidades de red, estaciones, servidores y dispositivos de red, pero pocas son tan eficientes y precisas como lo es Nessus. Lo que más me gusta de esta potente aplicación es que su base de datos de vulnerabilidades se actualiza constantemente. en Nessus, conocido como Pugins, no solo le permite detectar vulnerabilidades que afectan a su equipo, sino que también le permite descubrir su red, a través de la cual puede validar si se encuentran dispositivos no autorizados conectados a ella, es simplemente una excelente herramienta.”*

Netsparker

Detalles generales

- Licencias: de costo.
- Lenguaje de programación: Perl
- Desarrollador: N/A.
- Último lanzamiento: 5.3.0.23731[2019-05-15]
- Sistemas operativos: Windows.

Netsparker es una solución de seguridad web avanzada y fácil de usar que puede ampliarse fácilmente y encontrar automáticamente vulnerabilidades en cientos y miles de aplicaciones web y servicios web en cuestión de horas.

Lo que consiste Netsparker:

- **Fácil de Usar:** Tiene una GUI de usuario que es intuitiva y que le permite iniciar un escaneo de sus aplicaciones web, en apenas segundos.
- **Informes precisos con escaneo basado en pruebas:** Tener una herramienta precisa que no informe falsos positivos y que su equipo confíe es una necesidad. De lo contrario, no puede ampliarse porque se requiere la verificación manual de las vulnerabilidades, lo que ralentiza el proceso de desarrollo y aumenta los errores.
- **Escanea todos tus activos web:** Netsparker tiene su Servicio de Aplicación y Descubrimiento, para que pueda identificar y escanear todas sus aplicaciones web antes de que lo hagan los piratas informáticos maliciosos.
- **Tecnología avanzada de escaneo y rastreo:** Netsparker cuenta con un motor de rastreo basado en Chrome que puede rastrear y encontrar vulnerabilidades en todo tipo de aplicaciones web, incluyendo HTML5, Web 2.0 y aplicaciones de página única.
- **No necesita verificar manualmente las vulnerabilidades web:** Usted no tiene que verificar manualmente las vulnerabilidades que el escáner Netsparker identifica durante un escaneo porque el mismo las explota en una forma segura y solo de lectura. El escáner también genera una evidencia del impacto de la exposición destacando su impacto. Netsparker lo alertará si una vulnerabilidad no se pudo verificar automáticamente.
- **Herramientas incorporadas para evaluaciones avanzadas:** Aunque Netsparker es una solución de seguridad automatizada de nivel empresarial, también tiene todas las herramientas que los profesionales necesitan cuando realizan evaluaciones avanzadas y pruebas de penetración.

Opiniones

Respecto al uso de la herramienta Netsparker, podemos encontrar, en el sitio web <https://www.trustradius.com/reviews/netsparker-2018-04-10-10-48-47> (N.A., Netsparker

Reviews , 2019), que el Sr. Arquitecto de Sistemas y Seguridad Glenn Jones, comenta que: *“Netsparker es utilizado por Application Security Group en Mathematica para escanear dinámicamente sitios web de desarrollo y producción de manera regular. Actualmente analiza todas las aplicaciones que tenemos asignadas a una autoridad para operar. Esto nos permite asegurarnos de que la cantidad de vulnerabilidades en la aplicación no se descubran fácilmente y nos permite compartir el informe de vulnerabilidad de Netsparker con nuestros clientes gubernamentales. Al ejecutar Netsparker en un horario regular, podemos estar seguros de que se han introducido nuevas vulnerabilidades en nuestras aplicaciones a pesar de que no hemos modificado la aplicación desde que se realizó el último análisis. Netsparker también nos permite mitigar los informes de falsos positivos una vez que nos han sido reportados.”*

3.2.3 Etapa de Explotación

Metasploit Framework

Detalles generales

- Licencias: Metasploit Framework License (BSD 3-clause)
- Lenguaje de programación: Ruby
- Desarrollador: HD Moore
- Último lanzamiento: 4.11.7 [2016-01-07]
- Sistemas operativos: Linux

Este framework está compuesto por:

- Librerías: Son el núcleo de MSF, ellas son las encargadas de brindar las funcionalidades básicas, así como la mayoría de las tareas, manejando sockets, protocolos y operaciones de codificación (XOR, Base64 o Unicode), proporcionan las APIs a través de las cuales interactúan interfaces, módulos y plugins.
- Módulos: Implementan funcionalidades a MSF, son 6 y se presentan a continuación:
 - Auxiliares (auxiliary): Estos módulos ofrecen funciones para ejecutar sobre un equipo como inicio de sesión, escáner de puertos, herramientas de denegación de servicios, fuzzers, etc.

- Codificadores (encoders): Se encargan de realizar la codificación /decodificación de los payloads³⁹ de modo que se pueda evitar que los antivirus puedan detectarlos.
- De explotación (exploits): Se trata de aquellos módulos donde se encuentran alojados los procedimientos que a través del uso de payloads toman el control de un equipo.
- Cargas (payload): Se trata del código malicioso que se ejecuta en la host víctima luego de la explotación o el acceso al mismo.
- Generadores de no operación (nops): Estos módulos contienen código capaz de generar instrucciones NOP⁴⁰ para los códigos maliciosos.
- De post-explotación (post): Contienen acciones que nos permiten mantener el acceso, escalar privilegios, capturar pruebas sobre la máquina, entre otras, cuando ya se ha alcanzado la explotación.
- Interfaces:
 - Msfconsole: Es la interfaz más popular debido a su “todo en uno”, es decir, permite a través de esta consola acceder a todas las opciones del framework. Además de que es la más estable entre las interfaces, permite la ejecución de comandos externos como por ejemplo ping, brinda las opciones para completar los comandos o rutas escritas al presionar la tecla tabuladora (tab).
 - Msfcli: A través de una interfaz de línea comandos se permite ejecutar exploits y módulos auxiliares, lo cuales se personalizan con los parámetros apropiados para realizar el ataque. Existen comandos que nos permiten conocer los parámetros obligatorios que deben ser configurados para la ejecución de un exploit.
 - Armitage: Es la interfaz gráfica para Metasploit Framework a través de la cual se pueden realizar las mismas opciones que en consola de una manera más práctica e intuitiva. A Armitage la podemos encontrar independiente en el menú de Kali en: Aplicaciones- Kali Linux- Herramientas de Explotación – Network Explotation- Armitage.

- Web: La interfaz se provee en las versiones Community, Express y Pro, siendo las dos últimas de pago, y a través de las cuales se puede interactuar con las opciones de MSF.

Las opciones con las que cuenta esta versión son las siguientes:

- Permite la creación de espacios de trabajo (workspaces), por defecto siempre se trabaja en el espacio de trabajo por defecto “default”, a menos que se cree y se seleccione otro.
- Importa información obtenida desde otras herramientas como: reportes de Nmap, Burp, Nessus, Nexpose, OpenVAS, entre otras. Donde el formato que recibe en su gran mayoría es XML.
- Cuenta con la colección más amplia de exploits que existe hasta el momento.
- Permite la explotación manual: Se selecciona un solo exploit para lanzar contra un único host.
- Proxy Pivoting: Usa una máquina comprometida para lanzar un exploit contra otro objetivo.
- Cuenta con el soporte de la comunidad activa Rapid7 Security Street.

Opiniones:

Respeto al uso de la herramienta Metasploit, podemos encontrar, en el sitio web <https://www.trustradius.com/reviews/metasploit-2018-05-11-18-09-00> (N.A., Metasploit Reviews, 2019), que el ingeniero senior de seguridad de Redes Alan Matson, comenta que: *“He usado Metasploit en mis posiciones actuales y pasadas para validar las vulnerabilidades encontradas en otros escáneres y para ejecutar análisis y pruebas adicionales que no se encontraron con un escáner de vulnerabilidades. Metasploit también es muy bueno para el fortalecimiento del servidor al permitir pruebas completas antes del despliegue.”*

De igual forma, en la página <https://www.trustradius.com/reviews/metasploit-2017-04-03-17-30-29> (N.A., Metasploit Reviews, 2019), el ingeniero de Tecnologías de la información dice que. *“Regularmente uso el marco Metasploit para ejecutar nuestras pruebas de seguridad internas. Ayuda a identificar posibles debilidades en nuestra red interna antes de que ocurra*

un compromiso. También en muchas ocasiones me ayudó a justificar a veces actualizaciones costosas de software y prácticas comerciales permitiéndome ilustrar el posible uso de una vulnerabilidad en la naturaleza.”

Social- Engineer Toolkit

Detalles generales

- Licencias: Licencia personalizada.
- Lenguaje de programación: Python
- Desarrollador: David Kennedy, TrustedSec, LLC
- Último lanzamiento: 7.7.9[2018-07-28]
- Sistemas operativos: Linux y macOS.

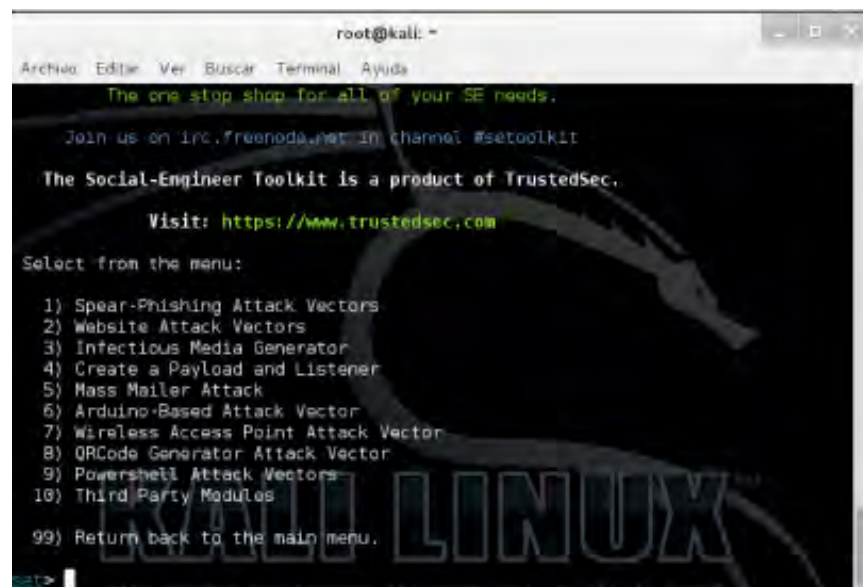


Figura 5 Submenú Opción 1 de SET.

Para ejecutar esta herramienta, se debe abrir una ventana de terminal y escribir setoolkit, posterior a ello nos pedirá aceptar las condiciones de uso del software y nos aparecerá el menú principal.

La opción número 1 trata de ataques de ingeniería social, y esta opción nos llevará hacia otro submenú desde donde se podrá realizar lo siguiente:

1. Métodos de Ataques a E-mail: Desde esta opción se puede enviar correo electrónico de forma masiva o dirigida hacia individuos, además también se puede generar correos con archivo adjunto infectado para poder tomar el control de la máquina cliente.
2. Ataques a Sitios Web: Esta opción nos permitirá darle vida a un sitio web duplicado del cual se tenga una copia previa (esto puede realizarse con otras herramientas de software como por ejemplo HTTrack). Se puede realizar múltiples ataques utilizando diferentes técnicas de modo que con un solo clic el cliente quede comprometido.
3. Generador para Infectar Unidades de Almacenamiento: Desde esta opción se podrá desarrollar un archivo infectado con el nombre de autorun.inf que una vez localizado en un medio USB disparará a otro programa que infectará y comprometerá el sistema objetivo.
4. Generación de Payload y Listener: Desde esta opción se podrá crear un archivo con extensión .exe que permitirá abrir el canal de comunicación entre víctima e intruso.
5. Ataques Masivos de Correo Electrónico: Mediante esta opción se podrá enviar múltiples correos electrónicos, a diferencia de la primera opción, éste no permite adjuntar archivos y es mayormente utilizado para ejecutar ataques de fraude mediante correo como por ejemplo indicar que se es ganador a la lotería.
6. Ataques basados en Arduino: Esta opción permite programar los dispositivos basados en Arduino.
7. Ataques a Puntos de Acceso Inalámbricos: Desde esta opción se podrá crear una red wifi (utilizando una tarjeta de red en el equipo del atacante), permitiendo la conexión a supuestos sitios web reales, que estarán montados desde la máquina del atacante.
8. Ataques mediante Código QR: Esta opción permite generar códigos QR en Python, los mismos que cuando son escaneados redireccionarán hacia lugares de dominio del atacante.
9. Ataques Powershell: Permitirá usar PowerShell, una consola de comandos que permite interactuar con el sistema operativo y está disponible por defecto en Windows desde Windows Vista hasta la actualidad. Con lo cual se podrá ejecutar código malicioso lo

que permitirá ejecutar funciones que de forma preventiva el Sistema Operativo no lo iniciaría.

10. Módulos de Terceros: Esta opción permitirá incorporar módulos de terceros a las opciones de SET.

Opiniones

Devanshu Shukla: Respecto al uso de la herramienta SET, en el sitio web <https://inuxsecurity.expert/tools/social-engineer-toolkit-set/>, (N.A., Social-Engineer Toolkit, 2019) que Devanshu Shukla, comenta que: *“SET es una herramienta increíble que he usado hasta el núcleo. Todas y cada una de las opciones. Bueno, está muy bien documentado, pero creo que se debe incorporar algo así como documentos detallados, por el uso de herramientas complicadas para una mejor comprensión y el aprendizaje de la tecnología de seguridad (uso con el emulador de Android para la suplantación de mensajes y más) y la exposición a más y más La gente, por ahí, se ocupa de algún tipo de acciones relacionadas con la ingeniería social. Lo mejor de SET es que se puede usar para usuarios normales que no son hackers o expertos en seguridad o PostMan maliciosos. SET expande el pensamiento de los usuarios para usar y aprender las tecnologías sociales. Mucho más que decir, pero las palabras no son suficientes para describir la belleza de SET.”*

John The Ripper

Detalles del proyecto

- Licencias: Freeware
- Lenguaje de programación: C
- Desarrollador: Openwall
- Último lanzamiento: 1.9.0[2019-05-20]
- Sistemas operativos: Unix, Windows, DOS, OpenVMS. (John the Ripper 1.9.0, 2019)

Hay básicamente dos tipos principales de ataques aprovechados por John the Ripper para que pueda descifrar cualquier contraseña.

Ataque de diccionario

- Las muestras de cadenas se toman esencialmente de una lista de palabras específica, un archivo de texto, un diccionario o pasadas contraseñas crackeadas.
- Luego se cifran de manera idéntica al método, la clave y el algoritmo en el que se cifró originalmente la contraseña deseada
- Las palabras del diccionario también podrían modificarse de forma aleatoria para comprobar si funcionan de esta manera
- El modo de ataque individual de John the Ripper puede hacer tales alteraciones. En consecuencia, las variaciones de hashes diferentes se comparan cuando se utilizan diferentes alteraciones. (HSAMANOUDY, 2017)

Ataque de fuerza bruta

- Todas las palabras clave compuestas de nombres de usuario con contraseñas encriptadas se agotan para encontrar la correcta
- Todos están en hash y se comparan con el hash originalmente ingresado.
- El programa utiliza las tablas de frecuencia de caracteres para incluir primero los caracteres más probables.
- Este método es muy lento, pero podría identificar aquellas contraseñas que no existen en un diccionario.

En lo que consiste:

- Una gran cantidad de crackers de contraseñas están todos compactados en la plataforma o paquete.
- Los tipos de hash utilizados por las contraseñas pueden ser autodetectados
- John the Ripper puede romper diferentes tipos de contraseñas cifradas basadas en hashes variados, como
 - Los tipos de hash de contraseñas de cifrado se basan esencialmente en los hashes de Data Encryption Standard (DES), MD5 y Blowfish utilizados en muchas versiones de Unix.
 - Sistema de archivos Kerberos Andrew (Kerberos AFS) hash
 - Hash de tipo Windows NT / 2000 / XP / 2003 LM

- Los hashes de contraseña que también dependen del MD-4 son detectados por algunos módulos adicionales
- Dichos módulos tienen la capacidad de detectar contraseñas que dependen del Protocolo ligero de acceso a directorios (LDAP) y MySQL también.
- Cracker también podría ser personalizado por el usuario.

Opinones:

Respecto al uso de la herramienta John the Ripper, podemos encontrar, en el sitio web <https://www.techulator.com/reviews/172-John-The-Ripper.aspx> (Review: John The Ripper Review, s.f.), que Krishna Verma, comenta que: *“En mi opinión, John the Ripper es un software de recuperación de contraseña muy confiable y también es efectivo. Aquí está el resumen de mi experiencia con John el destripador.*

Lo que me gustó en John The Ripper

- *Comenzar con él es gratis, a diferencia de otros softwares de recuperación de contraseña disponibles. En mi opinión esta es una de las ventajas clave.*
- *Es muy rápido y me funcionó en pocos minutos.*
- *Al final del día, me dio las contraseñas, por lo que funciona y es confiable.*
- *Es compatible con varios sistemas operativos que son buenos.*
- *Recuperé fácilmente la contraseña usando el símbolo del sistema con la ayuda de John The Ripper.”*

Cain & Abel

Detalles generales

- Licencias: Freeware
- Lenguaje de programación: Ruby
- Desarrollador: Openwall
- Último lanzamiento: 4.9.56[2019-05-20]
- Sistemas operativos: Windows /macOS/Linux (Fisher, 2019)

Lo que consiste Cain & Abel:

- Windows Vault Password Decoder.
- Soporte para Windows 8 en LSA Secret Dumper.
- Soporte para Windows 8 en Credential Manager Password Decoder.
- Soporte para Windows 8 en EditBox Revealer.
- La capacidad de mantener las extensiones originales en certificados falsos.
- Actualización de la biblioteca de Winpcap a la versión 4.1.3
- La función experimental de inyección de certificados para inyectar certificados personalizados en las respuestas de HTTPS / ProxyHTTPS dirigidas a los clientes de la APR víctima.
- Nuevo diálogo del decodificador de contraseña Base64.
- Actualización de la biblioteca OpenSSL a la versión 1.0.1f. (Daniel, 2014)

Opiniones:

Respecto al uso de la herramienta Cain & Abel, podemos encontrar, en el sitio web (Abel, s.f.), que el ingeniero senior de seguridad de TI William McGuire, comenta que: *“Una herramienta que he usado en numerosas ocasiones para descifrar las contraseñas de Windows para los empleados aquí internamente en nuestra organización. Cubre múltiples plataformas y tiene algunos complementos que puedes usar con él. No lo he usado en mucho tiempo, pero sigo siendo una herramienta útil.”*

De igual forma, en la página [https:// community.spiceworks.com/products/50660-cain-abel](https://community.spiceworks.com/products/50660-cain-abel) (Abel, s.f.), el administrador de sistema Marcin Ozga, dice que: *“Una de las primeras herramientas de descifrado de contraseñas que he usado. Puede descifrar las contraseñas de Windows, Cisco IOS y PIX, WEP y muchos más. Incluye generador de tabla arcoiris para criptoanálisis. Sin embargo, la falta de disponibilidad de código fuente pone un signo de interrogación en él. Solo ten cuidado cuando uses esta herramienta.”*

Capítulo 4 CONCLUSIONES

Un hacker ético es un experto en seguridad, el cual puede utilizar sus habilidades y conocimientos para la intrusión de sistemas, de forma que se permita evolucionar hacia sistemas más confiables y hacia la creación de nuevos estándares y programas que permitan cubrir vulnerabilidades existentes. Sin embargo, el experto en seguridad debe capacitarse en conocer y saber utilizar las herramientas de penetración que utilizarían atacantes, para que pueda identificar las vulnerabilidades e implementar las medidas de seguridad necesarias.

El área de la seguridad informática necesita ser tratada con conocimientos sólidos en sistemas y redes de computadoras, por los que el hacker ético tiene que capacitarse constantemente, debido a la rapidez con la que aparecen en el mercado nuevas soluciones y formas de intrusión, procurando siempre encontrarse un paso delante de los ciberdelincuentes.

Con el presente trabajo se ha podido mostrar una importante cantidad de herramientas que se utilizan para encontrar soluciones a diversas problemáticas y llevar a cabo el fortalecimiento de las áreas vulnerables al momento de revisar sistemas o redes empresariales. En la mayoría de las ocasiones no se trataba simplemente de herramientas con un solo fin, sino que se trataba de herramientas que aportaban a más de una actividad.

El estudio de las herramientas me permitió conocerlas con mayor detalle y descubrir sus ventajas, dejando a manos del lector la decisión de elegir la herramienta que más se adecúe a sus necesidades. Gracias a la investigación de herramientas fue posible dar una breve guía de la labor del hacker ético actualmente, siendo posible exponer de forma básica cómo los resultados de una fase son útiles para detectar las vulnerabilidades de un sistema.

Dicha guía se basa en la descripción de las herramientas observadas en el capítulo 2, así como en el análisis y estudio de algunas de ellas en el capítulo 3, incluyendo algunas de las funciones con las que cuentan y comentarios u opiniones sobre su uso, con la finalidad de dar a conocer la información básica sobre las herramientas.

Personalmente, considero que la recopilación de la información acerca de las herramientas vistas, es un trabajo que requiere de mucha investigación y paciencia, ya que no fue fácil encontrarse con personas profesionales que quieran compartir su preciado y valioso conocimiento, así como tampoco es fácil encontrar la bibliografía adecuada, concreta y actualizada, que sea de ayuda. Como he mencionado anteriormente, la información cambia constantemente y debemos mantenernos actualizados.

Puedo concluir, sin temor a equivocarme, de que el desarrollo y evolución de las herramientas que he descrito en el presente proyecto, así como todas aquellas que, a pesar de no encontrarse contempladas, son igual de importantes, seguirá evolucionando y avanzando en el tema de seguridad para la información, de tal manera que pueda ofrecer mayores beneficios y grandes aportes a la comunidad relacionada con el hacking ético.

Trabajo Futuro

Se pueden realizar trabajos de investigación relacionados para:

- Comparar las herramientas comerciales más destacadas en este campo con las seleccionadas, para detectar aquellas características que quizás pueden ser complementadas con más de una herramienta de código abierto.
- Contrastar herramientas que existen en algunas distribuciones compiladas para pruebas de penetración que puedan estar proporcionando características similares que otras existentes dentro del mismo grupo.
- Investigar cómo se puede incrementar la confiabilidad en campos específicos como: industriales, administrativos, tecnológicos, comerciales de tal forma que la utilización de un compendio de herramientas de código abierto permita asegurar entornos específicos.

Además, es posible encaminar este tipo de investigaciones hacia trabajos totalmente prácticos que permitan:

- La creación y configuración de ambientes o laboratorios de pruebas que ofrezcan un entorno local para el entrenamiento y capacitación del hacker ético.
- Creación de una academia virtual que permita la capacitación y medición de conocimientos del principiante de hacker ético, basándose en herramientas de código abierto.

Referencias

- Abel, C. &. (s.f.). *Cain & Abel*. Obtenido de community.spiceworks.com:
<https://community.spiceworks.com/products/50660-cain-abel>
- Acosta, A. (N.A.). *John The Ripper*. Obtenido de ecured.cu:
https://www.ecured.cu/John_The_Ripper
- Cedeño, E. Y. (2015). *Análisis de las herramientas para el proceso de auditoría de seguridad informática utilizando Kali Linux*. Madrid.
- Combs, G. (22 de mayo de 2019). *wireshark*. Obtenido de wireshark.org:
<https://www.wireshark.org/>
- Culoccioni, S. (02 de julio de 2015). *SQLMAP herramienta de Inyección de SQL y Ethical hacking de bases de datos*. Obtenido de solvetic:
<https://www.solvetic.com/tutoriales/article/1615-sqlmap-herramienta-de-inyecci%C3%B3n-de-sql-y-ethical-hacking-de-bases-de-datos/>
- Daniel, P. (27 de marzo de 2014). *Cain & Abel 4.9.56*. Obtenido de download3k.com:
<https://www.download3k.com/Security/Encrypting-Tools/Download-Cain-Abel.html>
- Ferranti, M. (17 de august de 2018). *What is Nmap? Why you need this network mapper*. Obtenido de networkworld: <https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html>
- Fisher, T. (01 de mayo de 2019). *Cain and Abel v4.9.56*. Obtenido de lifewire:
<https://www.lifewire.com/cain-and-abel-review-2626136>
- G2 Crowd, I. (2019). *Nessus Reviews*. Obtenido de g2.com:
<https://www.g2.com/products/nessus/reviews/nessus-review-2139524>
- G2 Crowd, I. (2019). *Nessus Reviews* . Obtenido de g2.com:
<https://www.g2.com/products/nessus/reviews/nessus-review-2202331>
- G2 Crowd, I. (2019). *SQLmap*. Obtenido de g2.com:
<https://www.g2.com/products/sqlmap/reviews/sqlmap-review-2205376>
- G2 Crowd, I. (2019). *SQLmap*. Obtenido de g2.com:
<https://www.g2.com/products/sqlmap/reviews/sqlmap-review-1828212>

- GitHub. (s.f.). *ZAP, The OWASP Zed Attack Proxy*. Obtenido de zaproxy.org:
<https://www.zaproxy.org/>
- HSAMANOUDY. (13 de julio de 2017). *John the Ripper*. Obtenido de infosecaddicts:
<https://infosecaddicts.com/john-ripper/>
- John the Ripper 1.9.0*. (2019). Obtenido de techspot:
<https://www.techspot.com/downloads/6970-john-the-ripper.html>
- LINUX, I. U. (2014). *INFORMÁTICA UTILIZANDO KALI LINUX*. Toledo- España.
- Miller, K. (2019). *Nessus Reviews*. Obtenido de g2:
<https://www.g2.com/products/nessus/reviews/nessus-review-2202331>
- N.A. (2019). *Burp Suite Reviews*. Obtenido de trustradius.com:
<https://www.trustradius.com/reviews/burp-suite-2018-08-24-12-43-34>
- N.A. (2019). *Burp Suite Reviews*. Obtenido de trustradius.com:
<https://www.trustradius.com/reviews/g-suite-2018-06-11-22-23-20>
- N.A. (2019). *Metasploit Reviews*. Obtenido de trustradius.com:
<https://www.trustradius.com/reviews/metasploit-2018-05-11-18-09-00>
- N.A. (2019). *Metasploit Reviews*. Obtenido de trustradius.com:
<https://www.trustradius.com/reviews/metasploit-2017-04-03-17-30-29>
- N.A. (2019). *Netsparker Reviews* . Obtenido de trustradius.com:
<https://www.trustradius.com/reviews/netsparker-2018-04-10-10-48-47>
- N.A. (2019). *Nmap Review*. Obtenido de trustradius.com:
<https://www.trustradius.com/reviews/nmap-2019-01-30-15-49-52>
- N.A. (2019). *Nmap Review* . Obtenido de trustradius.com:
<https://www.trustradius.com/reviews/nmap-2019-01-30-17-52-53>
- N.A. (2019). *Our Most Advanced Penetration Testing Distribution, Ever*. Obtenido de kali.org:
<https://www.kali.org/>
- N.A. (24 de abril de 2019). *Social-Engineer Toolkit* . Obtenido de linuxsecurity.expert:
<https://linuxsecurity.expert/tools/social-engineer-toolkit-set/>
- N.A. (2019). *The Nessus Family*. Obtenido de tenable.com:
<https://www.tenable.com/products/nessus>
- N.A. (2019). *Wireshark Reviews* . Obtenido de trustradius.com:
<https://www.trustradius.com/products/wireshark/reviews>

- neoslab. (16 de julio de 2018). *COMO USAR SQLMAP PARA PRINCIPIANTES*. Obtenido de neoslab.com: <https://neoslab.com/es/2018/07/16/como-usar-sqlmap-para-principiantes/>
- Nessus. (s.f.). Obtenido de fferia.wordpress: <https://fferia.wordpress.com/nessus/>
- Oissg. (s.f.). *Open Information Security Service Group*. Obtenido de oissggroup: <https://oissggroup.com/>
- Perez, J. V. (9 de junio de 2013). *Manual De Wireshark En Español*. Obtenido de <http://manualwireshark.blogspot.com/>
- R, K. (2019). *Social Engineer Toolkit (SET) tutorial for penetration testers*. Obtenido de computerweekly.com: <https://www.computerweekly.com/tutorial/Social-Engineer-Toolkit-SET-tutorial-for-penetration-testers>
- Review: *John The Ripper Review*. (s.f.). Obtenido de techulator: <https://www.techulator.com/reviews/172-John-The-Ripper.aspx>
- Rizaldos, H. (22 de octubre de 2018). *Qué es Metasploit framework*. Obtenido de openwebinars.net: <https://openwebinars.net/blog/que-es-metasploit/>
- Shay Chen, S. H. (2019). *Web Application Security Solution*. Obtenido de netsparker: <https://www.netsparker.com/>
- Station, I. C. (2019). *Owasp Zap Reviews*. Obtenido de itcentralstation.com: <https://www.itcentralstation.com/products/owasp-zap-reviews>
- Terrill, R. (15 de abril de 2019). *comofriki.com*. Obtenido de *Cómo usar Wireshark para capturar, filtrar y analizar paquetes*: <https://comofriki.com/como-usar-wireshark-capturar-filtrar-analizar-paquetes/>
- Weidman, G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking*. USA: William Pollock.