CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

ALEXANDER ARAQUE GARZON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN
BOGOTA
2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

ALEXANDER ARAQUE GARZON

TRABAJO INFORME FINAL

INGENIERO ALEXANDER LARRAHONDO N

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN
BOGOTA
2021

.TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

COMANDO: Una orden/instrucción (también conocida con el extendido anglicismo/barbarismo comando

NMAP: Nmap (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad

EXPLOIT: Exploit es una palabra inglesa que significa explotar o aprovechar

LEY: Ley es una declaración de la voluntad soberana manifestada en la forma prevenida en la Constitución Nacional. El carácter general de la ley es mandar, prohibir, permitir o castigar.

DECRETO: El Decreto es un acto administrativo promulgado por el poder ejecutivo con contenido normativo reglamentario sin necesidad de ser sometida al órgano legislativo

IDS: Sistema de detección de intrusiones

IPS: Sistemas de Prevención de Intrusos

VPN: Red privada virtual

SIEM: Gestión de información y eventos de seguridad

ANTIVIRUS: Los antivirus son programas cuyo objetivo es detectar y eliminar virus informáticos

FIREWALL: Es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado.

INTRODUCCION

Este trabajo es de mucha importancia para las personas que están relacionadas con el área de la seguridad informática, seguridad de la información, seguridad perimetral, como todas las personas que algún día se vieron afectados por la falta de seguridad informática generando una clara necesidad de todo lo que con lleve a que la seguridad sea cada día más robusta, ya que en él se tratan esos temas a través de una metodología de fases en las a que el autor se sumerge para explicar de una manera fácil de comprender el caso expuesto para su análisis, el objetivo general del trabajo es realizar el diagnostico como consultor independiente sobre el caso de la empresa the whitehouse security, en donde el equipo de tecnología presume que se realizó una grave fuga de información, por medio de un ataque informático a una máquina de la empresa y como objetivo específico nos indican que se debe realizar el análisis de la situación, verificando la información proporcionada por la empresa, y como otro objetivo específico hacer las recomendaciones para lograr la mitigación del ataque o del caso observado a lo largo del curso.

Esto se realiza desde la perspectiva como miembro del equipo blue team y se debe presentar las diferentes alternativas de cómo se debe realizar la mitigación de este tipo de casos una vez se presentan, de manera técnica, ética y legal como lo están solicitando en los requerimientos de la rúbrica de evaluación, y para eso se utilizaran una serie de herramientas, procesos, protocolos de seguridad, que se explicaran a su debido tiempo que se siga avanzando en el tema.

JUSTIFICACIÓN

Este trabajo se realiza para la universidad nacional a distancia, curso o seminario de Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, porque se está optando por el título de especialista en seguridad informática, para lo cual es requerimiento este para las personas que optaron por esta opción de grado y se debe cumplir con el requerimiento, en el cual se tratan los diferentes temas a lo largo del mismo de las diferentes ,técnicas, temáticas o procesos, protocolos de seguridad poniéndolos en práctica como se observa en este trabajo.

OBJETIVOS

OBJETIVO GENERAL

Objetivo general del trabajo es realizar el diagnostico como consultor independiente sobre el caso de la empresa the whitehouse security, en donde el equipo de tecnología presume que se realizó una grave fuga de información, por medio de un ataque informático a una máquina de la empresa.

OBJETIVOS ESPECÍFICOS

Verificar que leyes se pueden evidenciar fueron omitidas o violadas en Colombia al momento de presentarse el caso expuesto.

Realizar el análisis de la situación, verificando la información proporcionada por la empresa.

Describir los pasos que se deben efectuar al momento de hacer un pentesting de manera ética y legal.

Consultar que tipo de herramientas se pueden utilizar para realizar el pentesting de manera ética y legal.

Formular las recomendaciones que se deben seguir si se quiere lograr la mitigación del ataque si se evidencio el mismo.

PLANTEAMIENTO DEL PROBLEMA

A lo largo de este trabajo se presentaron varios problemas complejos y para iniciar con el mismo se definió o se realizó la solicitud por parte de la empresa the white house security que se debe realizar el montaje banco de trabajo para poder llevar a cabo la utilización de herramientas de licencia abierta, y realizar las simulaciones en un entorno legal y seguro como se menciona en los diferentes anexos o comunicados por parte de la empresa que se toman como base para realizar el análisis correspondiente de la situación o caso presentado al interior de la misma en donde se presume de una grave fuga de información, a través de un ataque que se le realizo a una máquina que es la que solicitan que sea analizada.

FORMULACIÓN DEL PROBLEMA

¿Se presento fuga de información en la maquina analizada mediante el presunto ataque?

1 MÉTODOLOGIA

La metodología que se realizo fue por fases iniciando por la conceptualización de las leyes de Colombia.

1.1 LEYES, DECRETOS

Para este cuso o seminario en el contexto en el que estamos a lo que se refiere a seguridad de la información, seguridad informática y realizando el análisis de los diferentes delitos informáticos en Colombia, el congreso de Colombia crea en el año 2009 por fin la ley 1273 el día 5 de enero del año mencionado, debido a que era un gran vacío en la ley colombiana aunque se realiza un avance frente a los ciberdelincuentes aún falta mucho por hacer, por ello se observara esta ley y cómo podemos apoyarnos en ella, para no caer en malas prácticas debido al desconocimiento de la misma, respetando las buenas prácticas, con ética dentro del marco legal en Colombia.

Para ello se hace mención a sus respectivos artículos como lo son:

> **"Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.".[1]

Esto es aplicable a todo sistema informático, como lo indica el articulo lo que quiere decir que esto es aplicable a redes, cableadas, como wifi ya que esto también comprende sistemas informático de comunicación en los cuales se hace transferencia de información, personal o privada, no interesando los dispositivos que se utilicen para este efecto, la ley indica que se está cometiendo un delito que tiene multa en dinero de 100 a 1000 salarios mínimos legales o prisión 4 a 8 años, eso según lo decida el juez que tiene la decisión de dictar la una sentencia y condena según las pruebas que se presenten.

[1] Avance Jurídico Casa Editorial Ltda. (s/f). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]*. Gov.co. Recuperado el 30 de agosto de 2021, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

"Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA. INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.".[2]

Como se viene analizando el artículo anteriormente citados hace mención a los delitos informáticos que tienen una condena, por consiguiente es de vital importancia que todos los ciudadanos en Colombia tengan presente esta ley, porque el desconocimiento de la misma no lo exonera de la ley, se debe ser muy claro en este articulo porque los usuarios, por creer que el hacer una interceptación de las telecomunicaciones, como es una transferencia de datos que está en el espectro electromagnético en el caso de la transferencia de datos por medio de señales de radio, wifi, o el realizar un ataque de hombre en el medio, no tiene ninguna clase de castigo por parte de la justicia, y en cuanto a las trasmisiones por parte de las que se realizan por, teléfono, cable coaxial, fibra de vidrio, se les puede aplicar estos dos artículos a la vez.

"Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) eses.".[3]

Esto quiere decir que el realizar este tipo e practicas sin una orden judicial pueden ser penalizados y sin posibilidad de una sanción económica en Colombia se presentó un caso que fue famoso por que se le realizo a un político que se encontraba en campaña electoral y un hacker(Andrés Sepúlveda), realizo la grabación de las entrevistas y llamadas telefónicas cuando le hacían los requerimientos y el pago para realizar esta tarea por cual fue condenado, para más información sobre este caso puede hacer las consultas en la red o puede ver el artículo.

"Artículo 269D. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.".[4]

---

[2] Ibid., p.1.

[3] Avance Jurídico Casa Editorial Ltda. (s/f). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]*. Gov.co. Recuperado el 30 de agosto de 2021, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[4] Ibid., p.1.

Este tipo de delitos no hace referencia a quienes realicen estas acciones tengan o no conocimiento o formación para ello lo que hace que cual quiere persona está en la posibilidad de realizar un delito informático, porque como lo indica el articulo citado, no se trata de solo la parte lógica de los sistemas sino de su infraestructura la cual puede ser vulnerada sino está bien protegida, o a los profesionales que se extralimiten en sus funciones realizando tares que creen que puede hacer ocasionado daños a los mismos sin estar facultados para ello, esto es muy común en las empresas en Colombia que por evitar pagar a un profesional idóneo le pide o el empleado, o a un tercero creyendo que al realizar esa tarea sin el conocimiento realiza cierto tipos de procedimientos que no son éticos o legales sin ningún tipo de castigo por parte de la ley.

> **"Artículo 269E. USO DE SOFTWARE MALICIOSO.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.".[5]

En Colombia es muy común el ver en las empresas que utilicen herramientas para trabajar de manera pirata como se dice en la calle o que no cuente con su respectiva licencia para trabajar en dichas empresas, o en los hogares de los colombiano lo que con lleva no solo un gran riesgo en la seguridad de las empresas y hogares, si no para los usuarios de los mismos ya que no se sabe qué tipo de alteraciones tengan esa clase de programas, como el hacer la comercialización de los mismos tiene castigo por la ley como lo citamos en el artículo, también la instalación de los mismos sin tener una autorización y aunque la tengan es el deber de todos los colombinos el tener la ética de decir no ese tipo de herramientas o de solicitudes por parte de terceros.

> "**Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.".[6]

Esto está muy ligado a las personas que se dedican o tiene algún tipo de información sensible ya sea personal o de la empresa o de cierto sector para su provecho, por lo que es de vital importancia el hacer que los trabajadores firmen y pongan en práctica las cláusulas de confidencialidad como la ética de los profesionales y los

---

[5] Ibid., p.1.

[6] Avance Jurídico Casa Editorial Ltda. (s/f). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. Gov.co. Recuperado el 30 de agosto de 2021, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

que no lo son, esto frente a los empleados de una empresa, a las personas que se dedican a realizar ciertas tareas como mantenimientos de algún tipo de información donde tenga la posibilidad de ver u obtener al tipo de información. Esto no solo aplica a la información del trabajo sino a la información como lo es los estados financieros de las personas.

> "**Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más Grave.
> En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.".[7]

En este artículo se puede evidenciar que en Colombia falta mucho más por estas leyes, o que las leyes se han mucho más fuertes con penas más extensas para este tipo de delitos informáticos no se presente con tanta frecuencia como lo hace hoy en día, porque de 4 a 8 años de prisión no es suficiente para que las personas tomen este tipo de delitos como algo grave que se tenga que ver y no realizar la suplantación de sitios web ya que desde que sea una suplantación de cualquier tipo ya es un delito, captando información para así realizar estafas, robo de información, de dinero o extorsión por la información y daño a bien ajeno.

> "**Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA:** Las penas imponible de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
> 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
> 2. Por servidor público en ejercicio de sus funciones.
> 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
> 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
> 5. Obteniendo provecho para si o para un tercero.
> 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
> 7. Utilizando como instrumento a un tercero de buena fe.
> 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de

[7] Ibid., p.1.

inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.”.[8]

Como se mencionaba en el anterior párrafo este es un buen inicio para generar que los ciberdelincuentes lo piensen al tratar de hacer algún delito informático de este tipo por lo mismo se presenta este artículo en el cual se hace la anotación de *circunstancias de agravación punitiva* del incremento de la pena, lo que significa y hace ver que cada día más la importancia de la masificación de la información para que esto sea mucho mas de conocimiento público del que debe ser.

[8] Avance Jurídico Casa Editorial Ltda. (s/f). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. Gov.co. Recuperado el 30 de agosto de 2021, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

2 ETAPAS DEL PENTESTING

Para realizar un pentesting debemos realizar una serie de pasos lógicos y procesos los cuales se analizarán a continuación:

2.1 ETAPA DE INFORMACIÓN

Esta etapa en la más importante no solo porque es la primera sino porque es en la que recolectamos toda la información que más se pueda para que las etapas siguientes sean más concluyentes, y porque entre más información tengamos de la situación, más opciones tendremos al realizar los test con las diferentes herramientas que dispongamos para ello.

Para este caso utilizáremos una que es muy común y conocida (NMAP) pero que brinda mucha información, en el mercado se pueden encontrar más.

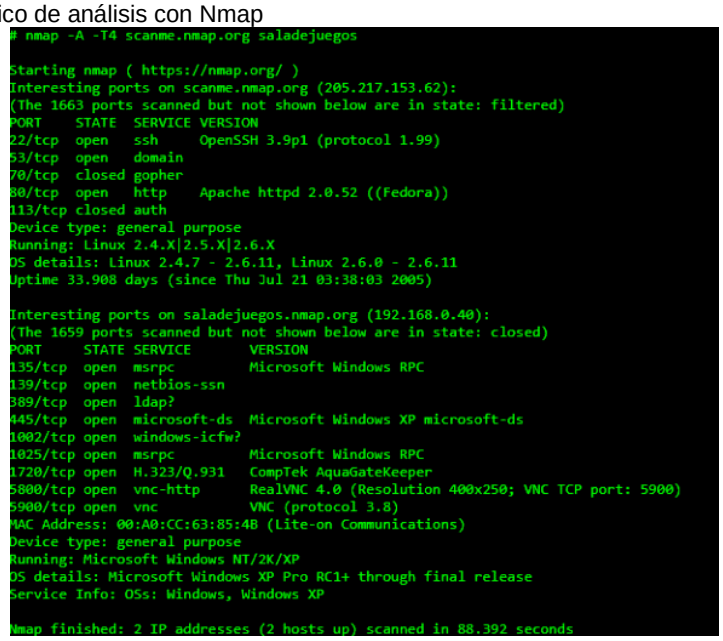
¿Qué es Nmap?

“Nmap (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad.”.[9]

Como se puede ver es una herramienta que es muy utilizada por los administradores de las redes o auditores, para realizar diferentes actividades como el ver cómo está la red, observar él comporta miento, observar los puertos que están abiertos y cuales cerrados, como se puede ver en la Figura en donde hay un ejemplo de cómo se hace el escaneo básico de una red.

[9] Guía de referencia de Nmap (Página de manual). (s/f). Nmap.org. Recuperado el 30 de agosto de 2021, de https://nmap.org/man/es/index.html

Figura 1. Ejemplo típico de análisis con Nmap



Fuente: Propia

2.2 ETAPA DE VULNERABILIDADES

Con la información que se obtuvo de la etapa anterior se inicia a buscar esas vulnerabilidades en la red.

Para ello se puede utilizar la herramienta como Nessus.

¿Qué es Nessus?

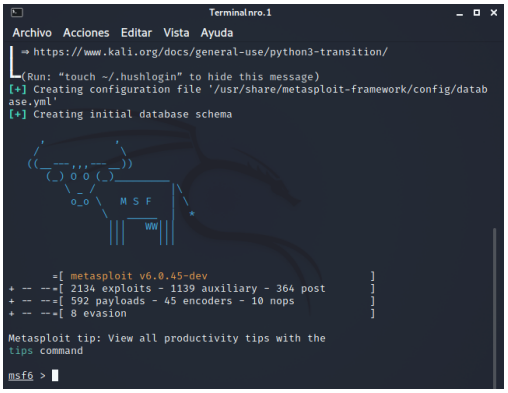
Es una herramienta o programa de test de vulnerabilidades que sirve para varios sistemas operativos, que nació o fue lanzado en el año de 1998 por su creador Renaud Deraison, quien quería tener un escáner remoto para la red libre pero ya su licencia no lo es. Este programa utiliza para realizar el escaneo un demonio o diablo llamado así por sus creadores *nessusd* que se instala en el sistema operativo que se requiere verificar y Nessus el que muestra cómo se va desarrollando de manera gráfica los escaneos, y como se va desarrollando el informe del mismo.[10]

[10] Familia de productos Nessus. (2019, mayo 14). Tenable.com. https://es-la.tenable.com/products/nessus?tns_redirect=true

2.3 ETAPA UTILIZACIÓN O EXPLOTACIÓN DE LAS VULNERABILIDADES

Esta etapa inicia cuando las dos anteriores han dado sus resultados para que por medio de lo que se ha encontrado, o se utilizar la información para realizar un ataque a las vulnerabilidades mucho más enfático en ellas se pueda utilizar a favor de quien está realizando este pentesting. En esta etapa se puede utilizar la herramienta o programa Metasploit es muy robusta para este tipo de tareas, porque no solo sigue realizando escaneo para saber más información esta permite él envió de ejecutables en el pc, pero esto no quiere decir que sea la única herramienta para ello en el mercado se pueden encontrar más.

Figura 2. Programa Metasploit-Linux



Fuente: Propia

2.4 ETAPA DE INFORME DE VULNERABILIDADES

En la etapa de informe de vulnerabilidades se indica a través del informe las vulnerabilidades que se encontraron con imágenes, gráficos y de las evidencias de lo realizado, se utiliza cual quiere procesador de texto para este informe, mas no el cómo se realizó eso hace parte del conocimiento adquirido por el auditor o el que realiza el pentesting y las recomendaciones para mitigar esas vulnerabilidades.

3 HERRAMIENTAS DE CIBERSEGURIDAD

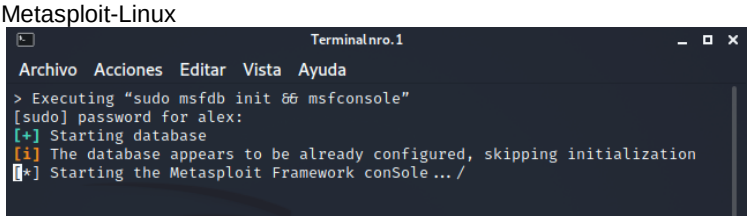
3.1 METASPLOIT

“Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.”.[11]

Como se mencionó anteriormente es una herramienta de gran valor para los profesionales de seguridad informática por sus grandes prestaciones, como lo es al realizar pentesting de vulnerabilidades en redes como a nivel local a diferentes maquinas.

Se hace el inicio de la herramienta como lo podemos ver en la Figura siguiente:

Figura 3. Programa Metasploit-Linux

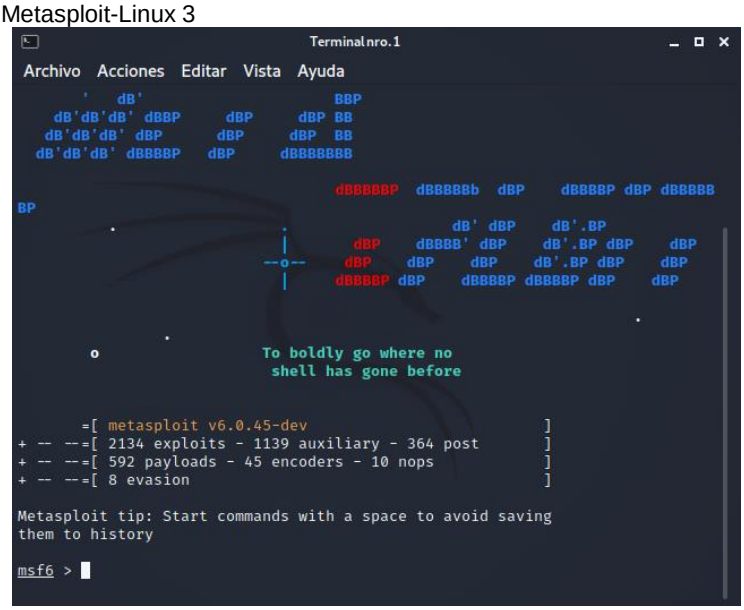


Fuente: Propia

Una vez la herramienta esta lista como se ve en la Figura se inicia el test como se quiera hacer se puede hacer de diferentes formas, por dirección IP, por nombre de dominio, puerto.

[11] Getting started with Metasploit for penetration testing. (n.d.). Metasploit.Com. Retrieved August 30, 2021, de https://www.metasploit.com/get-started

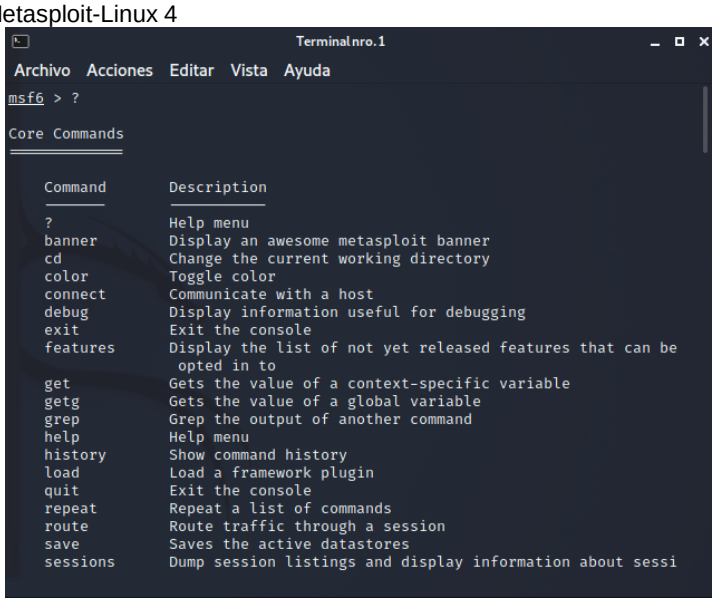
Figura 4. Programa Metasploit-Linux 3



Fuente: Propia

Ya una vez estamos en la consola de Metasploit, para ver los comandos se usa el siguiente símbolo *?* nos aparece las diferente opciones y comandos.

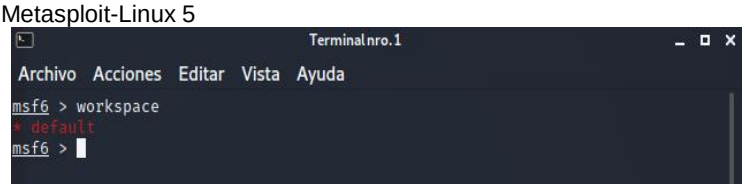
Figura 5. Programa Metasploit-Linux 4



Fuente: Propia

Se verifica que estemos trabajado en que espacio se digita *Works pace* y nos da como respuesta que estamos trabajando en el espacio por defecto por lo general se crea otro espacio para cada proyecto que se trabaje.

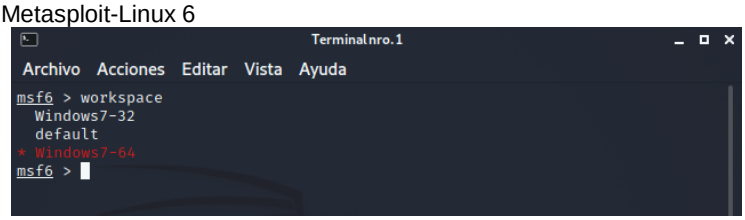
Figura 6. Programa Metasploit-Linux 5



Fuente: Propia

Para este caso o practica se crea los espacios para las dos máquinas que se van a explotar sus vulnerabilidades Windows 7 de 32 bits y Windows 7 de 64 bits.

Figura 7. Programa Metasploit-Linux 6



Fuente: Propia

3.2 NMAP

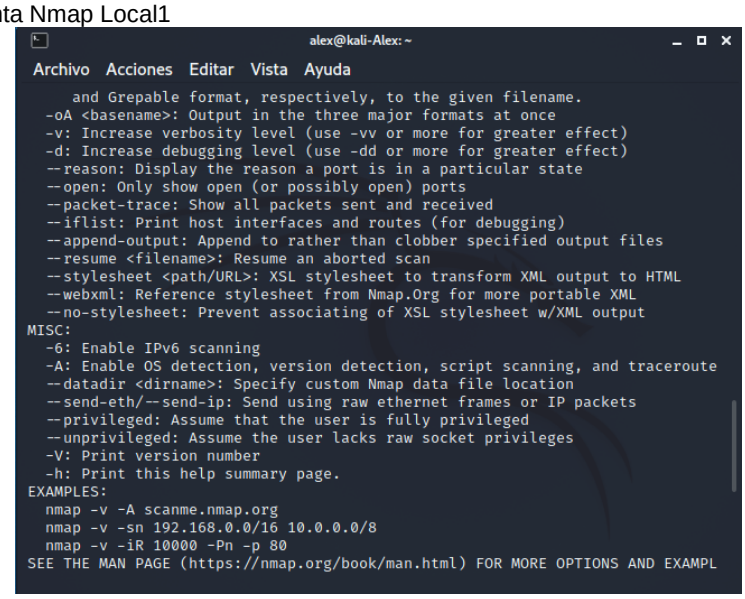
“Nmap ("Network Mapper") es un código abierto y gratuito (licencia) utilidad para el descubrimiento de redes y la auditoría de seguridad. Muchos administradores de sistemas y redes también lo encuentran útil para tareas como el inventario de la red, la gestión de los programas de actualización del servicio y la supervisión del tiempo de actividad del host o del servicio.”.[12]

Esta es otra de las herramientas que se pueden ver en el mercado para realizar ataques a las maquinas, de fácil uso, muy popular en la comunidad, por su flexibilidad, por puede hacer el escaneo de los puertos si son UDP o si son TCP, también es capaz de detectar los sistemas operativos de las maquinas atacadas sin importar su marca, por su potencia es capaz de realizar estos ataques a cientos de máquinas, de dependiendo de la red que esté trabajando, en muy amigable esta herramienta ya que su software es compatible con casi todas las versiones de sistemas operativos en la que se quiera utilizar, siguiendo con las ventajas de esta herramienta es de fácil comprensión para los novatos, porque es muy intuitiva, así

[12] (N.d.). Nmap.Org. Retrieved August 31, 2021, de https://nmap.org/

como también tiene las opciones avanzados para los más experimentados. Para continuar con este análisis de la herramienta se tomarán unas imágenes para observarla mejor.

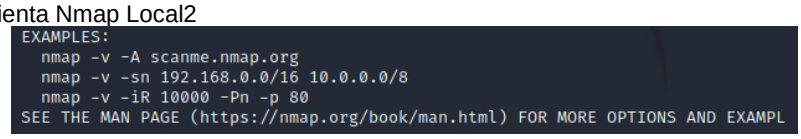
Figura 8. Herramienta Nmap Local1



Fuente: Propia

En la Figura anterior podemos ver el inicio de la herramienta por medio de la consola en donde nos indica con ejemplo como se puede iniciar con el escaneo de vulnerabilidades que se puede realizar por nombre de dominio, dirección IP, o por número de puerto, como se ve en la Figura siguiente.

Figura 9. Herramienta Nmap Local2

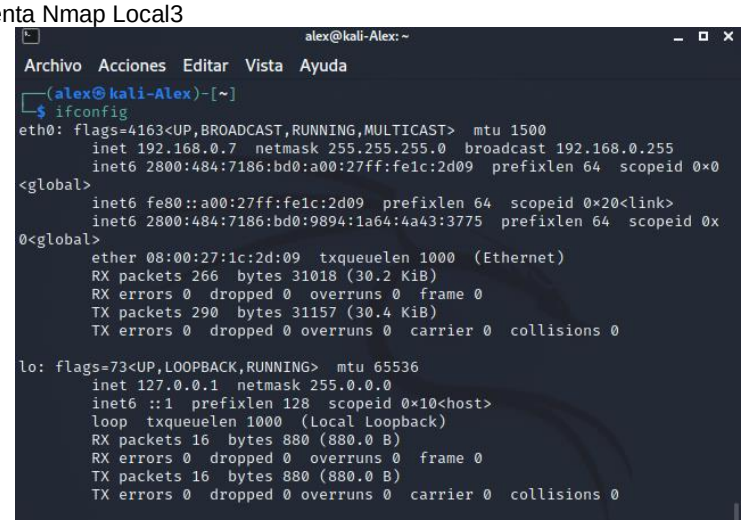


Fuente: Propia

Para ello las etapas anteriores del pentesting dieron información la cual será de mucha ayuda para empezar este tipo de ataque.

Se verifica la dirección de la maquina atacante para saber cómo esta su dirección IP, y hacer un respectivo ataque a una máquina que se configuro en un ambiente seguro y no ocasionar problemas a otras redes, incurriendo en salirnos de la ley 1273.

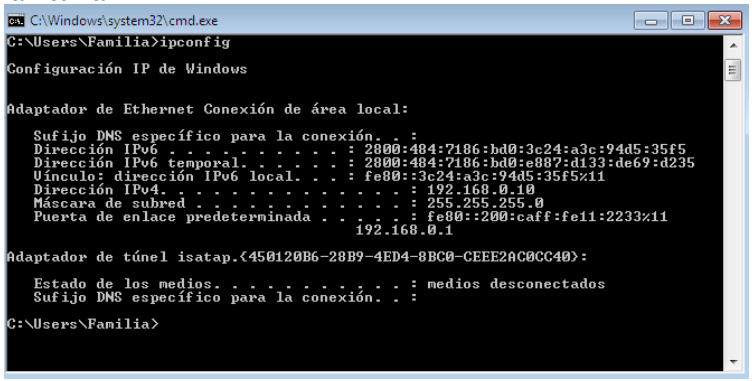
Figura 10. Herramienta Nmap Local3



Fuente: Propia

La máquina que se va atacar tiene la dirección:

Figura 11. IP maquina victima



Fuente: Propia

Con esta información se procede hacer el ataque con la herramienta Nmap y observar sus resultados.

Figura 12. Herramienta Nmap Local4 resultado

Fuente: Propia

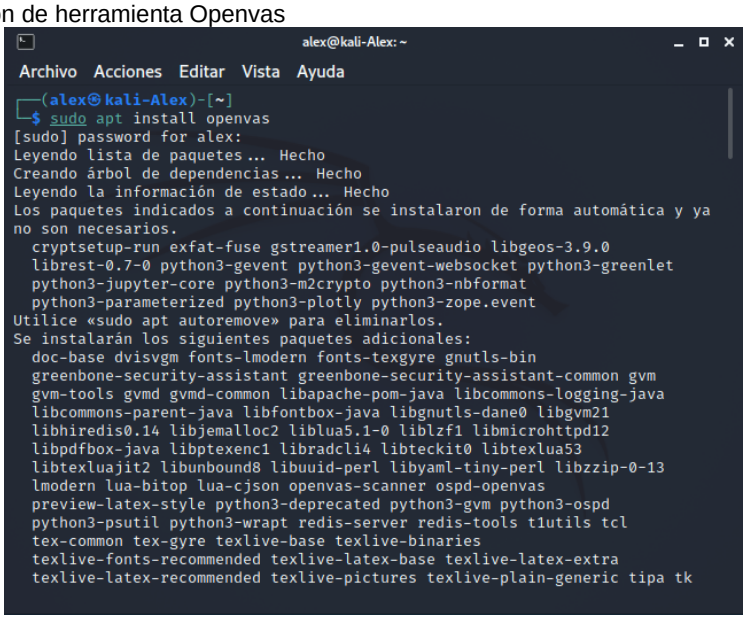
Como se observa el escaneo de esa máquina dio los resultados básicos de información, pero con consultas más complejas se pude saber mucho más.

3.3 OPENVAS

“Es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste del rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad.”.[13]

Openvas es una herramienta para realizar test que nos sirve para observar las vulnerabilidades que nos muestra de manera Figura y nos da hasta recomendaciones para mitigar esas vulnerabilidades en las machinas que queremos realizar un pentesting a continuación observaremos la instalación de esta herramienta en la máquina virtual en el sistema operativo Kali Linux creada para realizar nuestras prácticas. Previamente se tiene que realizar una actualización del sistema operativo para que tenga todas las actualizaciones.

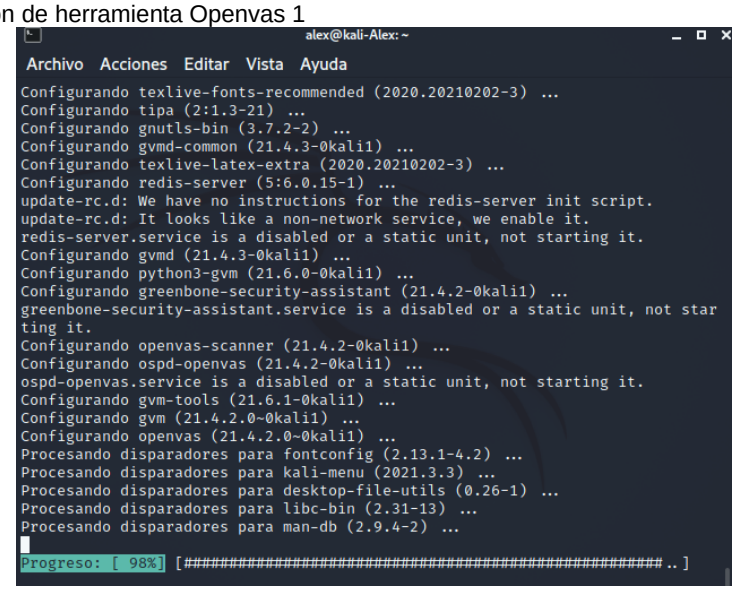
Figura 13. Instalación de herramienta Openvas



Fuente: Propia

[13] (N.d.). Openvas.Org. Retrieved August 31, 2021, from https://www.openvas.org/

Figura 14. Instalación de herramienta Openvas 1



Fuente: Propia

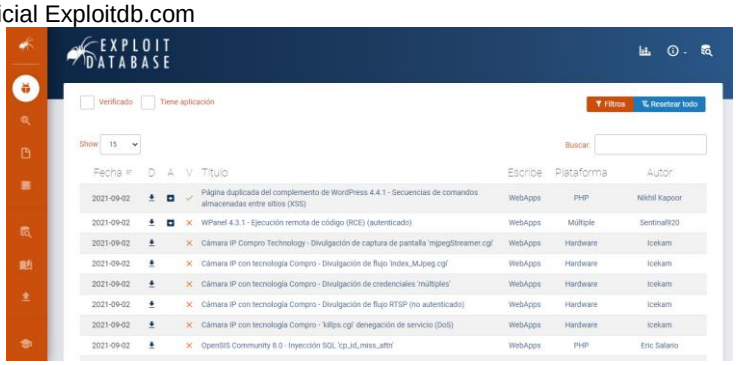
3.4 EXPLOITDB

Explitdb es una base de datos o un repositorio digital en donde reposa y es actualiza la información de los diferentes *exploit* que se pueden encontrar en la red, esto es gracias a la empresa *offensive security* de manera gratuita, donde los hackers comparten sus conocimientos sobre nuevos exploit o brechas de seguridad que se pueden encontrar en el mercado en la actualidad.

“Nuestro objetivo es servir la colección más completa de exploits recopilada a través de envíos directos, listas de correo y otras fuentes públicas, y presentarlas en una base de datos de fácil navegación y disponible de forma gratuita.”[14]

[14] Offensive Security’s Exploit Database Archive. (n.d.). Exploit-Db.Com. Obtenido septiembre 3, 2021, de https://www.exploit-db.com/about-exploit-db

Figura 15. Página oficial Exploitdb.com



Fuente: Exploit Database. (s. f.). Exploit-db.com. Recuperado 9 de septiembre de 2021, de https://www.exploit-db.com/

3.5 COMMON VULNERABILITIES AND EXPOSURES (CVE)

Es una lista de información registrada e identificada con *CVE-ID* que quiere decir vulnerabilidades y exposiciones comunes con un número de identificación, de las vulnerabilidades conocidas, o publicadas en su top 10 o informe general donde realizan una descripción sobres las mismas o del software que se encontró con esas afecciones, y sus posibles mitigaciones si es que ya se encuentra alguna.

Esta nomenclatura es aprobada y abalada por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos de Norte América, esta impórtate tarea la realiza la empresa *The MITRE Corportation* que es una organización sin ánimo de lucro, que le aporta a los Estados Unidos de América soporte sobre tecnologías de la información, investigación y desarrollo en el área de ingenieria de sistemas, por consiguiente, es el gobierno quien le da el apoyo económico a la misma.

Figura 16. Página oficial CVE - Inicio

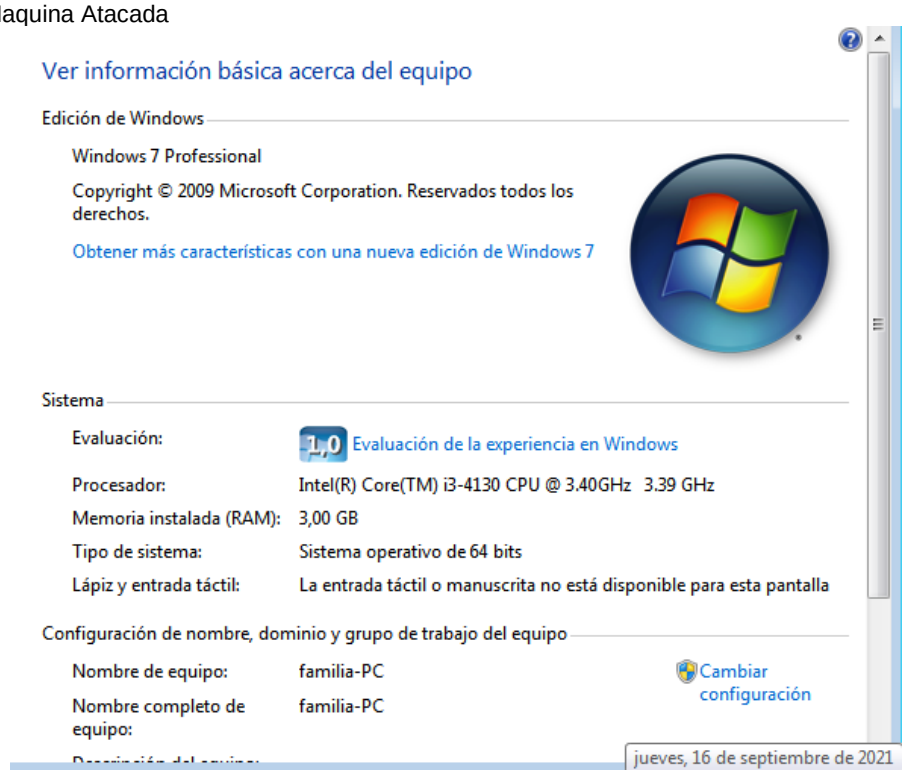
Fuente:(Dakota del Norte). Mitre.Org. Obtenido el 3 de septiembre de 2021 de https://cve.mitre.org/about/index.html

4 ANALISIS Y PRACTICA TECNICA DE VERIFICACION DE LA INFORAMCION DE LA EMPRESA THE WHITE HOUSE SECURITY MEDIANTE EL PROCESO RED TEAM.

Se procede con la primera etapa que es la de recolectar información de la máquina que se requiere testear, para eso aremos uso de las herramientas que se utilizan para hacer el ataque a la maquina requerida o previamente instala o emulada, en una máquina virtual.

Previamente se hace la verificación de la maquina como se observa para verificar las condiciones de la misma.

Figura 17. Maquina Atacada



Fuente: Propia

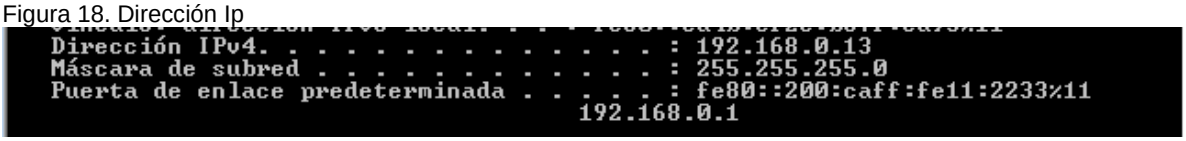
Como se observa la maquina tiene las características siguientes:

- Sistema operativo: Windows 7 a 64 bits.
- Memoria RAM 3 gb
- Procesador: Intel Core i3-4130 CPU @ 3.40 GHz

Está configurado como lo solicito los anexos anteriores para poder realizar la práctica sin problemas o salir de la parte legal.

Se verifica su dirección ip en la ventana de *cmd* con el comando *ipconfig* como se observa en la Figura 2.

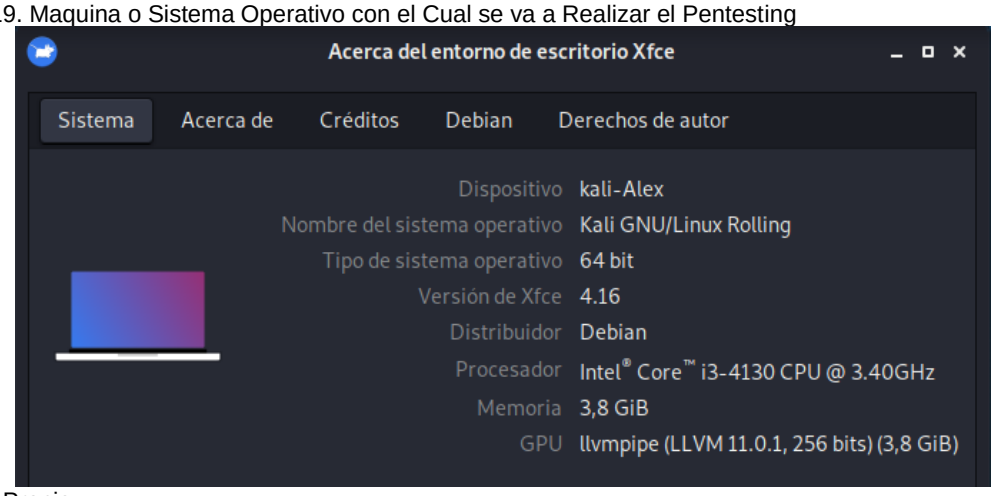
Figura 18. Dirección Ip



Fuente: Propia

Dando como resultado que su dirección ip es 192.168.0.13 lo que significa que está en la red local que necesitamos para realizar la práctica.

Figura 19. Maquina o Sistema Operativo con el Cual se va a Realizar el Pentesting



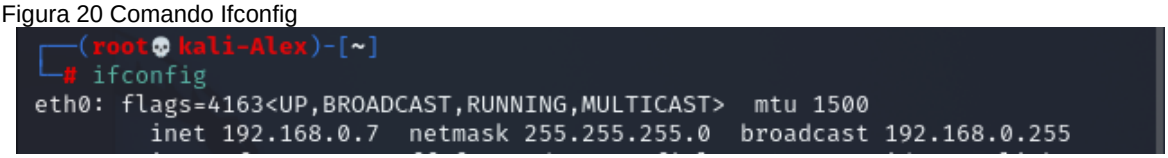
Fuente: Propia

Como se observa es una máquina que tiene y como lo solicita la rúbrica en anteriores anexos, y sus características son:

- Sistema operativo Kali Linux
- Memoria RAM de 4 gb
- Procesador Intel Core i3-4130 CPU @ 3,40 GHz

Se verifica su dirección ip en una ventana terminal con el comando *Ifconfig*

Figura 20 Comando Ifconfig

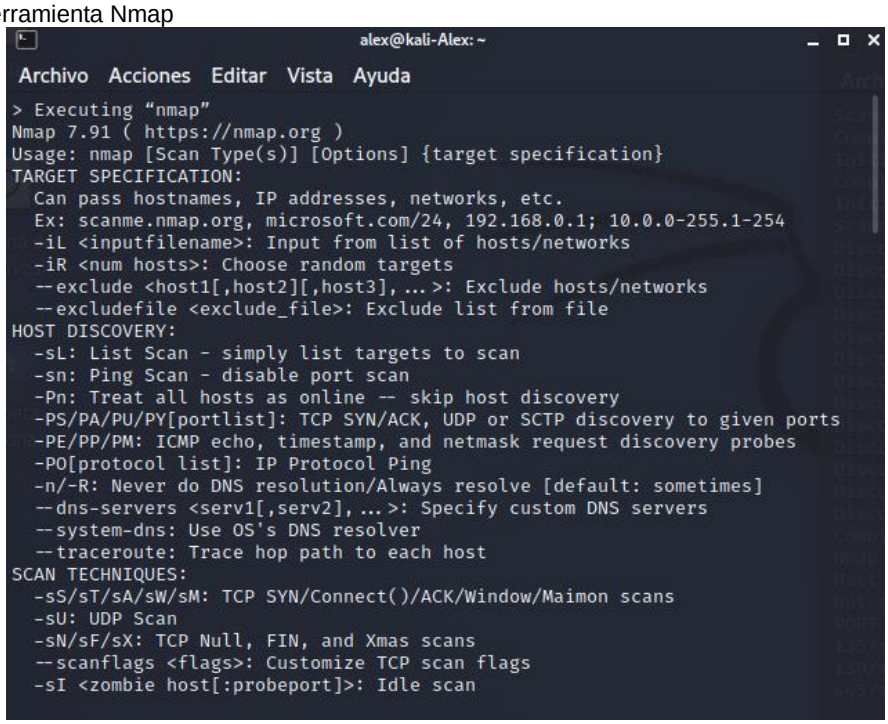


Fuente: Propia

El resultado del comando nos informa que la dirección ip de la maquina atacante es 192.168.0.7 lo que quiere decir que está en la misma red local para realizar la debida practica o ataque.

Se inicia con la herramienta Nmap:

Figura 21. Herramienta Nmap



Fuente: Propia

Ya una vez se tenga herramienta actualizada se procede con el comando *nmap –sn 192.168.0.13*

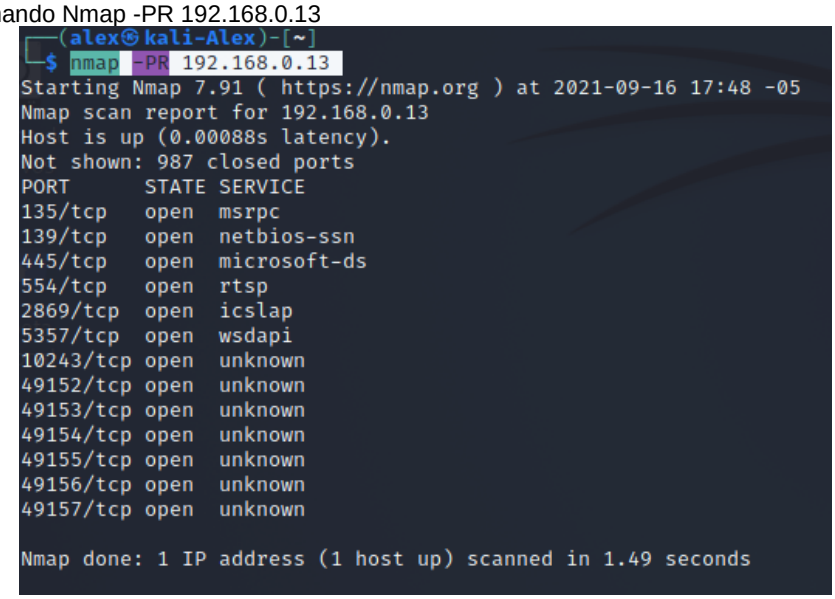
Figura 22. Comando Nmap – sn 192.168.0.13

Fuente: Propia

El resultado que nos da el comando nos informa que el host está arriba y responde positivamente, lo que nos indica que debemos realizar más comandos para saber más información del host o la maquina atacada.

Se realiza el siguiente comando *nmap -PR 192.168.0.13* para observar un poco más a fondo la máquina.

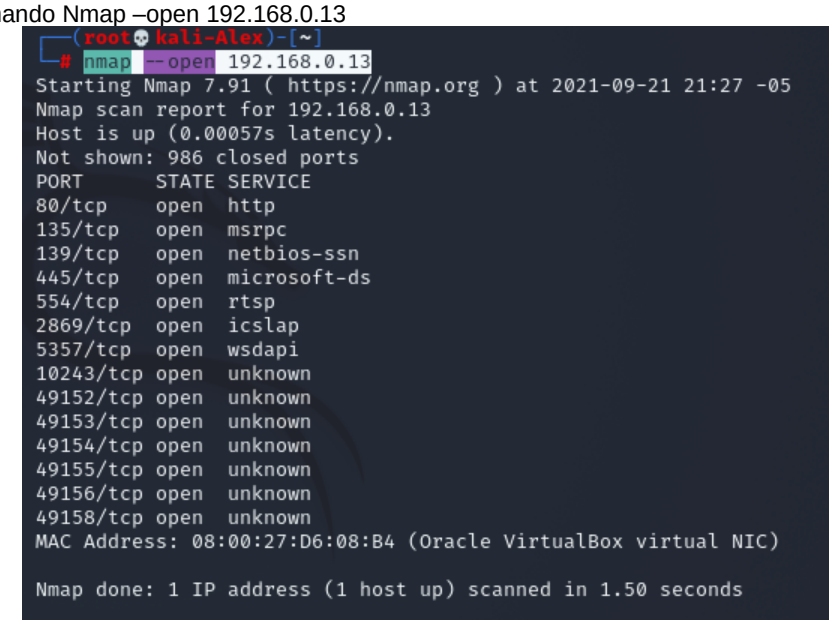
Figura 23. Comando Nmap -PR 192.168.0.13



Fuente: Propia

Lo que nos indica que 13 puertos están abiertos lo que significa que tiene vulnerabilidades que se pueden aprovechar o disponibles para ser atacados.
Se verifica esa información con el siguiente comando *nmap –open 192.168.0.13*

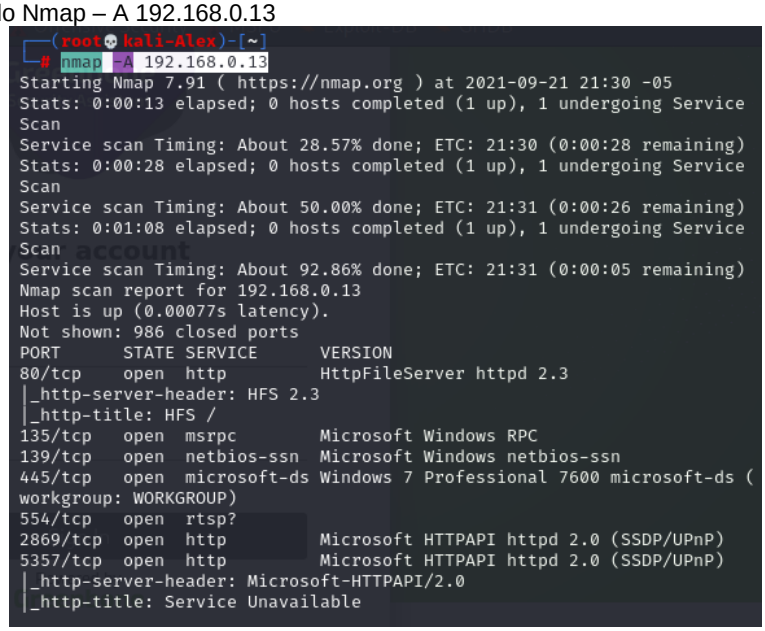
Figura 24. Comando Nmap –open 192.168.0.13



Fuente: Propia

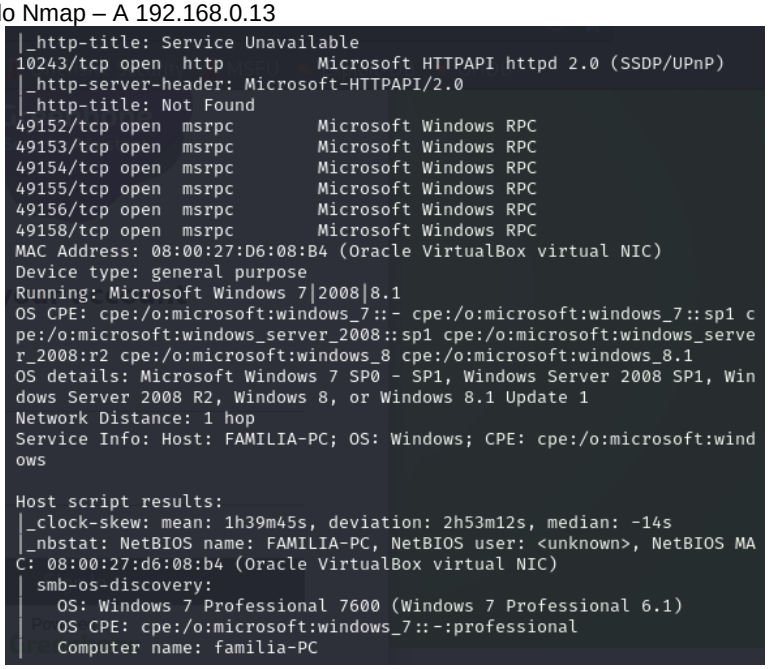
Como se observa hasta hora se tiene información básica de los puertos que están abiertos, se procede a dar un paso más con un escaneo más agresivo como lo indica nmap con el siguiente comando *nmap – A 192.168.0.13*

Figura 25. Comando Nmap – A 192.168.0.13



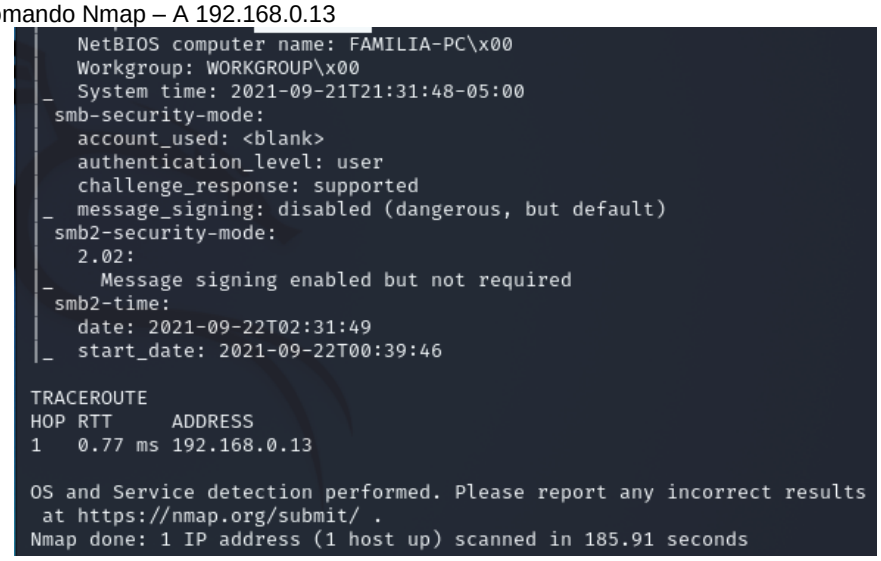
Fuente: Propia

Figura 26. Comando Nmap – A 192.168.0.13



Fuente: Propia

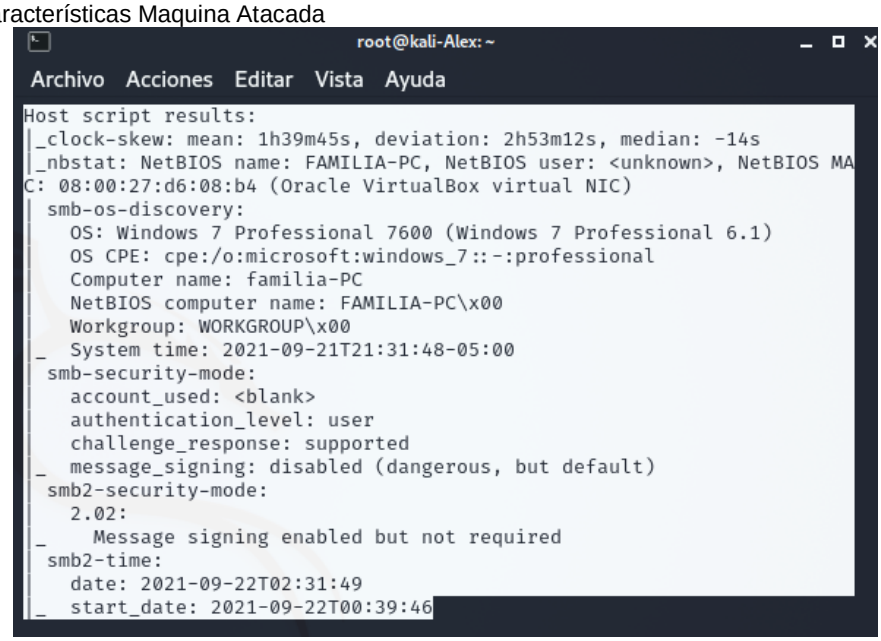
Figura 27. Comando Nmap – A 192.168.0.13



Fuente: Propia

Como se observa con este comando el resultado es mucho más completo en donde se puede ver diferentes características de la máquina que se está atacando como se observa en la siguiente *figura*:

Figura 28. Características Maquina Atacada



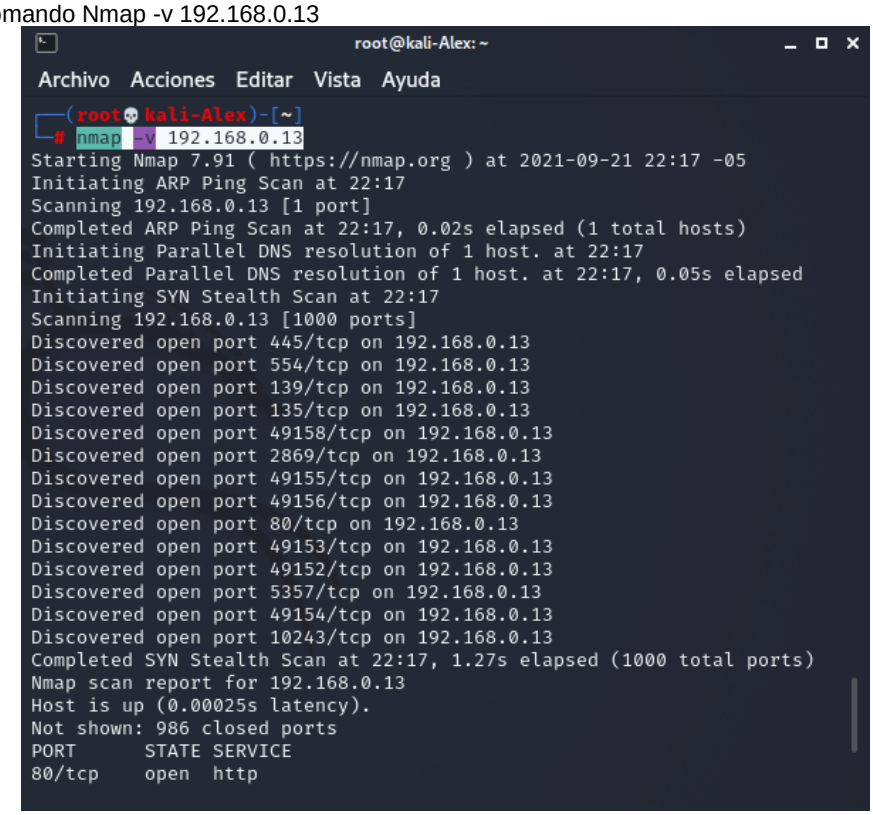
Fuente: Propia

La información que observamos es:

- Nombre del PC FAMILIA-PC
- Usuario: Desconocido.
- Su MAC 08:00:27:d6:08:b4 que esta virtualizada en Virtual Box
- Sistema operativo Windows 7 profesional en su versión 6.1
- Grupo de red WORKGROUP\x00
- Usuario o cuenta blanca
- Nivel de autenticación es de usuario

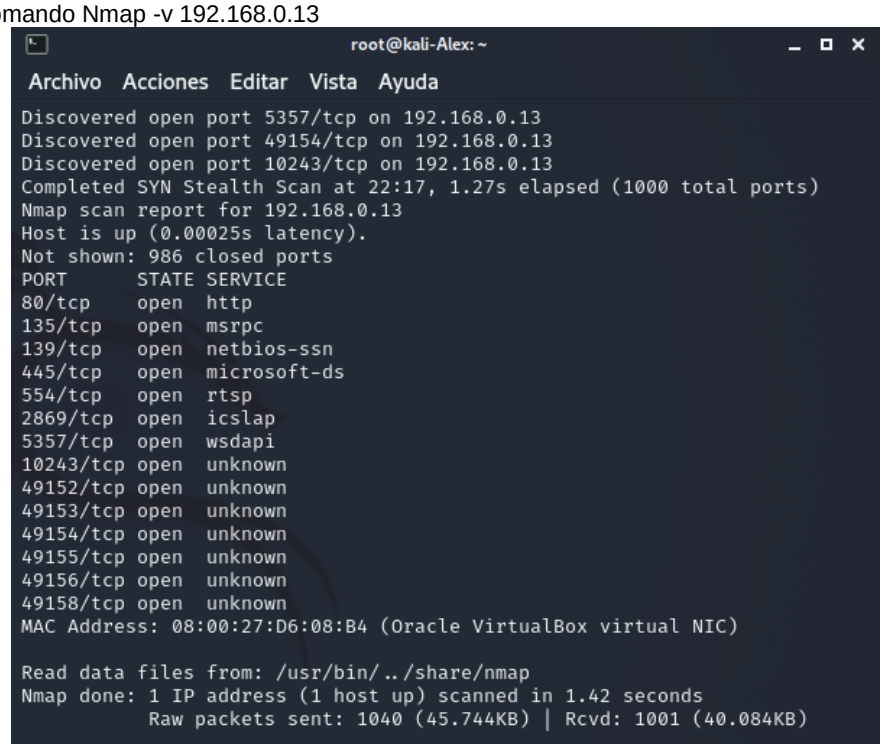
Con el comando *nmap -v 192.168.0.13* se hace un escaneo a los servicios de esos puertos para tener más información sobre ellos.

Figura 29. Comando Nmap -v 192.168.0.13



Fuente: Propia

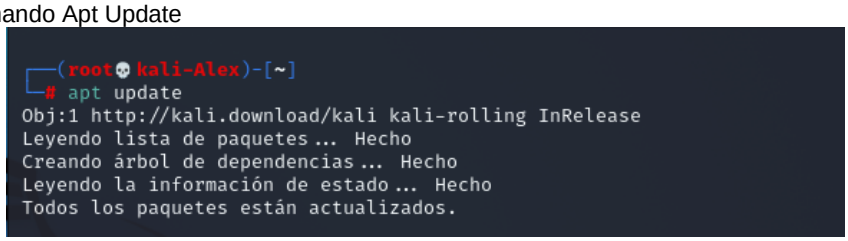
Figura 30. Comando Nmap -v 192.168.0.13



Fuente: Propia

Gracias a la ayuda de la herramienta nmap tenemos información que es muy importante para iniciar con los diferentes ataques y verificar la información para ellos vamos a tomar parte de la información y se utilizara en otra herramienta que es en este caso ***Openvas*** como lo podemos observar en la imagen siguiente en donde se inicia con la actualización del sistema operativo Kali Linux ya que debe estar con todas las actualizaciones o paquetes para eso se debe utilizar el comando *apt update.*

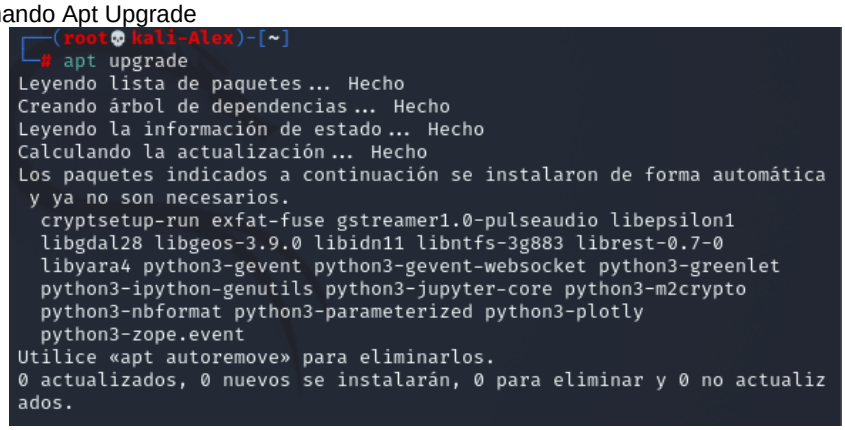
Figura 31. Comando Apt Update



Fuente: Propia

Seguido del comando apt upgrade.

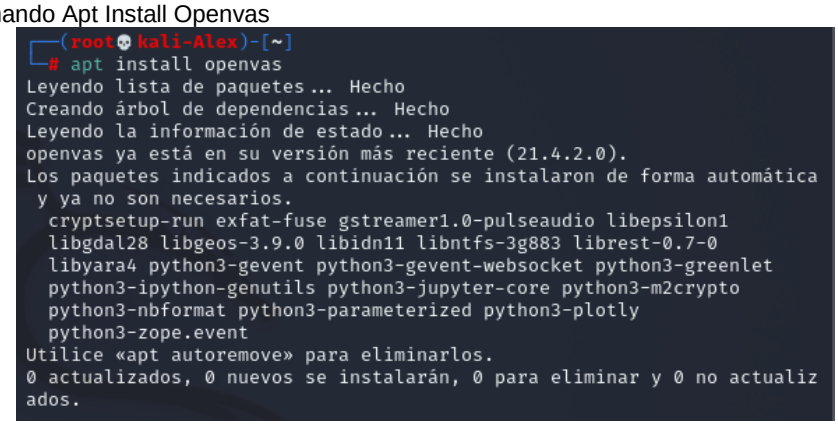
Figura 32. Comando Apt Upgrade



Fuente: Propia

Ya lista esa parte se puede realizar la instalación de la herramienta *Openvas* con el comando *apt install openvas.*

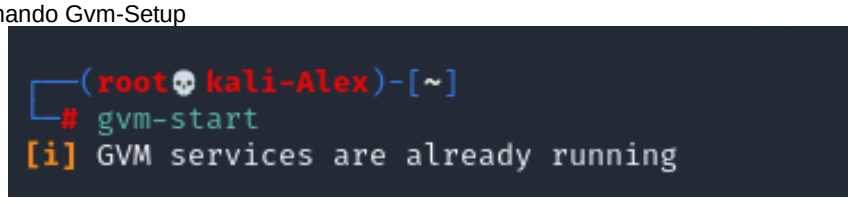
Figura 33. Comando Apt Install Openvas



Fuente: Propia

Una vez instalados todos los paquetes necesarios se inicia la configuración de la herramienta con el comando gvm-setup para realizar este comando se debe tener tiempo disponible porque esa configuración tarda más de tres horas eso depende de varias cosas como lo son la máquina y el internet que se tenga.

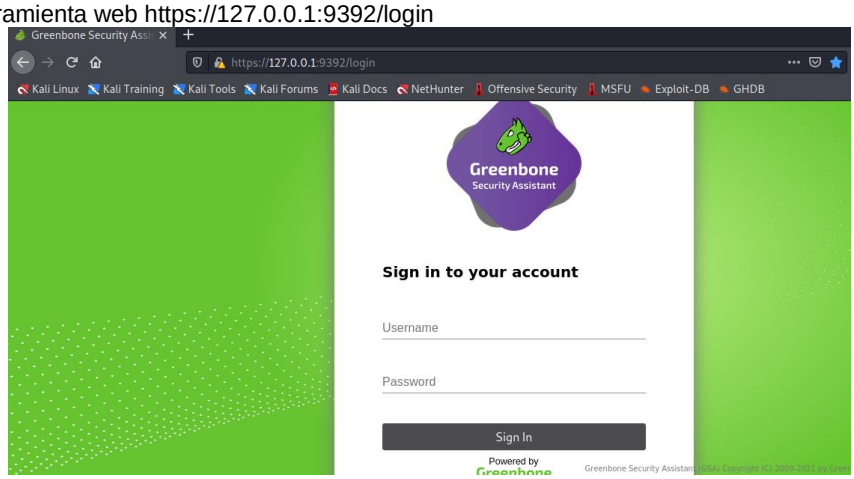
Figura 34. Comando Gvm-Setup



Fuente: Propia

Una vez se tenga el servicio corriendo, una vez acabe la configuración se debe tomar nota del usuario y contraseña que se asigna para el ingreso del programa que es una herramienta web **https://127.0.0.1:9392/login** que tiene salida por el puerto 9392 como se observa a continuación.

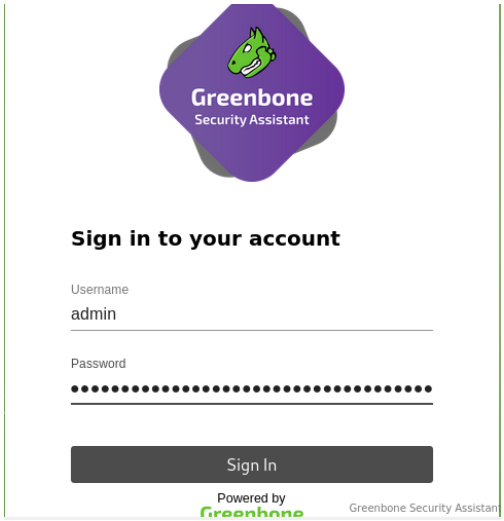
Figura 35. Herramienta web https://127.0.0.1:9392/login



Fuente: Propia

Se ingresa con las credenciales que dio el sistema al terminar.

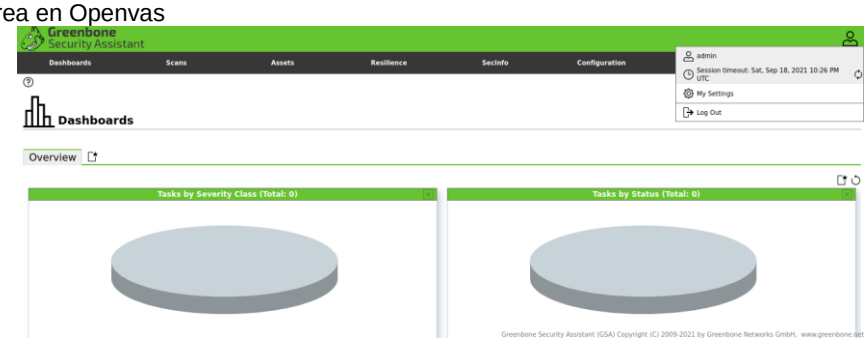
Figura 36. Login



Fuente: Propia

Una vez ingresamos a la herramienta se procede a realizar el análisis de las vulnerabilidades.

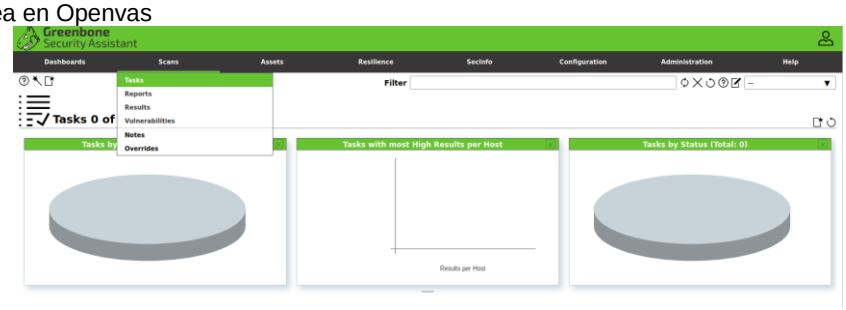
Figura 37. Tarea en Openvas



Fuente: Propia

Para iniciar con el análisis de las vulnerabilidades se debe hacer a través de su menú tareas.

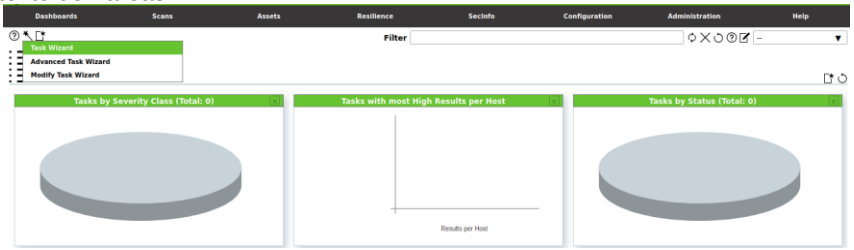
Figura 38. Tarea en Openvas



Fuente: Propia

Se realiza click en el asistente de tareas.

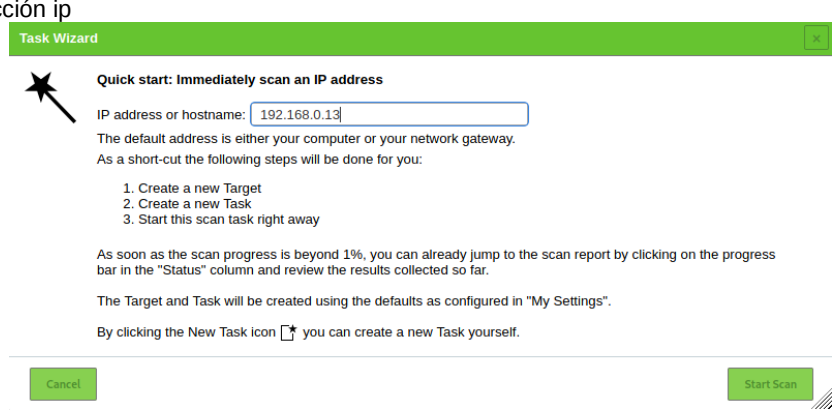
Figura 39. Asistente de Tareas



Fuente: Propia

Y es acá donde se coloca la dirección o el rango de direcciones que se quiere realizar el análisis de las vulnerabilidades para este caso es la dirección 192.168.0.13.

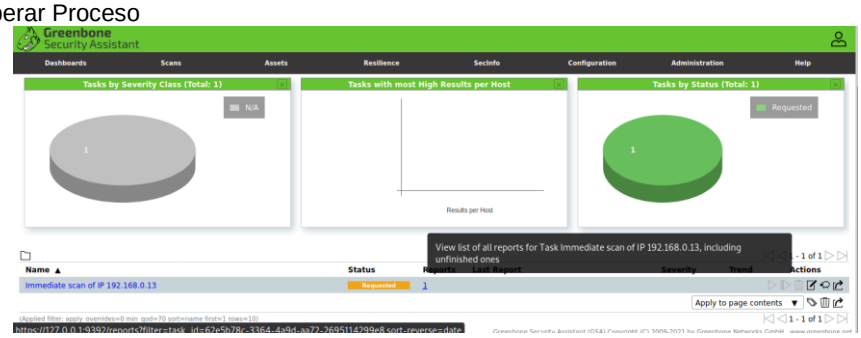
Figura 40. Dirección ip



Fuente: Propia

Se hace click en iniciar, como se puede ver la herramienta inicia a realizar la tarea se debe tener paciencia ya que se puede demorar un poco, pero se pude ir viendo su avance en la barra de estado en la parte inferior.

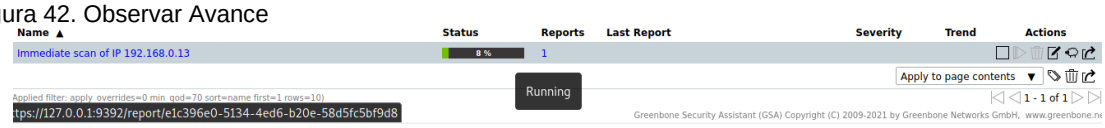
Figura 41. Esperar Proceso



Fuente: Propia

Se observa su avance:

Figura 42. Observar Avance



Fuente: Propia

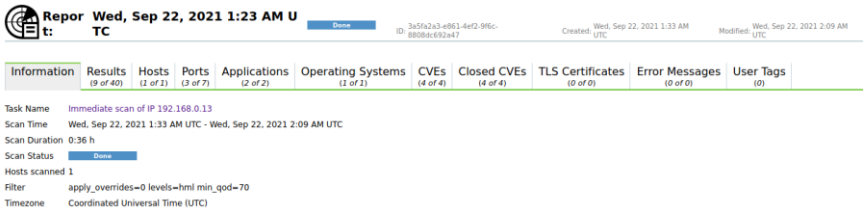
Una vez se termina de realizar el análisis de vulnerabilidades la herramienta nos ofrece varias formas de ver el resultado como lo podemos ver de manera web o si queremos descargar el reporte se puede exportar.

Figura 43. Reporte

Fuente: Propia

Se hace click en donde nos informa la fecha y la hora para ver el informe.

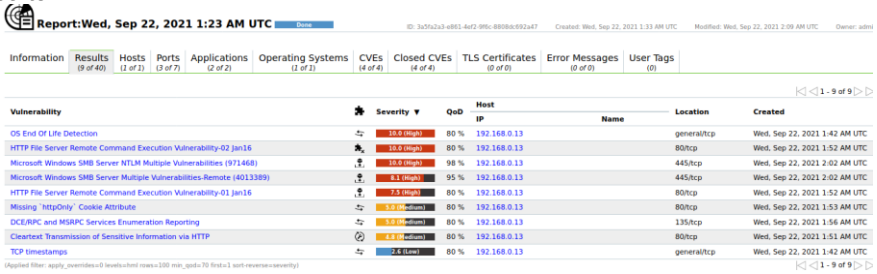
Figura 44. Reporte



Fuente: Propia

Y como se puede evidenciar encontró 40 vulnerabilidades como lo podemos observar en la pestaña de resultados que nos presenta los 9 primeros de 40 en las hojas siguientes podemos ver con mayor detalle.

Figura 45. Reporte



Fuente: Propia

La herramienta nos indica de las vulnerabilidades como su severidad con una calificación de 1 a 10 donde 10 es alta y en color naranja oscuro como esta en la Figura.

4.1 ¿QUÉ PUERTO ABRE LA APLICACIÓN O EL EXPLOIT EN LA MAQUINA ESPECÍFICA?

Para verificar las vulnerabilidades que tenía la maquina atacada se utilizó la herramienta anteriormente citada *openvas*, dando como resultado en su informe que se evidencio que el exploit *rejetto v. 2.3* abrió el puerto 80 para realizar la conexión remota y explotar su vulnerabilidad como se puede evidenciar en la siguiente figura.

Figura 46. Puerto 80

Fuente: Propia

Esto fue analizado gracias a que la información no fue proporcionada a tiempo realizando un análisis antes del exploit *rejetto v. 2.3* como se observó al momento de hacer las verificaciones de la maquina atacada al, porque se realiza la primera fase del pentesting que es la de recolección de información, observando que la instalación del sistema operativo Windows 7 64 bits que en este caso la maquina tiene como nombre de pc FAMILIA-PC estaba en limpio y al utilizar la herramienta nmap con el comando *nmap -PR 192.168.0.13* se observa que tenía unos puertos abiertos pero entre ellos no está el puerto 80 como se puede ver en la siguiente Figura.

Figura 47. Comando Nmap -PR 192.168.0.13

```
┌──(alex㉿kali-Alex)-[~]
└─$ nmap -PR 192.168.0.13
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-16 17:48 -05
Nmap scan report for 192.168.0.13
Host is up (0.00088s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

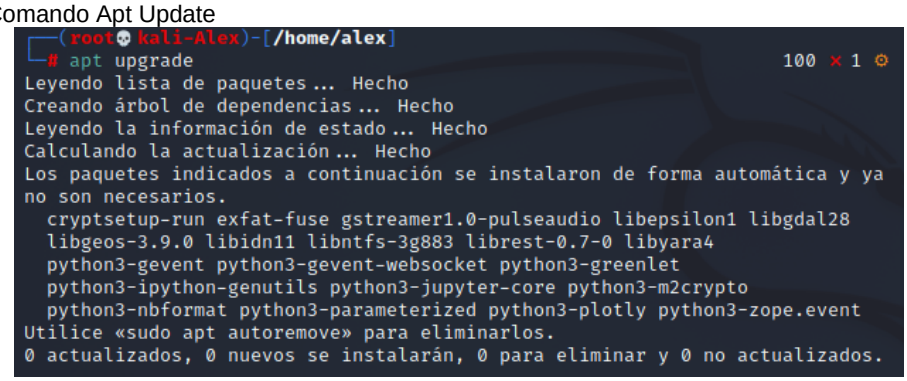
Fuente: Propia

Dando como resultado a este análisis que el exploit realizo su instalación con éxito y realizando la apertura del puerto 80, además de observar más información gracias a las demás funciones del exploit, como lo es la instalación de meterpreter.

4.2 EVIDENCIAS PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS

Primero se debe de realizar la actualización del sistema operativo Kali Linux y eso se debe realizar con privilegios de administrador *root* con el comando *apt update* se espera que se realice y se compaña con el comando *apt upgrade* se espera a que se actualicen los paquetes como lo podemos ver en la Figura y listo se puede iniciar.

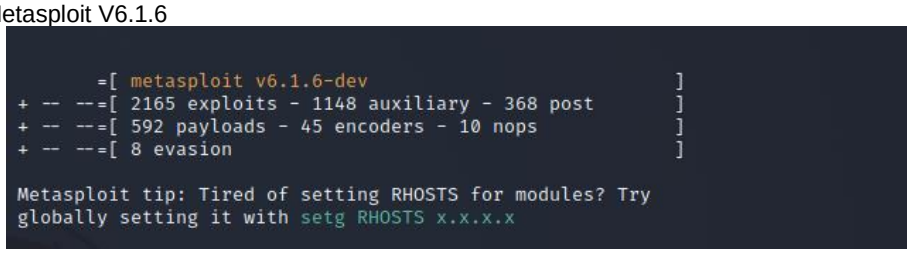
Figura 48. Comando Apt Update



Fuente: Propia

Para explotar la vulnerabilidad se necesita de la herramienta Metasploit y para ello vamos a abrirla en una consola o terminal como lo vemos a continuación.

Figura 49. Metasploit V6.1.6

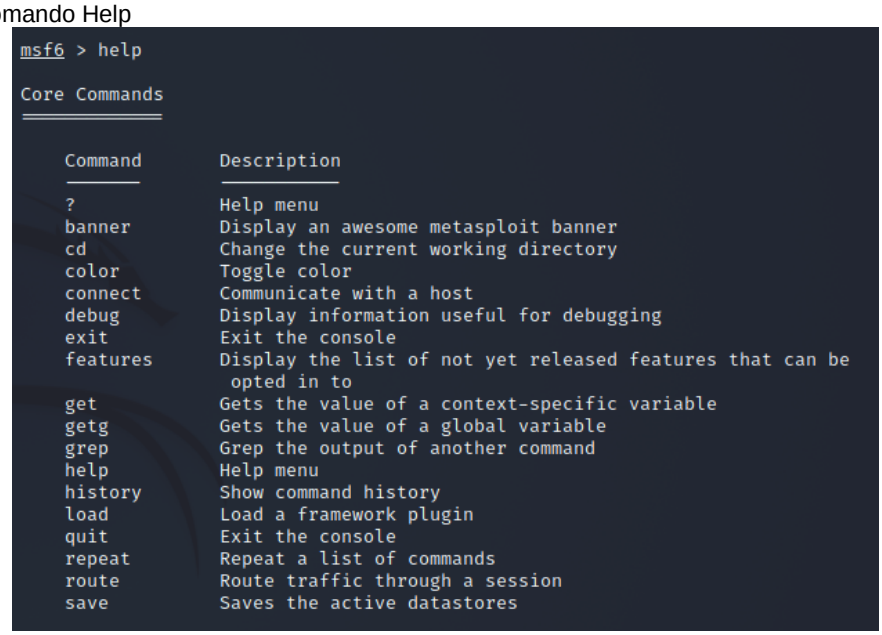


Fuente: Propia

Como se observa Metasploit está en su versión 6.1.6 se abrió sin problemas.

Se verifica los comandos para poder realizar nuestra explotación de la vulnerabilidad con el comando *help* podemos ver la ayuda de los comandos del mismo.

Figura 50. Comando Help



Fuente: Propia

Se puede realizar búsqueda de diferentes formas así que en este caso vamos a realizar la búsqueda de la vulnerabilidad por nombre con el comando *search rejetto 2.3* como lo podemos observar en la Figura.

Figura 51, Comando Search Rejetto 2.3

Fuente: Propia

Donde como vemos el resultado es positivo nos arroja que es uno de sus módulos.

Para lo cual usaremos el comando *use 0*

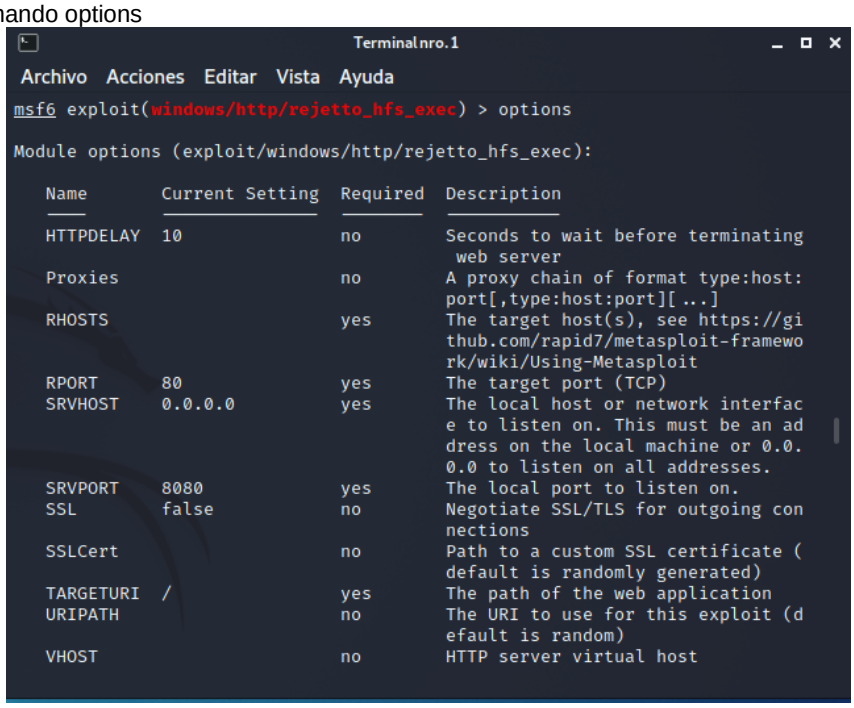
Figura 52. Comando Use 0

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > options
```

Fuente: Propia

Como se puede observar ya estamos en el módulo de exploit (Windows/http/rejetto_hfs_exec) y para observar sus opciones colocamos la palabra *options* dándonos como resultado lo siguiente.

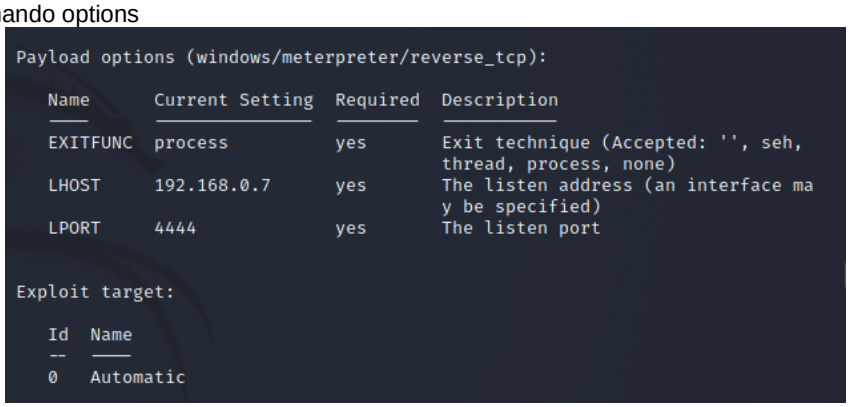
Figura 53. Comando options



Fuente: Propia

Como se observa nos indica las diferentes cosas que se puede hacer con este módulo e indicándonos que el puerto 80 está abierto con su protocolo *tcp.*

Figura 54. Comando options

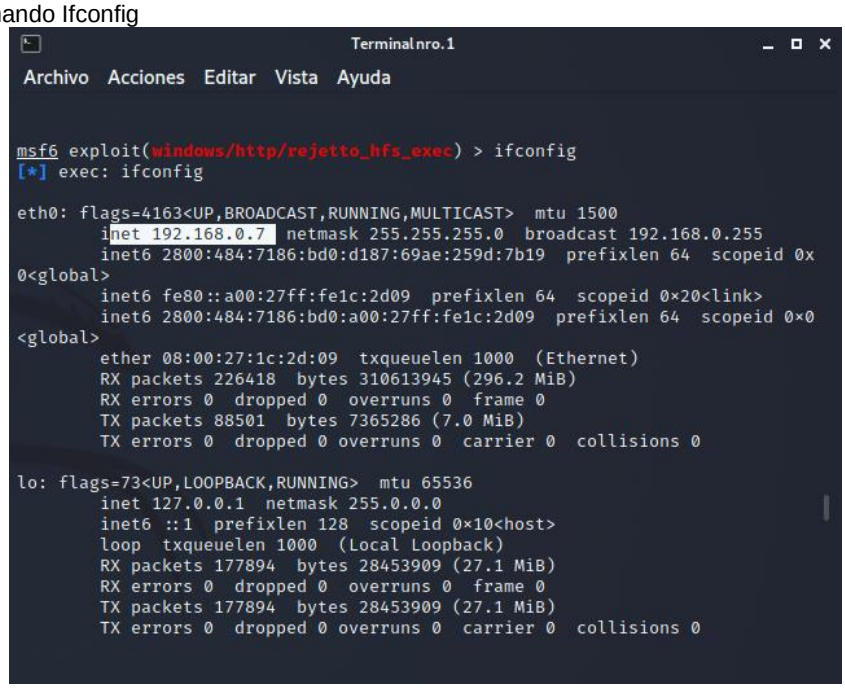


Fuente: Propia

En esta imagen se puede evidencia que la máquina que es la atacante o sea nuestro Kali Linux esta es cuchando con el nombre de *LHOST 192.168.0.7* por su puerto 4444 por defecto ósea que ya estamos listos para explotar la vulnerabilidad.

Se verifica esa información con el comando Ifconfig dándonos como resultado lo descrito anteriormente como se ve en la Figura.

Figura 55. Comando Ifconfig

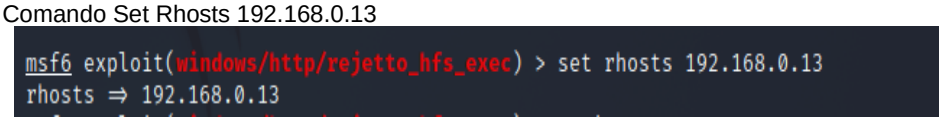


Fuente: Propia

Para tomar el control remoto de la maquina atacada como ya se ejecutó el programa o el exploit rejetto 2.3 solo se debe hacer la conexión con el comando *set rhosts*

192.168.0.13 que es la dirección de la máquina que se está atacando y su resultado lo podemos ver a continuación.

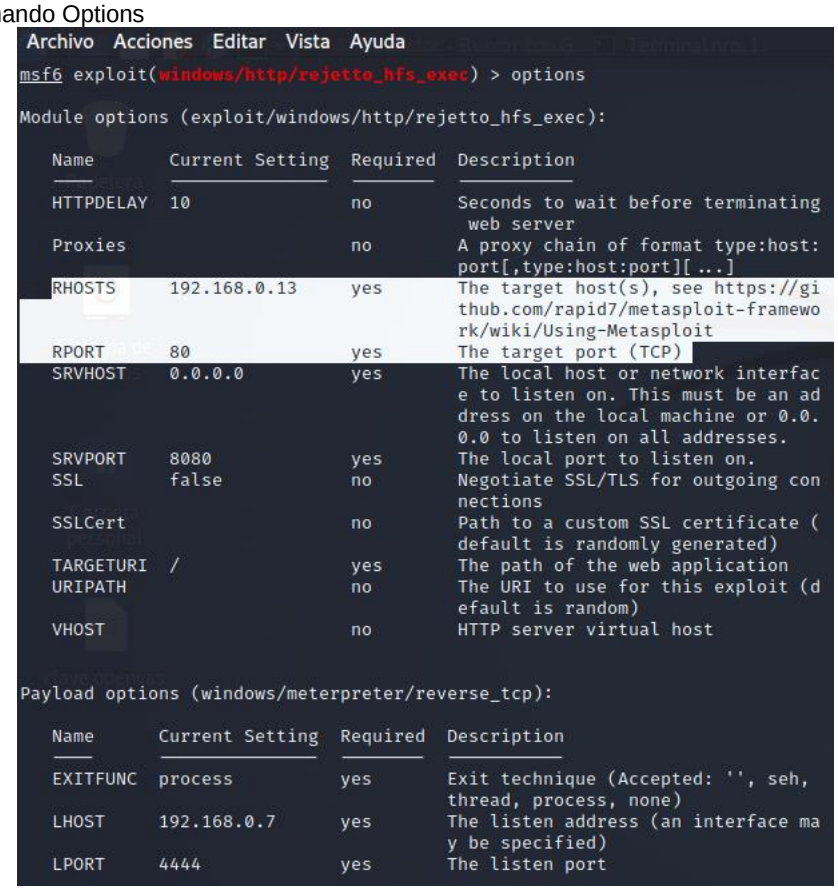
Figura 56. Comando Set Rhosts 192.168.0.13



Fuente: Propia

Para verificar eso nuevamente usamos el comando *options* dándonos como resultado lo siguiente.

Figura 57. Comando Options

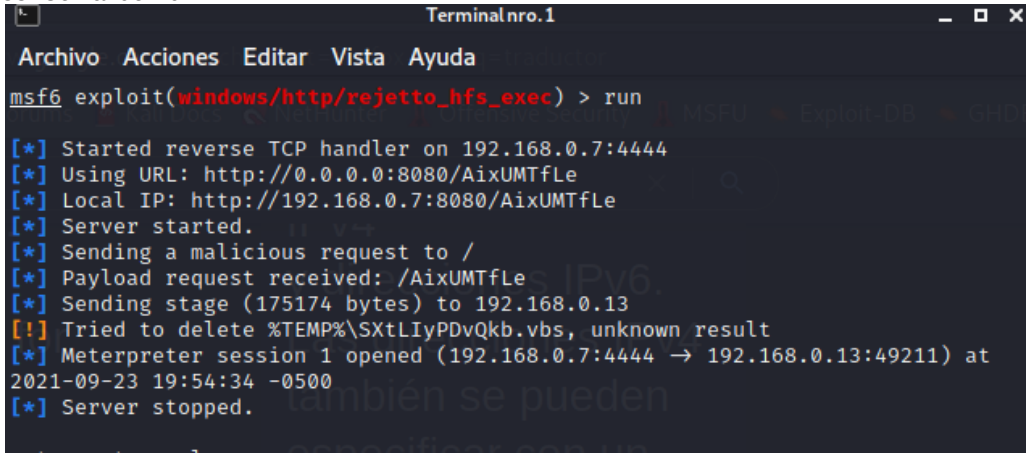


Fuente: Propia

Como se puede ver en la Figura anterior ya se está conectado a la maquina atacada, y como nosotros estamos listos escuchando para ejecutar o explotar la vulnerabilidad.

Con el comando *run* eso es posible como se evidencia a continuación.

Figura 58. Comando Run

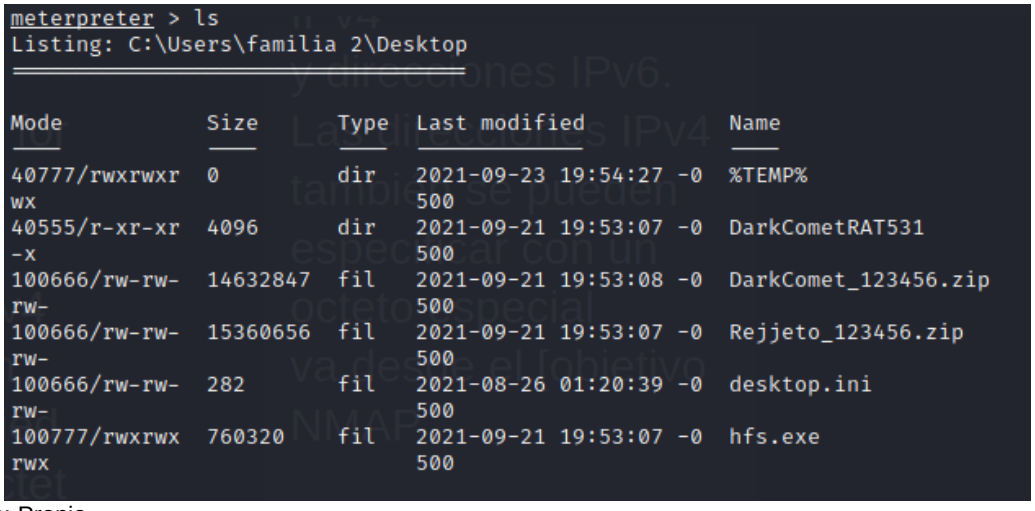


Fuente: Propia

Dando inicio a *meterpreter* para realizar o verificar la información o las diferentes características de la maquina atacada.

Para verificar los directorios o archivos de la maquina atacada con el comando *ls* se puede ver lo siguiente.

Figura . Comando Ls



Fuente: Propia

Se puede usar todos los comandos que se utilizan en Windows como un usuario normal como por ejemplo el comando *system*.

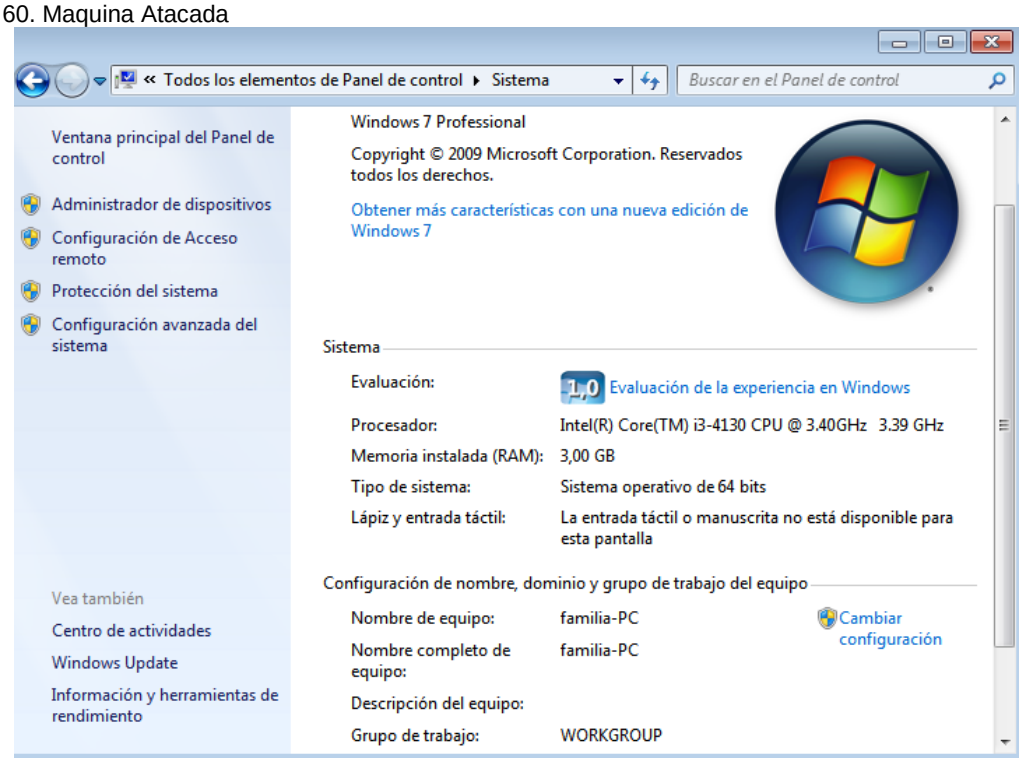
Figura 59. Comando system

```
meterpreter > sysinfo
Computer        : FAMILIA-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : es_CO
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Fuente: Propia

Se verifica la información con la maquina atacada y se observa que es la correspondiente.

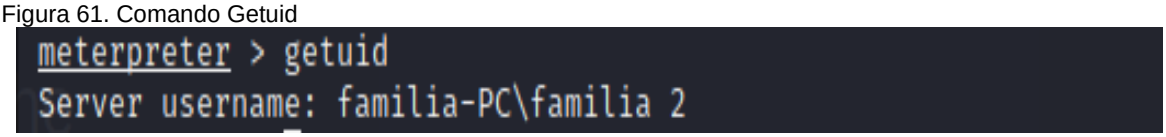
Figura 60. Maquina Atacada



Fuente: Propia

Para realizar el escalamiento de privilegios se debe hacer una serie de procedimientos para ello se verifica si ya se tiene los privilegios de administrador de la máquina atacada y se utiliza el comando *getuid* dando como resultado lo siguiente.

Figura 61. Comando Getuid



Fuente: Propia

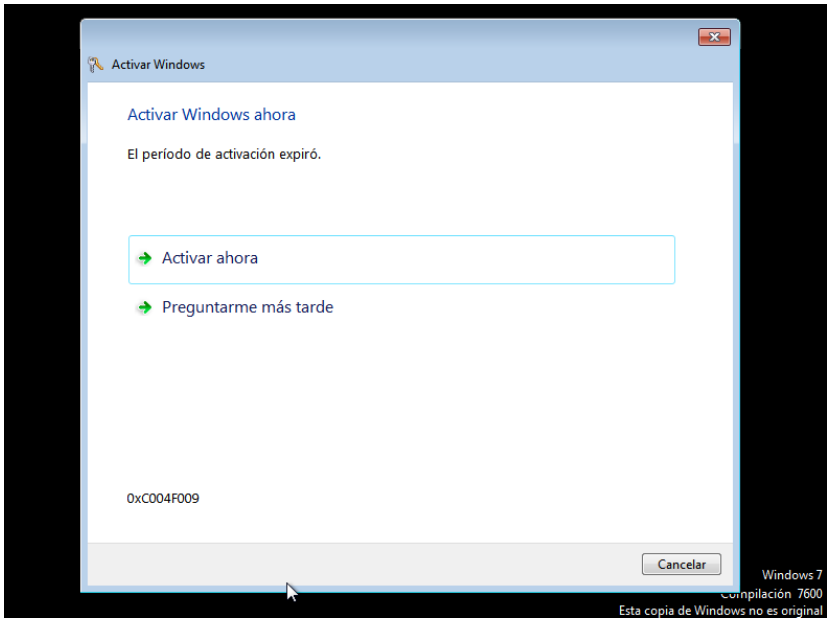
Lo que significa que no es el usuario administrador con los privilegios para realizar más cosas que un usuario normal

5 EL ENDURECIMIENTO DE LA MAQUINA PARA QUE EL ATAQUE NO SE VUELVA A PRESENTAR

Para mitigar el ataque se debe hacer la corrección de los problemas que tiene la maquina atacada con las siguientes sugerencias o recomendaciones, esto según se pueda realizar las diferentes actividades o buenas prácticas, porque eso tiene mucho que ver con las condiciones que se tengan a disposición en la empresa que se va a realizar la consulta:

- Se recomienda el realizar un borrado de todo el sistema operativo y hacer una actualización a un sistema operativo actual como Windows 11 si es posible y la maquina lo soporta, pero si no es posible el realizar esto por falta de presupuesto como lo indica el a nexo 5 escenario 4, se procede a realizar estos procedimientos.
- Activación del sistema operativo porque no está licenciado como se observa en la figura.

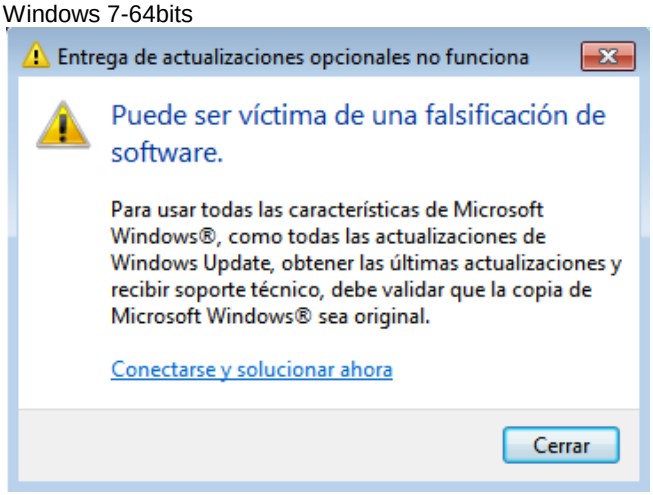
Figura 62. Activación de Windows 7-64bits



Fuente: Propia

Como se observa esta es una vulnerabilidad muy alta ya que por esa razón el sistema operativo no tiene instaladas las ultimas actualizaciones del mismo, seguridad, estabilidad, confiabilidad, integridad, para arreglar esas fallas que vienen con el sistema operativo y que a lo largo del tiempo el fabricante las lanza para arreglarlas.

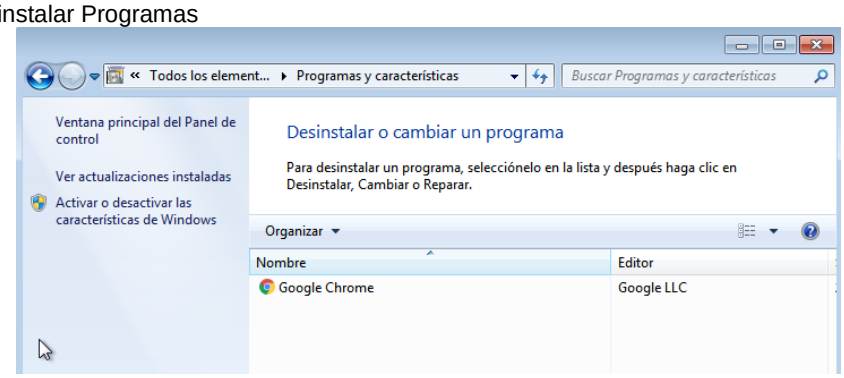
Figura 63. Activación de Windows 7-64bits



Fuente: Propia

Se debe desinstalar los programas que no sean necesarios para el trabajo que realice o utilice este pc, si se puede el aislar esta de internet.

Figura 64. Desinstalar Programas



Fuente: Propia

- Instalar todas las actualizaciones disponibles del sistema operativo hasta enero de 2020 que fue que se realizó soporte para el mismo esto debido a que ya el sistema operativo que quedo obsoleto según lo indico su fabricante.

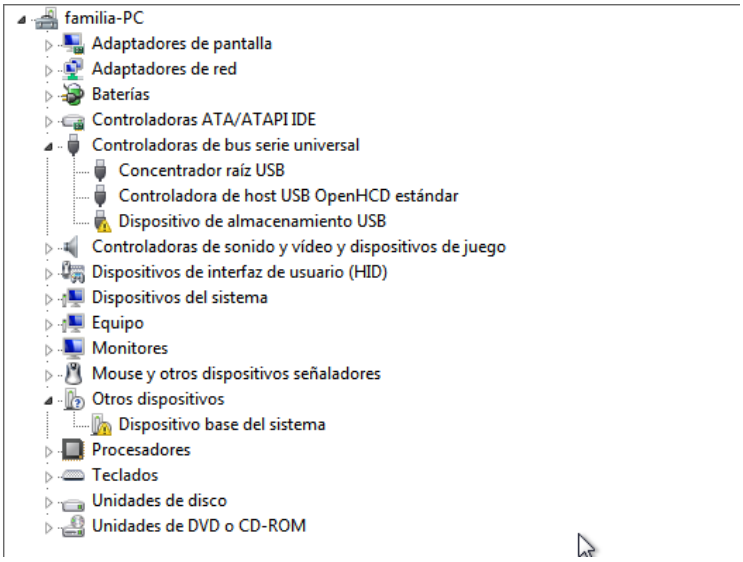
•

Figura 65. Actualización Sistema Operativo Windows 7-64 Bits

Fuente: Propia

- Instalar todos los controladores que hagan falta de la maquina como se observa en la figura.

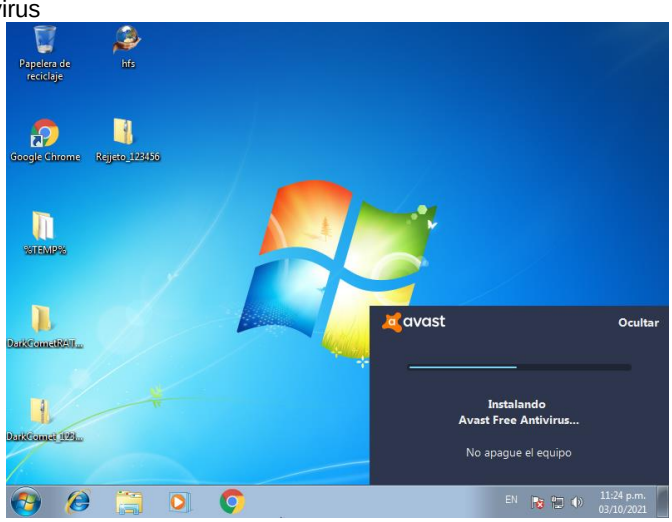
Figura 66. Drivers Windows 7-64Bits



Fuente: Propia

- Instalar antivirus licenciado o con licencia de pago de diferentes marcas si es posible, pero si no se dispone de dinero para ello utilizar los que son gratuitos en el mercado se puede encontrar varios como, por ejemplo: Se debe instalar un antivirus a si sea una de licencia gratis, no interesando la marca, pero el pc debe tener instalo un antivirus como lo muestra la figura.

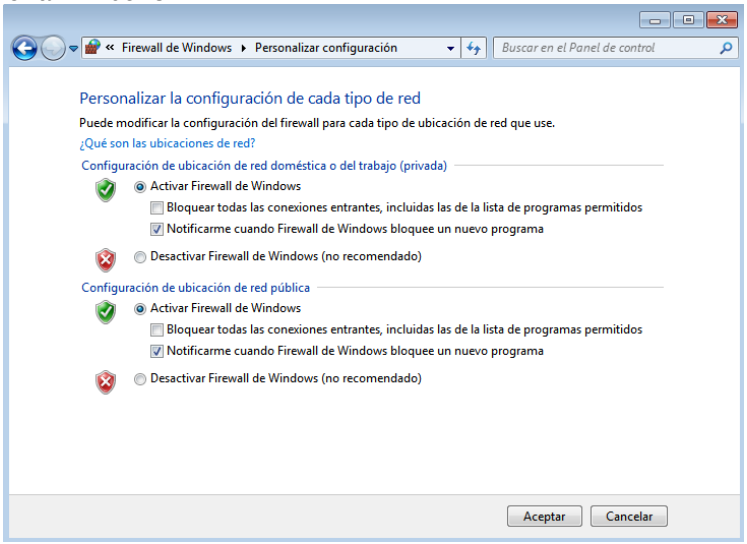
Figura 67. Instalar Antivirus



Fuente: Propia

- Activar firewall de Windows 7-64bits

Figura 68. Activar Firewall Windows



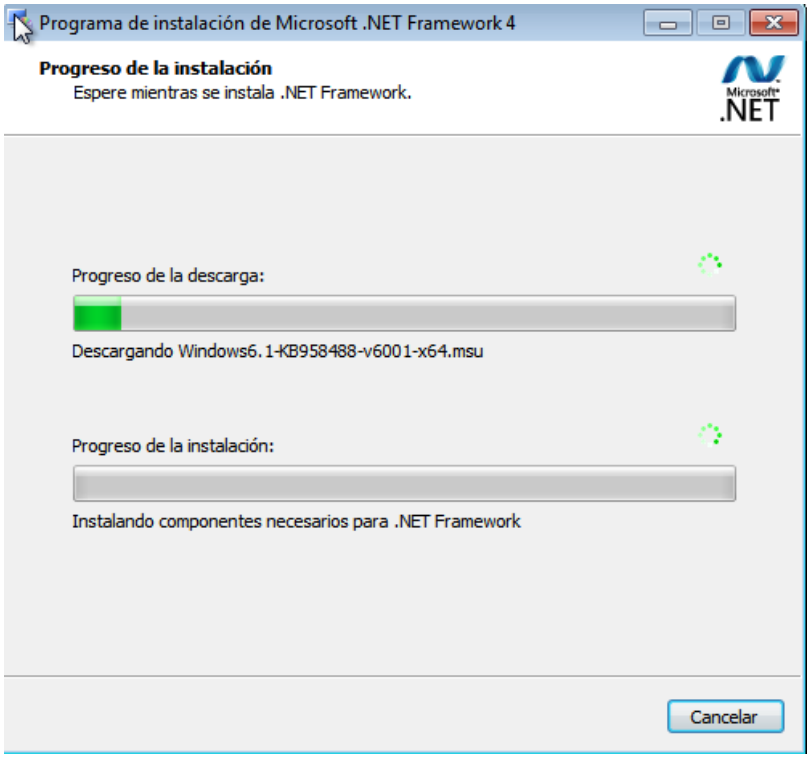
Fuente: Propia

- La máquina debe estar dentro del dominio de seguridad de la empresa.
- Se debe hacer uso de una VPN, para la conexión segura de la máquina.
- Se debe desactivar los puertos USB físicos
- Se debe realizar una capacitación a los empleados de la empresa en donde se les explique los riesgos de abrir correos de personas extrañas que no estén

relacionadas con el trabajo, que no deben abrir los archivos adjuntos de los mismos, capacitarlos en las buenas prácticas para mitigar este tipo de ataques.

- Fortalecer el firewall lógico como el físico de la empresa, actualizando las reglas de los programas permitidos por medio de listas blancas y listas negras.
- Instalar todos los framework que necesite el sistema operativo.

Figura 69. Instalar Framework



Fuente: Propia

6 EXPLIQUE Y REDACTE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LO QUE ES UN SIEM.

Un *SIEM* es el acrónimo que nace de la gestión de eventos de seguridad (*SEM*) más gestión de información de seguridad (*SIM*), quedando como resultado o reunidos gestión de eventos e información de seguridad (*SIEM)* esto debido a la necesidad de optimizar los tiempos de análisis de los datos obtenidos y poder enfocarse en el área específica debido a la falta de personal en las áreas it, que es algo habitual, pero que se debía realizar porque no sirve de nada los grandes volúmenes de información respecto a los eventos de seguridad si los datos no son analizados e interpretados para direccionar al grupo de respuesta, esto es lo que hace que esta herramienta sea muy útil para observar, determinar cuáles son los riesgos que se pueden manejar como otros que se deben priorizar y mitigar de manera prioritaria.
Las características de este software o herramienta son:

- Agrupar o reunir, centralizar el monitoreo de posibles amenazas.
- Catalogar o clasificar cuales amenazas son más importantes a la hora de solucionar o si las amenazas son un falso positivo.
- Esta herramienta ayuda a la asignación de las amenazas a los mejores analistas previamente cargados en el sistema para que su respuesta sea más rápida.
- Gracias a que el sistema proporciona o tiene una base de datos o un historial de casos se puede tener o tomar las decisiones bajo la iniciativa de estar bien documentado.
- El sistema proporciona un registro en el cual se puede hacer seguimiento a los casos o eventos para su auditoria observando cómo se les dio solución a ellos.
- La herramienta hace que sea más amigable, simple la cumplir con las reglamentaciones o estándares de la industria ya que cuenta con un formato de reporte sencillo o estándar.
-

Entre los *SIEM* que se encuentran en el mercado de uso privado o propietario, de licencia pagada se puede encontrar algunos como, por ejemplo:

- Empow
- IBM QRadar SIEM
- RSA enVision
- Security MARS
- AlienVault USM

Pero para este caso que no se tiene presupuesto ya que estas herramientas son costosas también se encuentra en el mercado herramientas de licencia abierta como lo es *elasticsearch, logshast* y *kibana* (ELK).

7 DEFINA POR LO MENOS 3 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS

Para hacer frente a las diferentes amenazas que se pueden encontrar todos los días las empresas, y para el caso que se está tratando se necesita realizar ciertas tareas o usar las siguientes herramientas que son de uso de licencia abierta, libre o de manera gratuita.

- Antivirus:
- Firewall
- Servidor proxy
- VPN

Solo por nombrar algunas de las herramientas con las que se puede mitigar las vulnerabilidades.

Aunque que existen sistema de prevención de intrusos (*IPS)* que son de licencia paga, que nacen o eran conocidas como sistema de detección de intrusos (*IDS*), que eran un complemento a un firewall para las redes y estaban siempre en ejecución atentos a la detección de ataques y entrar a responder al ataque y esto se logra gracias a la inteligencia artificial (*IA*) que realiza el estudio o el monitoreo de los comportamientos de los picos de la red y de la información o las horas de trabajo.

Esto lo logran porque no solo están basados en el monitoreo de actividades sospechosas en la red ose direcciones ip o los puertos como lo realizan los firewalls estos realizan su actividad realizando el control del acceso basados en el contenido de los paquetes.

Lo que hace que *IPS* se diferencie de *IDS* es que realiza la protección de manera proactiva y no reactiva como lo hace el *IDS.*

Dentro de los IPS de código abierto esta *Snort IPS*, en su forma más básica ya que las reglas, si depende del tipo de consumidor que se pueden o no obtener de manera gratuita o pagando por ellas.

Como se puede ver es un *IPS* por medio de software y aunque es uno de los mejores, pero una buena práctica nos indica que puede ser una herramienta que trabaje de manera paralela a la red para no generar un cuello de botella.
Como se trata de que el *IPS* sea una herramienta que haga su trabajo pero que no afecte el rendimiento de la red se puede escoger que tipo de IPS es el que más se adapta a las necesidades de la empresa por eso se debe de analizar muy bien cuál es el más favorable

Y entre ellos se encuentran los que se menciona a continuación ya que todos están bajo los mismos estándares de calidad.

- Basadas en firmas, como su nombre lo indica que trabaja buscando sobre una base de firmas conocidas para tomas las decisiones sobre ataque conocidos.
- Basado en anomalías: el sistema realiza un monitorea sobre el comportamiento de la red y al verificar una anomalía en su comportamiento lo que hace es que bloquea el acceso al pc de destino.
- Basado en políticas: eso depende de la empresa y sus políticas de seguridad, como de su infraestructura lo que con lleva a una programación o configuración específica para su red que no sobre pase sus políticas de seguridad que si se trata de salir de sus lineamientos envía una alerta al administrador para que realice la acción.

Uno de ellos es el *firewall NGFW* que es de última generación promete que cumplirá con esos requerimientos del mercado.

En el mercado se puede encontrar más *IPS* como o empresas que ofrecen sus servicios profesionales como *i4conAnalytics* que es basado en software que se instala en el firewall en donde la lista IPS se actualiza cada 15 minutos.

CONCLUSIONES

Se analizo las diferentes leyes que en este momento están rigiendo en Colombia desde el año 2009 y para esto se realizó la instalación de un ambiente virtual para más adelante realizar las practicas que nos soliciten y no incurrir en ninguna falta grave de la ley.

Analizando las leyes y los decretos se evidencia la importancia de hacer saber esta ley a los usuarios, para que sea un des motivante al realizar este tipo de actividades que se salen de la ley y que ya son penalizados.

Para realizar este tipo de prácticas es importante el realizarlo en ambientes controlados y no realizar actos ilícitos, es muy importante para los profesionales el conocer estas herramientas y bases de datos de exploit o los repositorios en donde la información nos puede ayudar a estar al día con las amenazas que van utilizando los ciberdelincuentes.

A lo largo de esta actividad se pudo evidenciar la importancia de la buena comunicación entre el área de sistemas, el área de la alta gerencia, dueños de las empresas que solicitan el estudio de un grupo de red team ya que aunque se estén muy preocupados por las consecuencias de los actos vistos o que se presumen por muy mal que este el panorama o la situación se debe establecer canales de comunicación claros y asertivos con la partes anteriormente citadas, ya que si se encuentran hallazgos de fuga de información se debe tomar con la mayor altura la situación.

Respetando los procesos, tramites, tiempos para llegar a tomar las evidencias del caso esto se debe aclarar a las partes relacionadas con el caso, ya que esto por lo general con lleva tiempo esfuerzo y dinero, y muchas veces los resultados no son muy alentadores.

Para este caso en especial se evidencia que se realizó una fuga de información a través de una máquina que fue atacada y vulnerada a través de la conocida vulnerabilidad rejetto 2.3, que en su momento realizo mucho daño, por diferentes factores que los analizamos con anterioridad dando una falla de, seguridad, integridad, en la información que se pudo a ver evitado, realizando uso de las mejores prácticas en cuanto a la configuración de la máquina.

Porque la maquina estaba sin seguridad alguna como se evidencio en el ejercicio donde la maquina no tiene ningún antivirus, firewall instalados, lo que es una falla de seguridad alta, no tiene instaladas las actualizaciones del respectivo sistema operativo, lo que es también una falla de seguridad alta que se debe mitigar lo más pronto posible.

El ataque se realizó por una persona que tiene los conocimientos avanzados para realizar este tipo de ataque, porque es necesario que tenga bastantes conocimientos de los sistemas operativos a los cuales quiere afectar por más que es una vulnerabilidad ya conocida y documentada pero que en su momento no se conocía de ella mucho y no se tenía idea de cómo solucionarla o mitigarla por eso fue utilizada por la persona para realizar la filtración de información.

Para que se solucione o se mitigue este tipo de casos o de vulnerabilidades es preciso que se cuente con el personal idóneo y capacitado para hacer frente a este tipo de situaciones, lo que con lleva a que el personal debe estar siempre capacitándose y buscado donde están los puntos débiles de la red de la empresa para que se fortalezcan y no sea un tema recurrente, lo que significa que se debe designar presupuesto para que se utilice en la red y en los computadores de la empresa afectada.

Esto se debe a que se descuida la infraestructura de la empresa no solo en la parte económica, sino en la parte de la responsabilidad de los empleados en ser el primer anillo de seguridad en cuanto detectan un comportamiento extraño en la red, como en los correos entrantes y salientes de la empresa, lo que hace que se deba responsabilizar a los usuarios en sus funciones que hagan un buen uso de los pc de la empresa como de la información sensible si la manejan, por ello se debe de capacitar al personal con frecuencia para que no pasen por alto este tipo de cosas, evitando que se vuelva a repetir si es posible aunque este tema es un tema de todos los días ya que todos los días salen nuevas y mejores vulnerabilidades que deben ser mitigadas por el área correspondiente.

RECOMENDACIONES

Es muy importante el realizar la documentación de los ataques llegado el caso, alimentando los diferentes programas o herramientas que disponga la empresa, para que en una nueva oportunidad la base del conocimiento del ataque no se pierda y sea mucho más fácil el responder a los mismos solo que su tiempo de respuesta y mitigación serán mucho mejor o si debido a la base del conocimiento no se vuelve a presentar mucho mejor, que será el deber ser de los objetivos del área de seguridad informática o de la información.

Es de vital importancia el estar verificando los informes de seguridad de las autoridades correspondientes así como sus nuevos reportes de seguridad, para aprender de las nuevas vulnerabilidades, ataques, que suelen estar documentados en sus informes y esa información la podemos aplicar de manera ética y legal para nuestro beneficio o de la empresa en la que estemos trabajando para aplicarla en la misma y con ello nos evitamos dolores de cabeza el día de mañana cuando los ataques lleguen ya se sabe cómo se puede evitar que se salga de control el mismo.

El ser proactivos frente a los ataques nos ayudara en el trabajo, en el hogar o en lo personal porque la información es el activo que más vale hoy en día.

Aunque no se tenga presupuesto para las herramientas es muy importante el aprender, a utilizar, configurar y administra las mismas que el mercado ofrece y que existen muchas herramientas de código abierto que nos pueden ayudar con el tema de los ataques ya sea de manera proactiva, como reactiva, o de monitoreo.

BIBLIOGRAFÍA

(N.d.). Cursodehackers.Com. Retrieved August 31, 2021, from http://www.cursodehackers.com/metasploit.html

(N.d.). Nmap.Org. Retrieved August 31, 2021, from https://nmap.org/

(S. f.). Helpsystems.com. Recuperado 4 de octubre de 2021, de https://www.helpsystems.com/es/blog/que-es-un-siem

(S. f.-a). Vuldb.com. Recuperado 23 de septiembre de 2021, de https://vuldb.com/es/?id.71861

(S. f.-b). Cert.org. Recuperado 23 de septiembre de 2021, de https://www.kb.cert.org/vuls/id/251276

¿Qué es ELK? ElasticSearch, Logstash y Kibana. (2018, julio 30). Openwebinars.net. https://openwebinars.net/blog/que-es-elk-elasticsearch-logstash-y-kibana/

Active el Firewall de cualquier sistema (Windows/Linux) o hardware corporativo. (2019, noviembre 25). Incibe.es. https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/active-el-firewall-cualquier

Alejandro. (2018, febrero 22). Mejores IDS Opensource para Detección de Intrusiones. Protegermipc.net. https://protegermipc.net/2018/02/22/mejores-ids-opensource-deteccion-de-intrusiones/

Avance Jurídico Casa Editorial Ltda. (s/f). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. Gov.co. Recuperado el 30 de agosto de 2021, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Colaboradores de Wikipedia. (Dakota del Norte) Explotar. Wikipedia, la enciclopedia libre. Obtenido el 3 de septiembre de 2021 de https://es.wikipedia.org/w/index.php?title=Exploit&oldid=137080875

Computer Network Defense. (s. f.). Archive.org. Recuperado 3 de octubre de 2021, de https://web.archive.org/web/20160425120250/https://www.sypriselectronics.com/information-security/cyber-security-solutions/computer-network-defense/

CVE - Home. (n.d.). Mitre.Org. Obtenido septiembre 3, 2021, de https://cve.mitre.org/about/index.html

CVE - Inicio. (Dakota del Norte). Mitre.Org. Obtenido el 3 de septiembre de 2021 de https://cve.mitre.org/about/index.html

CVE - Search Results. (s. f.). Mitre.org. Recuperado 23 de septiembre de 2021, de https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=rejetto

CVE-2020-13432. (2020, junio 8). Incibe-cert.es. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-13432

Evolución en el uso de herramientas de seguridad informática en Instituciones de Educación Superior de México. (s. f.). Unam.mx. Recuperado 4 de octubre de 2021, de https://revista.seguridad.unam.mx/numero29/evolucion-herramientas-seguridad-ies

Familia de productos Nessus. (2019, mayo 14). Tenable.com. https://es-la.tenable.com/products/nessus?tns_redirect=true

Guía de referencia de Nmap (Página de manual). (s/f). Nmap.org. Recuperado el 30 de agosto de 2021, de https://nmap.org/man/es/index.html

Guía Normas APA. Normas-apa.org. Recuperado 25 de septiembre de 2021, de https://normas-apa.org/wp-content/uploads/Guia-Normas-APA-7ma-edicion.pdf

Homepage - CIS. (2016, diciembre 6). Cisecurity.Org. https://www.cisecurity.org/

How your red team penetration testers can help improve your blue team. (2015, agosto 18). Archive.org. https://web.archive.org/web/20160530230034/http://www.scmagazineuk.com/how-your-red-team-penetration-testers-can-help-improve-your-blue-team/article/431023/

IPS: Sistema de Prevención de Intrusos. (s. f.). Infotecs.mx. Recuperado 4 de octubre de 2021, de https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html

IT Digital Media Group. (2018). ¿Qué es un Blue Team y cómo trabaja? | Actualidad | IT Digital Security. https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

Justicia. (2020, diciembre 18). Hacker Andrés Sepúlveda saldrá de la cárcel por decisión de juez. El Tiempo. https://www.eltiempo.com/justicia/delitos/juez-deja-en-libertad-al-hacker-andres-sepulveda-555749

Ley 57 de 1887 - EVA - Función Pública. (Dakota del Norte). Gobernador Co. recuperado el 3 de septiembre de 2021 de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=39535

Meskauskas, T. (2020, febrero 18). Cómo eliminar Troyano Meterpreter - guía para eliminar virus. Pcrisk.es; PCrisk. https://www.pcrisk.es/guias-de-desinfeccion/9601-meterpreter-trojan

NVD - CVE-2014-6287. (s. f.). Nist.gov. Recuperado 23 de septiembre de 2021, de https://nvd.nist.gov/vuln/detail/CVE-2014-6287

Offensive Security's Exploit Database Archive. (n.d.). Exploit-Db.Com. recuperado septiembre 3, 2021, de https://www.exploit-db.com/about-exploit-db

Perez, J. H. J. (s. f.). CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM. Edu.co. Recuperado 23 de septiembre de 2021, de https://repository.unad.edu.co/bitstream/handle/10596/40242/jhjimenezp.pdf?sequence=1&isAllowed=y

Rayome, A. D. (2021, abril 5). Still using Windows 7? These security tips will protect your laptop now that support is dead. CNET. https://www.cnet.com/tech/services-and-software/still-using-windows-7-these-security-tips-will-protect-your-laptop-now-that-support-is-dead/

Rejetto HFS Http File Server denial of service CVE-2020-13432 Vulnerability Report. (s. f.). Ibmcloud.com. Recuperado 23 de septiembre de 2021, de https://exchange.xforce.ibmcloud.com/vulnerabilities/183065

Snort - network intrusion detection & prevention system. (s. f.). Snort.org. Recuperado 5 de octubre de 2021, de https://www.snort.org/

Thapa, A. (2016, enero 4). Rejetto HTTP File Server (HFS) 2.3.X - Remote Command Execution (2). Exploit-db.com. https://www.exploit-db.com/exploits/39161

Top 10 de los CVE Web más críticos de 2020. (Dakota del Norte). Com. Ar. recuperado el 3 de septiembre de 2021 de https://blog.segu-info.com.ar/2021/01/top-10-de-los-cve-web-mas-criticos-de.html

VIII OWASP Spanish Chapter Meeting. (s. f.). Equipo de Respuesta a Incidentes. Owasp.org. Recuperado 3 de octubre de 2021, de https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf

Wikipedia contributors. (2021, abril 24). Blue team (computer security). Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Blue_team_(computer_security)&oldid=1019593399

Wikipedia contributors. (s. f.-a). Gestión de información y eventos de seguridad. Wikipedia, The Free Encyclopedia. Recuperado 3 de octubre de 2021, de https://es.wikipedia.org/w/index.php?title=Gesti%C3%B3n_de_informaci%C3%B3n_y_eventos_de_seguridad&oldid=133566996

Wikipedia contributors. (s. f.-b). RSA Security. Wikipedia, The Free Encyclopedia. Recuperado 4 de octubre de 2021, de https://es.wikipedia.org/w/index.php?title=RSA_Security&oldid=117367730

Wikipedia contributors. (s. f.-c). Sistema de prevención de intrusos. Wikipedia, The Free Encyclopedia. Recuperado 4 de octubre de 2021, de https://es.wikipedia.org/w/index.php?title=Sistema_de_prevenci%C3%B3n_de_intrusos&oldid=124965359

ANEXOS

Enlace de presentación o sustentación del informe final:
https://youtu.be/RQgrPDV8Z_4