CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Ing. ELKIN LEONARDO MARTÍN MARTÍNEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2023

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Ing. ELKIN LEONARDO MARTÍN MARTÍNEZ

M.Sc. JOHN FREDDY QUINTERO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2023

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

Pag

GLOSARIO

BLUE TEAM: Equipo de especialistas en seguridad informática encargado de combatir posibles ataques.

CVE: Acrónimo de "Common Vulnerabilities and Exposures" es una lista de vulnerabilidades identificadas, cada una con un código CVE:CVE-0000-0000

DATO: Conjunto de documentos, archivos y demás información propia de una persona o entidad.

FIREWALL: Llamado cortafuegos, sistema por hardware o software para restringir los accesos a la red informática.

INFRAESCTRUTURA INFORMATICA: Conjunto de red tanto a nivel de software y hardware de una empresa u organización.

INTRUSIÓN: Proceso con el cual se ingresa de forma no autorizada a una red, servidor o sistema informático.

MALWARE: Software de tipo dañino.

PENTESTING: Conocida como “prueba o test de intrusión”, hace referencia a realizar un ataque controlado de tipo cibernético.

PURPLE TEAM: Equipo de especialistas en seguridad informática que realizan las funciones de ataque y defensa, propios de los equipos Red Tema y Blue Team.

RED TEAM: Equipo de especialistas en seguridad informática que realizan pruebas de intrusión.

SEGURIDAD INFORMÁTICA: Procesos relacionados para dar seguridad en el área de sistemas a cualquier organización o individuo.

SERVIDOR: Computador o conjunto de computadores en los cuales se almacena información, la cual puede ser accedida desde otros computadores o dispositivos conectados a la red.

VIRTUAL BOX: Aplicación de uso gratuito para la implementación de máquinas (computadores) de forma virtualizada.

RESUMEN

En Colombia se destacan dos leyes sobre delitos informáticos, la ley 1273 de 2009, la cual se denomina “de la protección de la información y de los datos” y la ley 1581 de 2012 sobre “Protección de datos personales” ambos como su nombre lo indican, buscan proteger los datos y sancionar los accesos no autorizados a los mismos.

Los especialistas en seguridad informática deben tener en cuenta las anteriores leyes a la hora de realizar pruebas de instrucción a una infraestructura informática, o cuando se realizan los contratos con las respectivas empresas u organizaciones para para no infringir la ley, ya que es un tema bastante delicado.

Una de las mejores formas para poner a prueba la seguridad de una infraestructura informática es realizar pruebas simulando un ataque real y a la vez realizar la contención del mismo ataque, al equipo de profesionales que realiza el ataque se le denomina “Red Team” y al equipo de profesionales que realizan la parte defensiva de la organización se le llama “Blue Team”, al final la idea es buscar todas las vulnerabilidades de la infraestructura para corregirlas y así fortalecer la seguridad ante un posible ataque real.

Cada uno de los dos equipos, utiliza herramientas, aplicativos y técnicas para realizar los procesos de ataque y defensa, en el caso de los equipos Blue Team pueden implementar normas y conjuntos de buenas prácticas como lo es el “CIS” (Center For Internet Security) que en su última versión sugiere 18 controles, los cuales complementados con sistemas como los SIEM (Security Information and Event Management) que son soluciones que integran procesos de identificación y análisis de vulnerabilidades, ayudan a fortalecer la seguridad en una infraestructura informática.

ABSTRACT

In Colombia, two laws on computer crimes stand out, Law 1273 of 2009, which is called "information and data protection" and Law 1581 of 2012 on "Personal data protection" both as their name suggests. they indicate, they seek to protect the data and penalize unauthorized access to them.

Computer security specialists must take into account the previous laws when carrying out instructional tests on a computer infrastructure, or when contracts are made with the respective companies or organizations so as not to infringe the law, since it is quite a subject. delicate.

One of the best ways to test the security of a computer infrastructure is to carry out tests simulating a real attack and at the same time carry out the containment of the attack itself. The team of professionals that carry out the attack is called "Red Team" and the team of professionals who carry out the defensive part of the organization is called "Blue Team", in the end the idea is to look for all the vulnerabilities in the infrastructure to correct them and thus strengthen security against a possible real attack.

Each of the two teams uses tools, applications and techniques to carry out the attack and defense processes, in the case of the Blue Team teams they can implement standards and sets of good practices such as the "CIS" (Center For Internet Security) which in its latest version suggests 18 controls, which, complemented with systems such as SIEM (Security Information and Event Management), which are solutions that integrate vulnerability identification and analysis processes, help to strengthen security in a computer infrastructure.

INTRODUCCIÓN

En la actualidad con el auge de las nuevas tecnológicas en información y comunicación, la información es cada vez más accesible desde cualquier lugar, pero a la vez genera un problema cada vez más crítico, la protección de los datos, bien sea a nivel personal o empresarial.

Para las empresas u organizaciones uno de los mayores activos a proteger son los datos, los cuales pueden ser modificados, robados, secuestrados entre otros muchos incidentes, que dependiendo del dato involucrado puede ser perjudicial para la empresa u organización, por tal motivo se debe contar con un sistema de seguridad que permita garantizar la confidencialidad, la integridad y la disponibilidad de los datos, a estos tres parámetros se les conoce como los pilares de la seguridad informática.

Los ciberdelincuentes están en una constante búsqueda de nuevas formas de cometer sus actos ciber criminales, buscando nuevas técnicas y vulnerabilidades, y por esto los expertos en seguridad informática deben estar un paso adelante para enfrentar los nuevos ataques.

Existen muchas soluciones por hardware y software para ayudar a la seguridad de un sistema informático, como firewall, antivirus, sistemas IDS/IPS, soluciones CIS además de diversas normativas, todas con el propósito de ayudar a la seguridad informática, pero cuando la empresa u organización recibe un ataque real, es cuando se comprueba que tan efectiva era la seguridad implementada, el problema es que, si falla algún punto de la seguridad, los datos podrían resultar comprometidos.

En este orden de ideas una de las mejores formas para poner a prueba los diversos sistemas de seguridad de la organización, como si se estuviera bajo un ataque real de un ciber delincuente es realizar una prueba de intrusión o pentesting, la cual puede dejar en evidencia las posibles vulnerabilidades de la infraestructura informática, para corregirlas antes de que sean aprovechadas por un ciber criminal.

Entonces si un grupo de expertos en seguridad informática van a realizar un ataque a una infraestructura, lo ideal es que hubiera otro grupo de expertos preparados para combatir dicho ataque, a esto se le denomina “Red Team” y “Blue Team”, o Equipo Rojo y Equipo Azul, dos grupos que en el siguiente trabajo se quieren analizar, normativas legales, técnicas y herramientas usadas.

1 JUSTIFICACIÓN

Como se ha mencionado, en la actualidad uno de los principales activos a proteger son los datos, permitiendo que estos cumplan con los tres parámetros de seguridad informática, que son la confidencialidad, la integridad y la disponibilidad, para esto es de vital importancia implementar técnicas que puedan poner a prueba los sistemas se seguridad de una infraestructura informática.

En el siguiente trabajo se quiere analizar además de la parte legal relacionada a la protección de los datos, las técnicas y herramientas que los equipos Red Team y Blue Team pueden implementar para sus respectivas labores, todo esto realizado bajo un banco de trabajo instalado con la aplicación Virtual Box, para poder tener un escenario contralado y seguro para las diversas pruebas de ataque y defensa.

Además de esto analizar normativas como la “CIS” (Center For Internet Security) y sistemas integrados como los SIEM (Security Information and Event Management) para ayudar a los equipos Blue Team a implementar mejoras en la seguridad de una infraestructura informática.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Conocer que son los equipos Red Team y Blue Team, analizando sus técnicas, herramientas y procesos que pueden aplicar cada uno, además de las consideraciones legales y éticas que se deben tener en cuenta para realizar sus procesos.

2.2 OBJETIVOS ESPECÍFICOS

- Aprender la normativa legal colombiana referente a la protección de datos y como se deben tener en cuenta para realizar procesos de pentesting para pruebas de infraestructuras informáticas.

- Analizar las funciones de un equipo Red Team, conociendo las diversas técnicas y herramientas que puede usar para realizar sus funciones.

- Investigar acerca del equipo Blue Team, sus funciones, herramientas y normativas que ayudan al equipo a llevar a cabo sus respectivas tareas.

DESARROLLO DEL TRABAJO

3 LEYES Y DECRETOS SOBRE DELITOS INFORMÁTICOS EN COLOMBIA

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

Se pueden destacar dos leyes:

- Ley 1273 de 2009
- Ley 1581 de 2012 Protección de Datos Personales

A continuación, un resumen las principales características de estas leyes:

3.1 LEY 1273 DE 2009

Es una ley del código penal, denominada “de la protección de la información y de los datos”, consta dos capítulos.

Capítulo 1 - De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Este capítulo costa de 8 artículos, nombrados del 269A, hasta el 269H

Tabla 1, ley 1273 de 2009

Número de articulo	Título del articulo	Descripción	Pena de prisión en meses	Multa en salarios mínimos legales vigentes
269A	Acceso abusivo a un sistema informático	Acceder a datos sin autorización del propietario.	48 -96	100 a 1.000
269B	Obstaculización ilegítima de sistema informático o red de telecomunicación	Impedir u obstaculizar el acceso normal a redes o sistemas informáticos.	48 -96	100 a 1.000

269C	Interceptación de datos informáticos	Interceptar datos de sistemas informáticos de forma ilegal	36 – 72	-
269D	Daño Informático	Dañar, modificar, borrar o alterar datos, sin permiso del propietario	48 -96	100 a 1.000
269E	Uso de software malicioso	Producir, traficar, adquirir, distribuir software dañino sin autorización.	48 -96	100 a 1.000
269F	Violación de datos personales	Obtener, compilar, sustraer, ofrecer, vender o intercambiar datos personales, para provecho propio o de un tercero, sin autorización	48 -96	100 a 1.000
269G	Suplantación de sitios web para capturar datos personales	Desarrollar, traficar o vender programas o páginas con propósitos ilícitos.	48 -96	100 a 1.000
269H	Circunstancias de agravación punitiva	Las penas de los artículos anteriores, se puede incrementar en la mitad o tres cuartas partes en los siguientes casos: 1. Redes estatales, oficiales o sector financiero. 2. Servidores públicos que comentan estos delitos. 3. Abuso de confianza. 4. Revelar datos para perjuicio de otro. 5. Obtener provecho para sí y para otro. 6. Con fines terroristas o que		

	afecten la seguridad nacional. 7. Como instrumento para un tercero. 8. Si la persona que comente el delito, es administrador del sistema afectado, además se puede inhabilitar por tres años de su función

Fuente: SECRETARIASENADO. LEY 1273 DE 2009. [Sitio WEB].[08, febrero, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Capítulo 2 - De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes: hace referencia a manipular sistemas o suplantar usuarios, evadiendo sistemas de seguridad, incurrirá en las penas señaladas en el artículo 240.

Artículo 269J: Transferencia no consentida de activos: manipular información con ánimo de lucro, puede tener prisión de 48 a 120 meses y multas desde 200 a 1.500 salarios mínimos legales vigentes. [1]

Penas incurridas por los Black Hackers

Se identifican dos delitos:

- **Ataque a portal web**, se puede penalizar bajo el artículo 269B “obstaculización ilegítima de sistema informático o red de telecomunicación”, debido que el portal web sufrió múltiples peticiones, técnica utilizada para dejar fuera de servicio el servidor y por tanto el sitio web, con lo cual se está obstaculizando la red de información de la organización.

- **Ataque a computadoras de trabajo**, se puede penalizar bajo el artículo 269A “Acceso abusivo a un sistema informático”, debido a que en las computadas de detecto comportamientos anómalos, cual indica que estos sistemas fueron hackeados

[1] SECRETARIASENADO. LEY 1273 DE 2009. [Sitio WEB].[08, febrero, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

3.2 LEY 1581 DE 2012 PROTECCIÓN DE DATOS PERSONALES

Generalidades

Esta ley protege toda la información que cada persona suministra para ser almacenada en cualquier base de datos o archivos, y como debe tratarse dicha información.[2]

Consta de 9 títulos y cada uno de estos con sus respectivos artículos:

- Título I: objeto, ámbito de aplicación y definiciones
- Título II: principios rectores
- Título III: categorías especiales de datos
- Título IV: derechos y condiciones de legalidad para el tratamiento de datos
- Título V: procedimientos
- Título Vi: deberes de los responsables del tratamiento y encargados del tratamiento
- Título VII: de los mecanismos de vigilancia y sanción
- Título VIII: transferencia de datos a terceros países

Definición de dato personal

Es cualquier tipo de información que pertenece a una persona natural y puede ser de tipo público, semiprivado, privado y sensible[3].

- Dato personal público: es información que no necesita permiso del usuario para ser tratada.
- Dato personal semiprivado: son datos que no son de tipo íntimo del usuario, pero se necesita permiso de este para su tratamiento.
- Dato personal privado: son datos íntimos que necesita autorización del usuario para su tratamiento.
- Dato personal sensible: son datos que obligatoriamente necesita permiso del usuario para su tratamiento.

[2] FUNCIONPUBLICA. LEY ESTATUTARIA 1581 DE 2012. [Sitio WEB].[09, febrero, 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[3] IMSALUD. ABC Ley 1581 de 2012 Protección de Datos Personales. [Sitio WEB].[09, febrero, 2023]. Disponible en: https://www.imsalud.gov.co/web/sin-categoria/abc-ley-1581-de-2012-proteccion-de-datos-personales/

4 PASOS PARA REALIZAR UNA PRUEBA DE INTRUSIÓN

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Para ejecutar los procesos pentesting existen diversas metodologías como las siguientes:

- owasp: Open Web Application Security Project
- osstmm: Open Source Security Testing Methodology Manual
- nist: National Institute of Standards and Technology
- issaf: de OISSG (Open Information System Security Group
- OTP (OWASP Testitng Project)
- PTES: penetration testing execution standard
- WASC-TC: Web Application Security Consortium

Cada una de estas metodologías define los pasos a seguir en el proceso de la prueba de pentesting, pero en general todas compartes muchos pasos o fases, a continuación, se presenta de forma general los pasos principales, teniendo en cuenta que cada metodología puede agregar o llamar de forma diferente cada uno de estos[4]:

Paso 1. Interacciones previas

Negociación entre el cliente y el equipo de pentesting, donde se acuerda el alcance de la prueba.

Paso 2. Recolección de información

Se analiza la infraestructura a realizar la prueba, como tipo de servidores, equipos, sistemas operativos, antivirus, firewall, escaneo de puertos, dominios entre otros.

[4] CIBERSEGURIDADBIDAIDEA. ¿Cuál son la 5 Fases del Pentesting?. [Sitio WEB].[10, febrero, 2023]. Disponible en: https://ciberseguridadbidaidea.com/fases-del-pentesting/

Paso 3. Análisis de vulnerabilidades

Con la utilización de herramientas específicas como Kali Linux y sus diversas suites como Nessus, Metasploit, Nmap entre otros, se procede a realizar un análisis de las vulnerabilidades de la infraestructura en análisis.

Paso 4. Explotación de vulnerabilidades

Se procede a realizar el ataque teniendo en cuenta las vulnerabilidades encontradas en el paso anterior.

Paso 5. Informe

Se genera un informe detallado del proceso de pentesting, enumerando vulnerabilidades, ataques realizados y sugerencias para resolver todas las fallas de seguridad encontradas en la infraestructura en análisis.

1. Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

Herramientas:

- Metasploit: utiliza una base de datos para su funcionamiento, y se una vez encontrada la vulnerabilidad en el sistema, Metasploit permite conocer el daño que se podría ocasionar al aprovechar la vulnerabilidad descubierta.[5]

- Nmap: Esta herramienta permite realizar el proceso de escaneo de puertos, para analizar que puertos se encuentran abiertos y conocer que vulnerabilidades representan para la seguridad del sistema.[6]

- OpenVas: Este programa puede escanear vulnerabilidades, puertos abiertos, fallos en la configuración y similares con solo indicarle la IP que se desea atacar[7]

---

[5] VIEWNEXT. Las 8 herramientas imprescindibles de pentesting [Sitio WEB].[11, febrero, 2023]. Disponible en: https://www.viewnext.com/8-herramientas-imprescindibles-pentesting/

[6] VIEWNEXT. Las 8 herramientas imprescindibles de pentesting [Sitio WEB].[Sitio WEB].[11, febrero, 2023]. Disponible en: https://www.viewnext.com/8-herramientas-imprescindibles-pentesting/

[7] OPENWEBINARS. Para qué sirve OpenVAS. Sitio WEB].[11, febrero, 2023 https://openwebinars.net/blog/que-es-openvas/

Servicios en línea:

- ExploitDB: es una aplicación de tipo web desarrollado por la compañía Offensive Security, creado si ánimo de lucro, con la finalidad es reunir bases de datos públicas con exploit para vulnerabilidades que pueden ser utilizados de forma gratuita por el personal que trabaja en seguridad informática.[8]
- CVE: es el acrónimo de “Common Vulnerabilities and Exposures”, en español seria “Vulnerabilidades y exposiciones comunes”, como su nombre lo indica se trata de un listado de vulnerabilidades y exposiciones de seguridad las cuales pueden ser consultadas para realizar pruebas de pentesting y fortalecer las infraestructuras informáticas. [9]

5 CONFIGURACIÓN BANCO DE TRABAJO

Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1

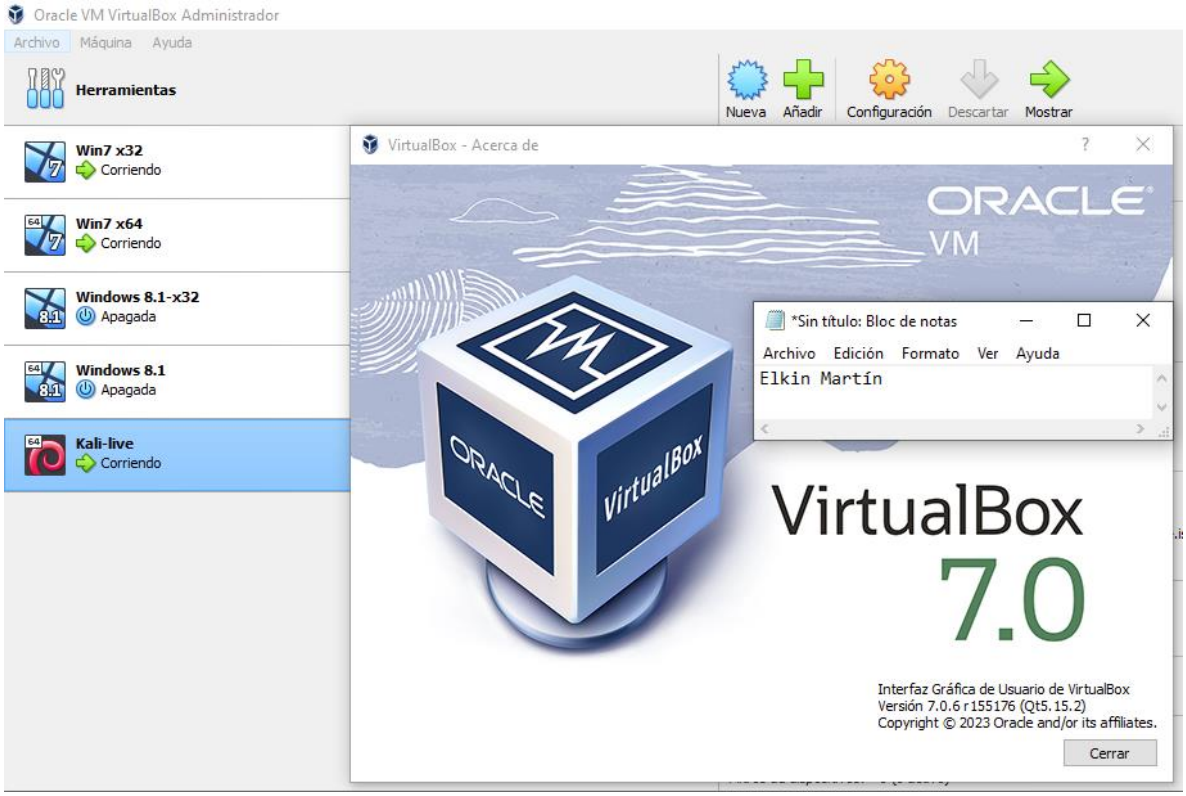
– Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1
– escenario 1 es lo siguiente:

- Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

La figura 1 evidencia la versión de Virtual Box utilizado para realizar el banco de trabajo.

[8] KEEPCODING. ¿Qué es ExploitDB?. [Sitio WEB].[12, febrero, 2023]. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/#Que_es_ExploitDB
[9] CIBERSEGURIDAD. ¿Qué es CVE?. [Sitio WEB].[12, febrero, 2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

Figura 1. Virtual box 7.0.

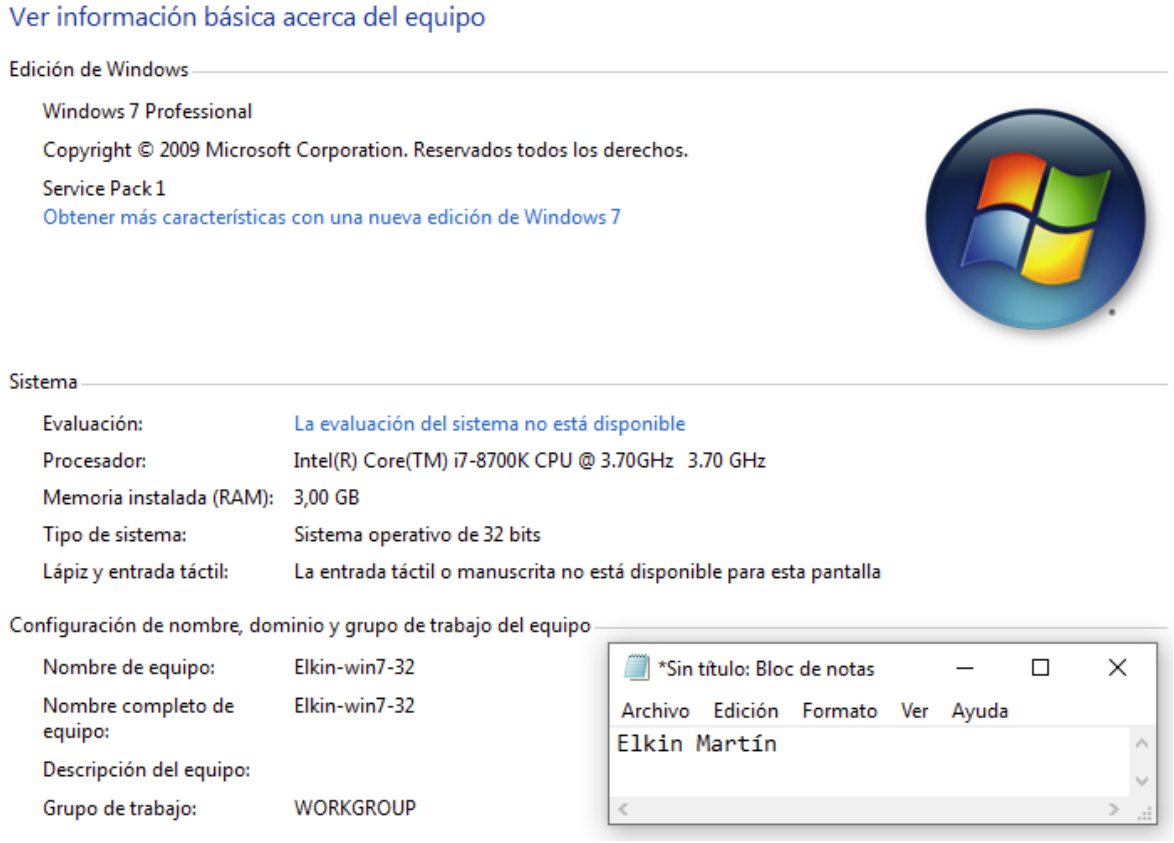


Fuente: autoría propia

- Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

En la figura 2, se evidencia la configuración de la maquina Windows 7 x32

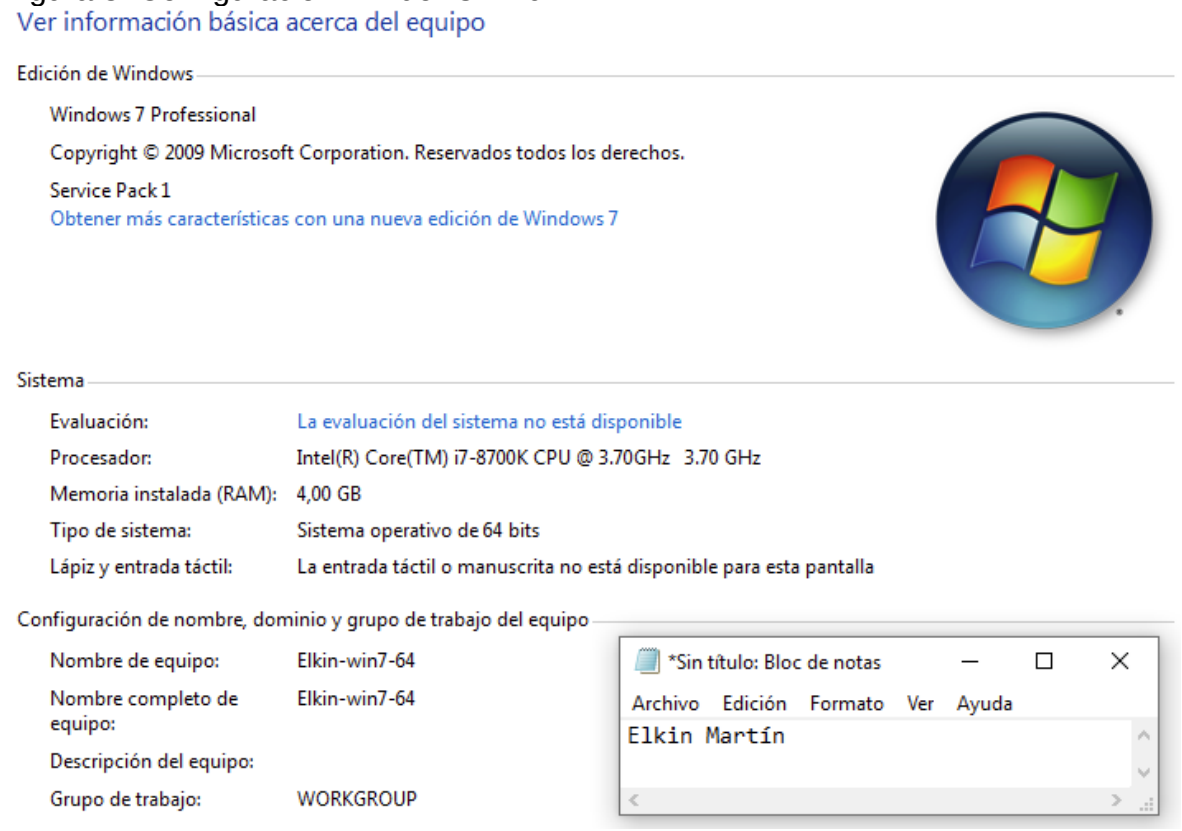
Figura 2. Configuración Windows 7 x32.



Fuente: autoría propia

En la figura 3, se evidencia la configuración de la maquina Windows 7 x64

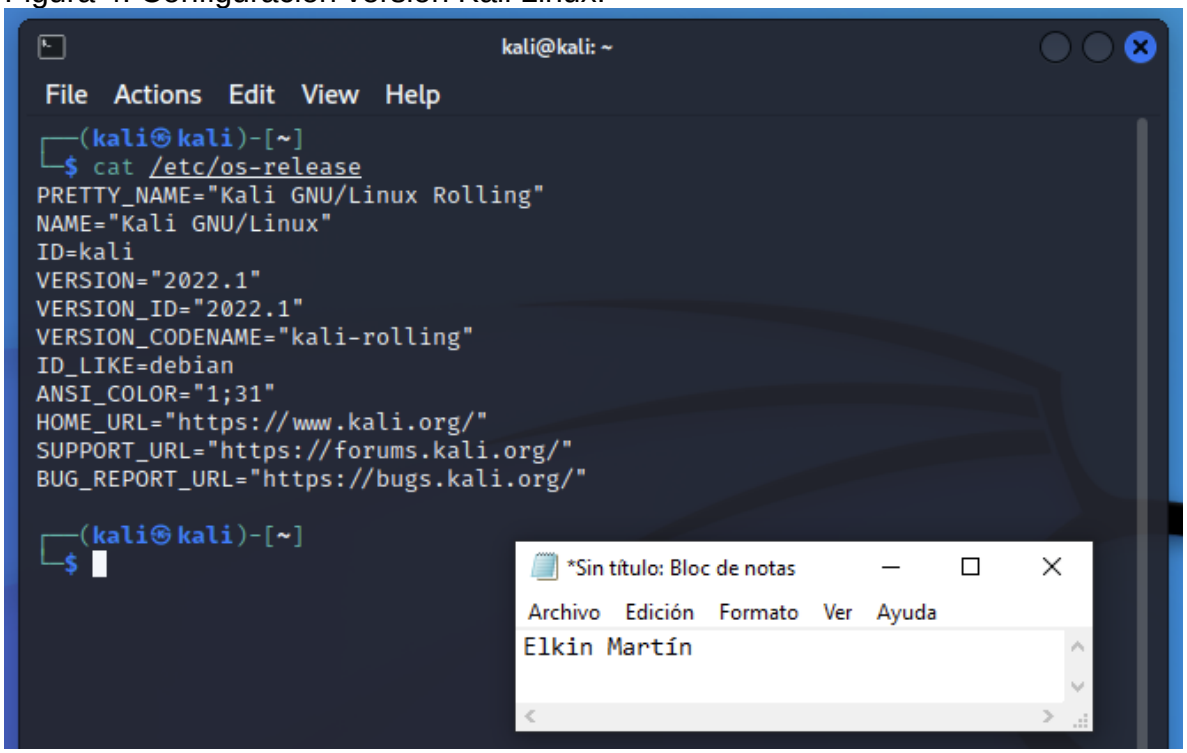
Figura 3. Configuración Windows 7 x64.



Fuente: autoría propia

En la figura 4, se evidencia la versión de la maquina Kali Linux utilizada para el banco de trabajo.

Figura 4. Configuración versión Kali Linux.

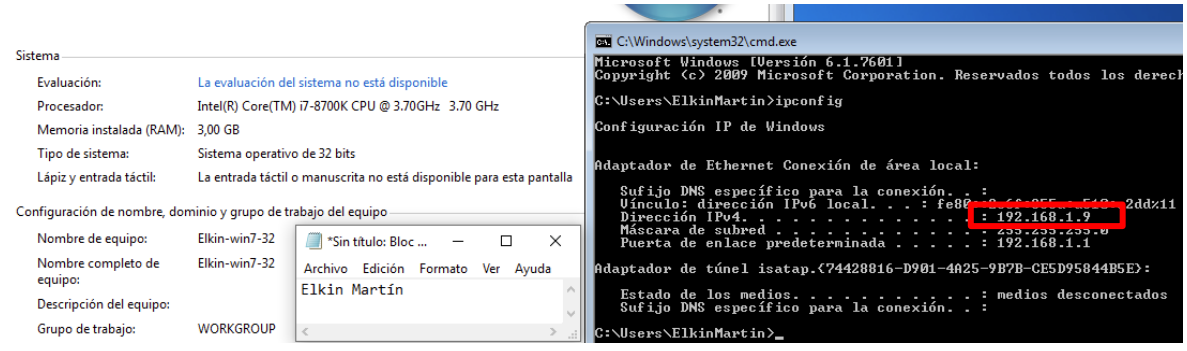


Fuente: autoría propia

- Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

La figura 5 evidencia la dirección IP de la maquina Windows 7 x32

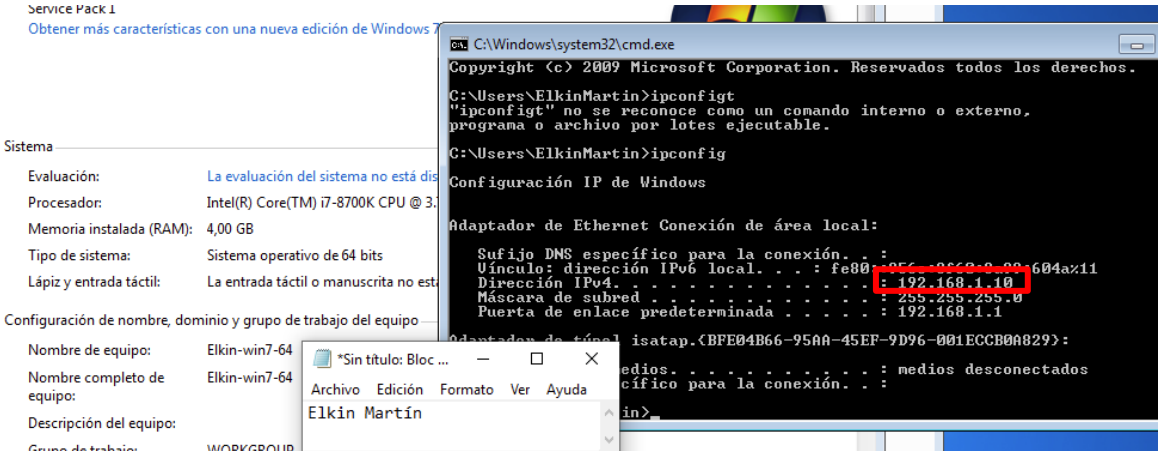
Figura 5. IP Windows 7 x32.



Fuente: autoría propia

La figura 6 evidencia la dirección IP de la maquina Windows 7 x64

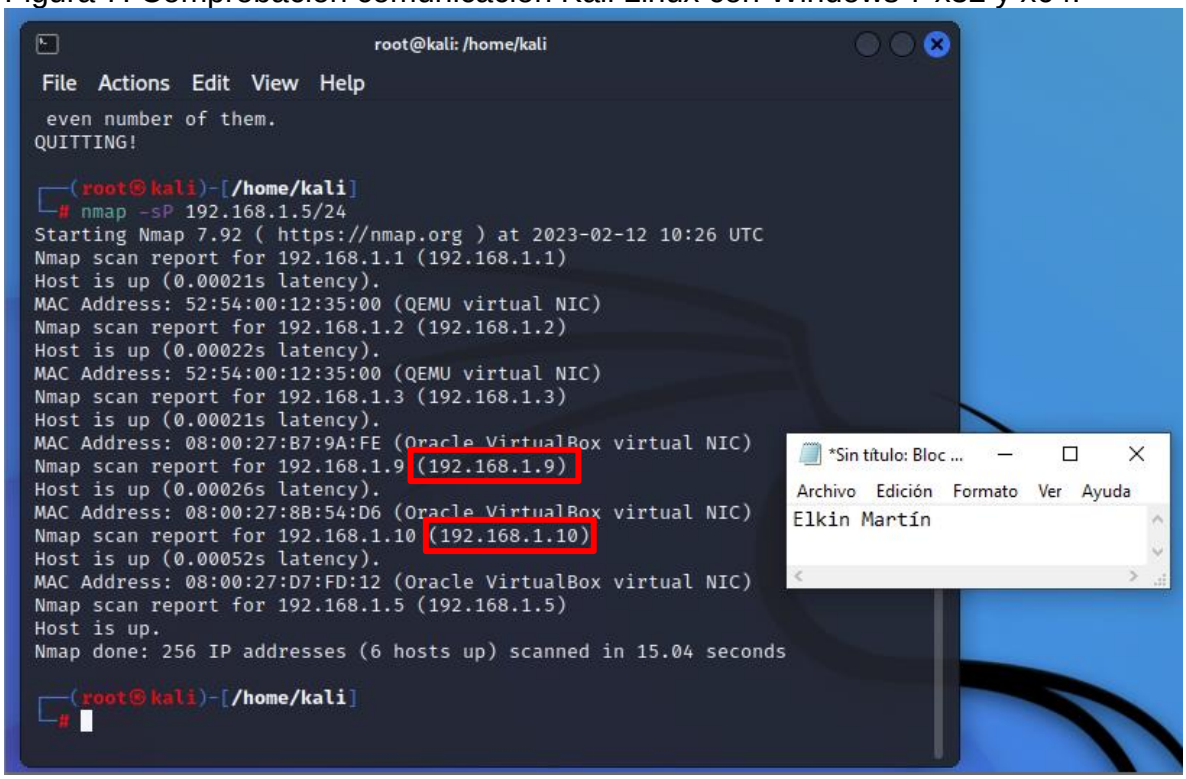
Figura 6. IP Windows 7 x64.



Fuente: autoría propia

En la figura 7 se está comprobando la comunicación entre la maquina Kali Linux y las dos máquinas Windows 7 x32 y x64

Figura 7. Comprobación comunicación Kali Linux con Windows 7 x32 y x64.



Fuente: autoría propia

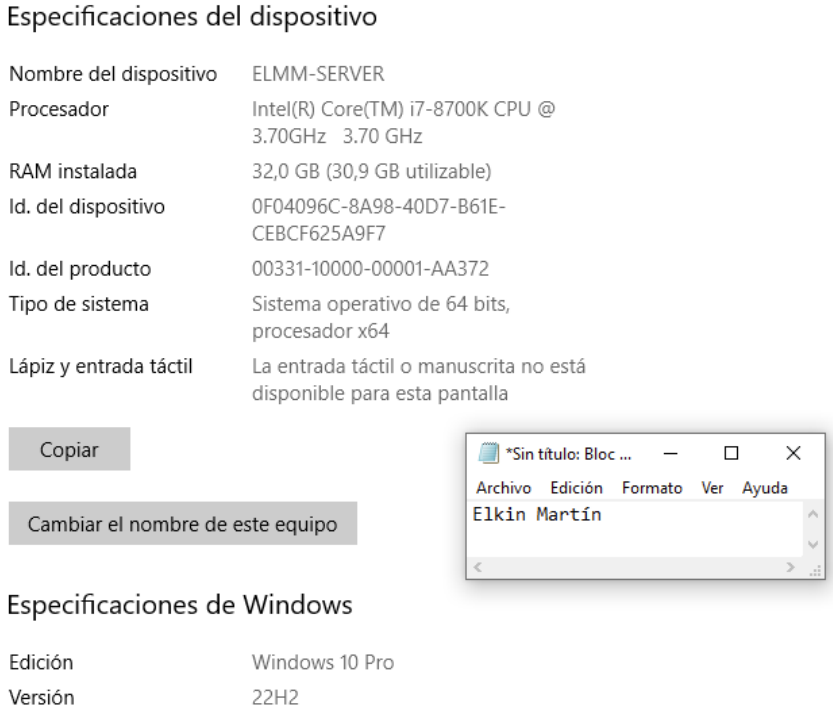
- Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

En la figura 8 se evidencia la configuración de la maquina host donde se va a montar el banco de trabajo con la aplicación Virtual Box.

Equipo host

Procesador: Intel i7 8700k
RAM: 32 gigas
Sistema operativo: Windows 10 22H2

Figura 8. Equipo host



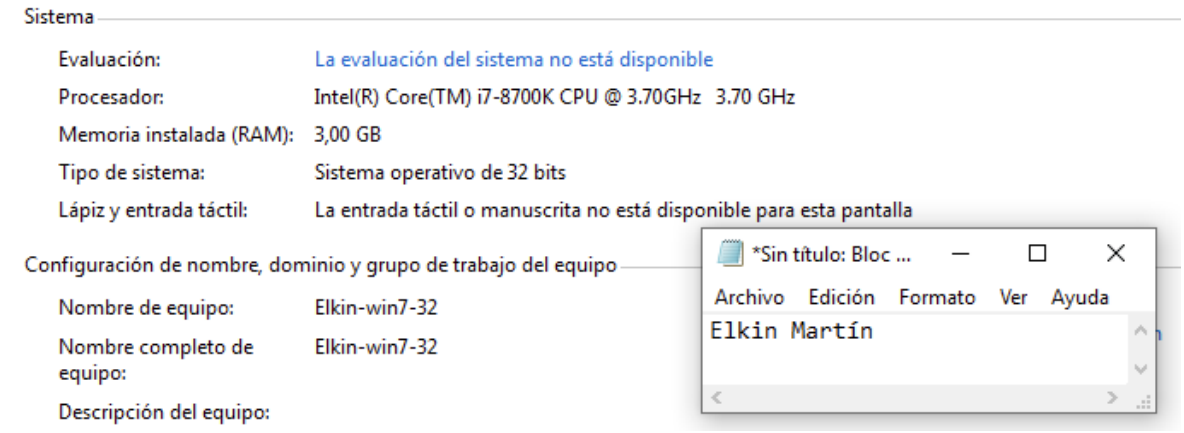
Fuente: autoría propia

Maquina 1. Windows 7 x32

Procesador: 4 núcleos
RAM: 3 gigas
Sistema operativo: Windows 7 x32

La figura 9 evidencia la configuración de la maquina Windows 7 x32 del banco de trabajo.

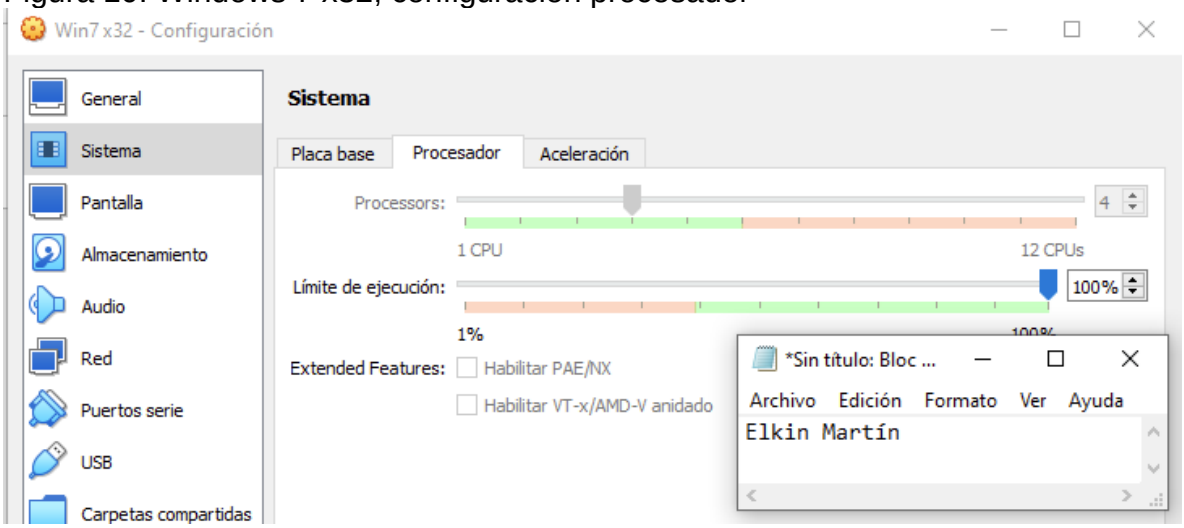
Figura 9. Maquina 1



Fuente: autoría propia

La figura 10 evidencia la configuración en Virtual Box de procesador de la maquina Windows 7 x32 con cuatro núcleos asignados.

Figura 10. Windows 7 x32, configuración procesador



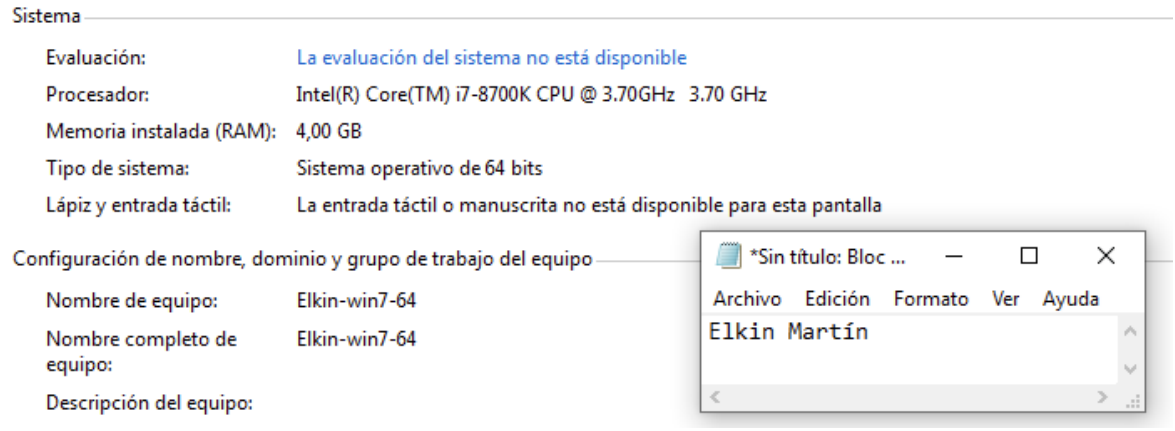
Fuente: autoría propia

Maquina 2. Windows 7 x32

Procesador: 4 núcleos
RAM: 4 gigas
Sistema operativo: Windows 7 x32

La figura 11 evidencia la configuración de la maquina Windows 7 x64 del banco de trabajo.

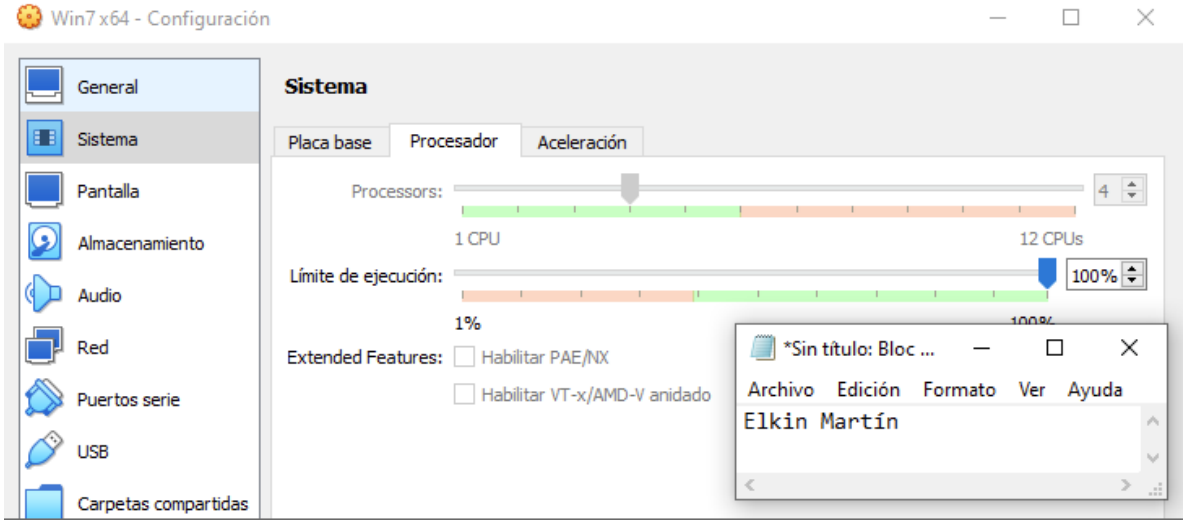
Figura 11. Maquina 2



Fuente: autoría propia

La figura 12 evidencia la configuración en Virtual Box de procesador de la maquina Windows 7 x64 con cuatro núcleos asignados.

Figura 12. Windows 7 x64, configuración procesador



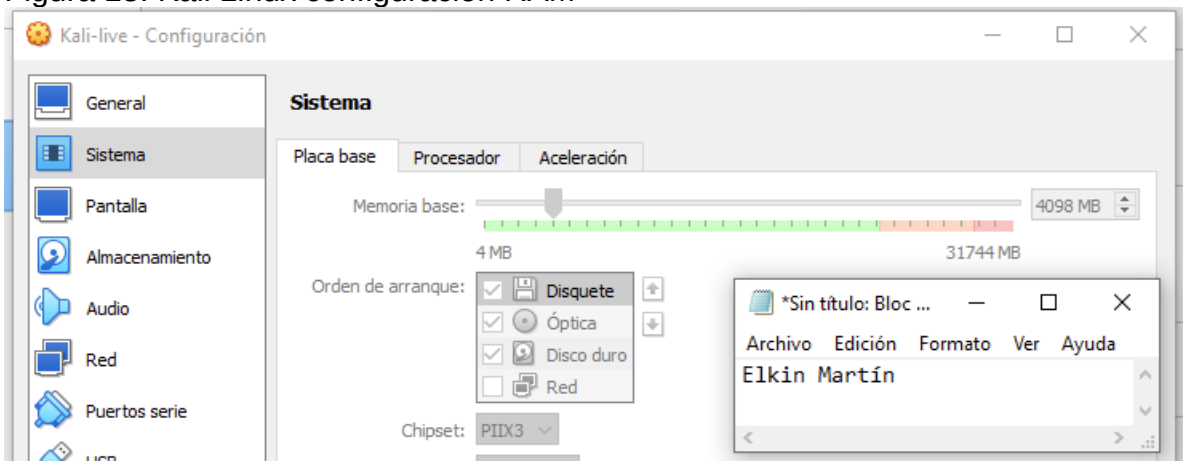
Fuente: autoría propia

Maquina 3. Kali Linux

Procesador: 4 núcleos
RAM: 4 gigas
Sistema operativo: Kali Linux

La figura 13 muestra la cantidad de memoria RAM asignada para la maquina Kali Linux.

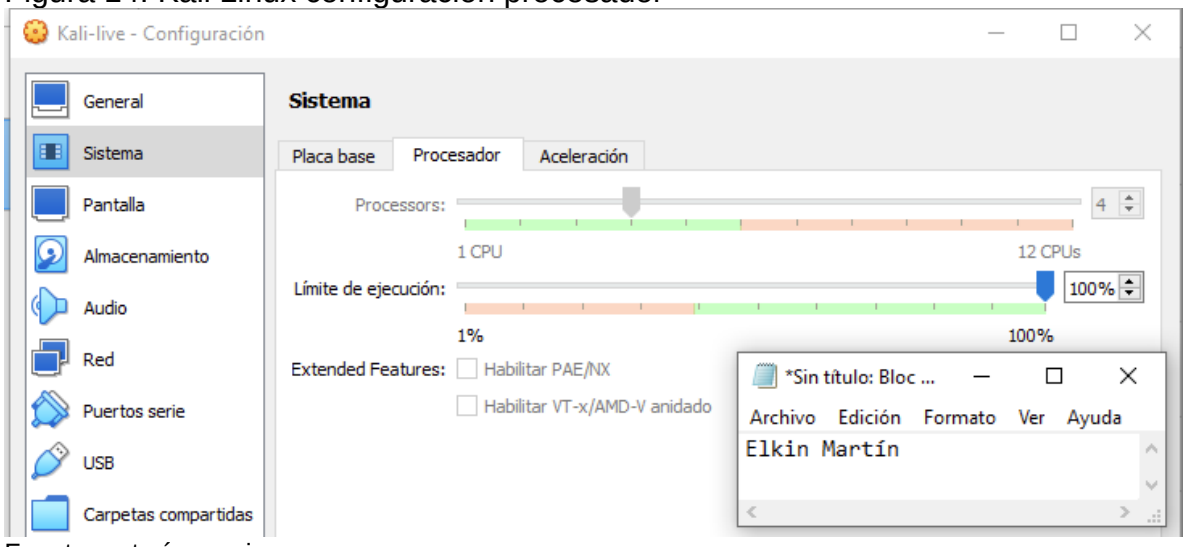
Figura 13. Kali Linux configuración RAM



Fuente: autoría propia

La figura 14 muestra la configuración de procesadores asignados para la maquina Kali Linux.

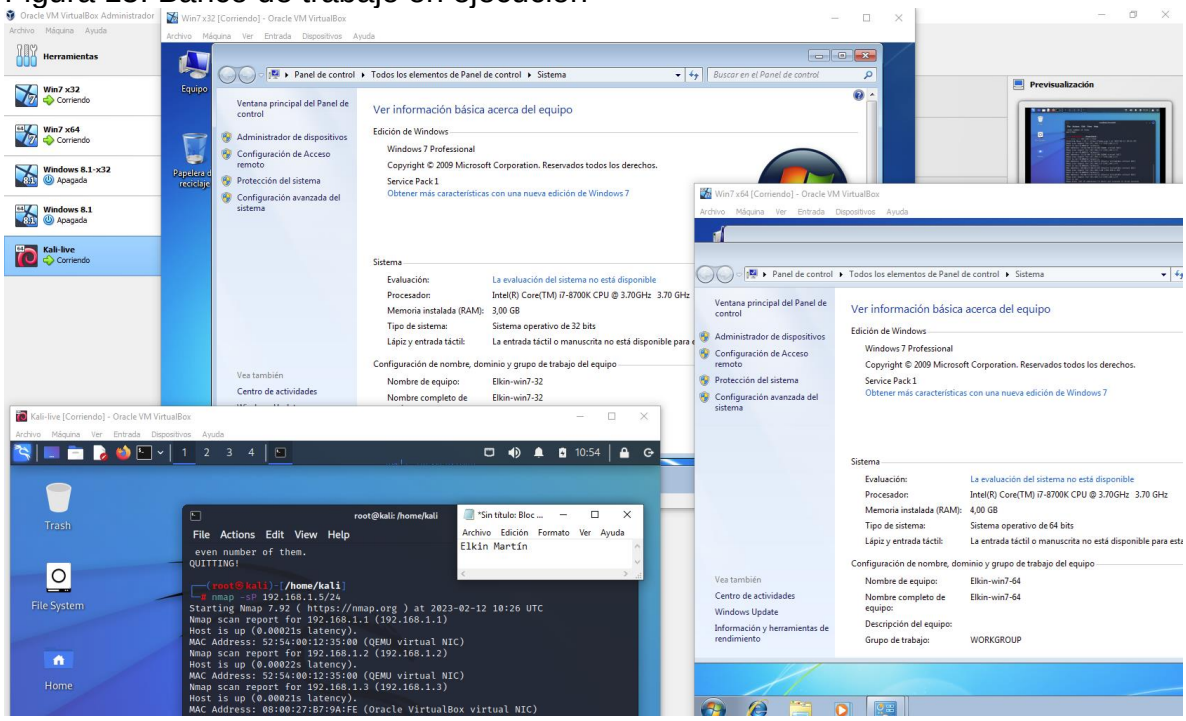
Figura 14. Kali Linux configuración procesador



Fuente: autoría propia

La figura 15 evidencia las tres máquinas del banco de trabajo en ejecución, Windows 7 x32, Windows x64 y Kali Linux.

Figura 15. Banco de trabajo en ejecución



Fuente: autoría propia

6 ANÁLISIS PRACTICO DE UN ACUERDO DE CONFIDENCIALIDAD

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Al leer con detenimiento el acuerdo de confidencialidad entre la parte receptora (estudiante – Elkin Martín) y parte receptora (la empresa – The WhiteHouse Security), se evidencia varias irregularidades, a continuación, se exponen los fragmentos de dichas irregularidades con su respectiva explicación.

- **Primera. Objetivo.** “la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados”

Cualquier acuerdo de confidencialidad debe establecer la no divulgación de la información o datos de la empresa, pero en este articulo habla de que la empresa Whitehouse Security realiza procesos ilegales, los cuales un profesional con ética no debería aceptar ni participar de tales procesos.

- **Segunda. Numeral 2.** “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”

En este artículo se da por entendido que la empresa Whitehouse Security obtiene datos de forma ilegal, que va en contra de la ética y de las leyes colombianas, como lo es la ley 1273 de 2009, artículo 269A el cual hace referencia a: “Acceso abusivo a un sistema informático”

- **Cuarta. Numeral 3.** “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.”

Según la descripción de la empresa Whitehouse Security, es de carácter privado y se enfoca a la ciberseguridad y la ciberdefensa, pero considero que no está habilitada para realizar actividades de espionaje y sospechas, como lo indica este artículo, por lo cual la empresa estaría infringiendo las leyes contra la protección datos, específicamente el artículo 269A de ley 1273 de 2009.

- **Cuarta. Numeral 4.** "Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca"

Se debe dejar claro que como profesionales se debe respetar la confidencialidad del cliente, empresa u organización a la cual se le está prestando el servicio, pero el artículo también habla de información ilegal, motivo por el cual como buenos profesionales y con ética se debería denunciar.

- **Cuarta. Numeral 7.** “Responder por el mal uso que le den sus representantes a la información confidencial”

Como buenos profesionales se debe tener responsabilidad y lealtad ante la empresa u organización a la cual se le está prestando algún servicio, pero por simple sentido común, y más aun conociendo que la empresa realiza actividades ilegales y sospechosas como ya se ha evidenciado en artículos anteriores, primero no se debería aceptar un trabajo de estos, y segundo, jamás se debería aceptar responder por las acciones que otro realice, en este caso los representantes de la información.

- **Cuarta. Numeral 8.** "Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento."

El articulo considero está mal diseñado, si hay información en nuestra posesión, se sobre entiende la empresa facilito dicha información para nuestro respetivo trabajo, en caso contrario si habría un delito, porque se estaría extrayendo información

confidencial sin autorización de la empresa, pero el articulo simplemente dice que el profesional debe responder por dicha información, sin lugar a explicación.

- **Octava. Solución de controversias.** “En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.”

Este artículo es similar al anterior, si el profesional tiene la información es porque la empresa le facilito dicha información para el respectivo trabajo, por tal motivo es la empresa la que debería responder por el tipo y la fuente de dicha información, en caso de que sea el profesional que tiene la información sin la autorización de la empresa, ahí de abría una falta y seria valido y necesario que el profesional acuda a su defensa con un abogado.

7 ANÁLISIS DE ACUERDO DE CONFIDENCIALIDAD DE ACUERDO A LA LEY 1243

Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 - Acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

En el acuerdo de confidencialidad entre la parte receptora (Elkin Martín) y la empresa The WhiteHouse Security, se evidencia infracciones a la ley 1273 en los siguientes artículos:

- **Segunda. Numeral 2.** “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”

El artículo segundo, numeral 2 infringe de manera clara el artículo 269A *Acceso abusivo a un sistema informático* de la ley 1273 de 2009 el cual dice:

> “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 1.000 salarios mínimos legales mensuales vigentes.[10]”

[10] SECRETARIASENADO. LEY 1273 DE 2009, [Sitio WEB].[18, febrero, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- **Cuarta. Numeral 3.** “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.”

El artículo cuarto, numeral 3 da por entendido que la empresa The WhiteHouse Security está obteniendo datos a través de actividades sospechosas o espionaje, lo cual infringe el articulo 269C *Interceptación de datos informáticos* de la ley 1273 de 2009 el cual dice:

> "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 transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.[11]"

8 TOMA DE DECISIÓN PARA ACEPTAR O NO ACUERDO DE CONFIDENCIALIDAD

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿usted como experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.

Teniendo en cuenta todas las irregularidades e infracciones a la ley 1273 de 2009 presentes en el acuerdo de confidencialidad entre la parte receptora (Elkin Martín) y la empresa The WhiteHouse Security, **no aplicaría** a este trabajo.

Además, varias de las irregularidades presentes en los artículos de confidencialidad de la empresa The WhiteHouse Security, van en contra de lo que dispone el código de ética para ingenieros COPNIA.

A continuación, se presentan los artículos del código de ética COPNIA, con su respectiva explicación, para respaldar la decisión de no aplicar para el trabajo con la empresa The WhiteHouse Security.

[11] SECRETARIASENADO. LEY 1273 DE 2009, [Sitio WEB].[18, febrero, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. Son prohibiciones especiales a los profesionales respecto de la sociedad:
a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación[12];

Teniendo en cuenta este articulo 34, no se debería aceptar un trabajo en el cual la empresa está realizando procesos ilegales e interceptación de información, con el acceso abusivo a sistemas informáticos, como lo deja en evidencia el acuerdo de confidencialidad en los puntos:

- **Primera. Objetivo.** “la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados”

- **Segunda. Numeral 2.** “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”

ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL. Son deberes de los profesionales para con sus clientes y el público en general:
a) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo[13];

Este articulo menciona como se debe mantener de forma confidencial los datos de los clientes, pero también permite exponer dicha información por obligaciones legales, lo cual estaría en conflicto con el contrato de confidencialidad de la empresa Whitehouse Security en los siguientes artículos:

- **Cuarta. Numeral 3.** “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.”

- **Cuarta. Numeral 4.** "Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca"

[12] COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares., [Sitio WEB].[18, febrero, 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf
[13] Ibid., p 14

ARTÍCULO 40. PROHIBICIONES A LOS PROFESIONALES RESPECTO DE SUS CLIENTES Y EL PÚBLICO EN GENERAL. Son prohibiciones a los profesionales respecto de sus clientes y el público en general:
a) Ofrecer la prestación de servicios cuyo objeto, por cualquier razón de orden técnico, jurídico, reglamentario, económico o social, sea de dudoso o imposible cumplimiento, o los que, por circunstancias de idoneidad personal, no pudiere satisfacer[14];

Como profesionales no se debería prestar servicios a clientes, empresas u organizaciones que tengan un "dudoso" proceder, lo cual se evidencia el contrato de confidencialidad de la empresa Whitehouse Security en el siguiente artículo:

- **Cuarta. Numeral 7.** "Responder por el mal uso que le den sus representantes a la información confidencial"

9 OPERACIÓN ANDROMEDA BUGGLY

Deberá buscar la noticia del caso "OPERACIÓN ANDROMEDA BUGGLY" en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.

Primero se debe tener claro lo sucedido, según el portal web enter.co, Buggly era un lugar de encuentro de aficionados y entendidos en el tema del hacking, se compartía conocimientos, se realizaban retos y demás temáticas relacionadas con el área del hacking, este sitio era promovido por Carlos Betancur, 'Bender' entre el 18 de septiembre de 2012 y el 3 de febrero de 2014, además de los encuentros de hacking, el sitio también era utilizado para otras actividades, todas con el propósito de promover el sitio, pero según investigaciones el sitio Buggly era una fachada para realizar tareas de espionaje, hackeo y similares, promovidas por el ejército nacional, además de buscar entre la población civil que frecuentaba el sitio, aquellos que tuvieran grandes habilidades y destreza en el área del hacking para luego ser reclutados[15].

[14] COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares., [Sitio WEB].[18, febrero, 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

[15] ENTER.CO. Detrás de Buggly: la historia de la fachada Andrómeda, [Sitio WEB].[20, febrero, 2023]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

El análisis de las implicaciones legales y éticas sobre este caso, es algo complejo, por un lado se supone que cualquier entidad del gobierno, como el ejército, la policía y otras organizaciones de inteligencia podrían realizar procesos de espionaje e inteligencia en contra de las organizaciones criminales, delincuencia organizada, y demás grupos al margen de la ley, lo que implica todas la utilización de todas las herramientas del hacking, con el propósito de desmantelar estas organizaciones y crear seguridad en la población.

Pero el problema se genera cuando estas organizaciones de inteligencia en vez de realizar lo anterior, realizan procesos de espionaje y hacking en contra de grupos políticos, étnicos y demás población que son perseguidos por al gobierno de turno, y en este caso considero que además de mal utilizar los recursos que tienen, solo por favorecer los intereses de unos pocos, quebrantan muchas leyes y artículos como los mencionados en la ley 1273 de 2009 “de la protección de la información y de los datos”, vulnerando la privacidad de la población.

En el cado de la operación Andrómeda, es muy poco ético tener una fachada para buscar talentos en el área del hacking. Si una organización bien sea privada o gubernamental desea encontrar nuevos talentos humanos debería hacerlo a través de la vías legales y éticas, como abrir algún tipo de convocatoria o concurso, de esta manera quienes se presenten saben exactamente para que están siendo convocados.

Este tipo de conductas además de ser poco ético e ilegal, solo crea una mala imagen de las entidades gubernamentales, en este caso el ejército, por decisión de unos pocos involucrados, toda la entidad sufre de esa imagen negativa y pierden credibilidad ante la población.

10 HERRAMIENTAS Y PROCEDIMIENTOS DE ACUERDO A LOS PASOS DE PENTESTING

Teniendo en cuenta los pasos generales para realizar un proceso del pentesting, se procede de la siguiente manera:

10.1 PASO 1. INTERACCIONES PREVIAS

- Cliente: The WhiteHouse Security
- Pentesting: Elkin Leonardo Martín Martínez
- Problema: fuga de información en PC con sistema operativo Windows 7 – x64
- Resultado esperado: identificación de fuga, creación de usuario con privilegios de administrador.

10.2 PASO 2. RECOLECCIÓN DE INFORMACIÓN

- Fugas de información
- Computador con sistema operativo Windows 7 - x64
- Ejecución de aplicación Rejetto v. 2.3
- Posibles exploit asociados a Shell reversa

10.3 PASO 3. ANÁLISIS DE VULNERABILIDADES

Para el análisis de las vulnerabilidades se va a utilizar la aplicación NMAP corriendo desde la suite de Kali Linux (proceso realizado en el numeral 12, página 41 - herramientas utilizadas)

10.4 PASO 4. EXPLOTACIÓN DE VULNERABILIDADES

Con la herramienta Metasploit Framework (msfconsole) se procede a realizar la explotación de la vulnerabilidad encontradas (proceso realizado en el numeral 14, página 44 – explotación de vulnerabilidad)

10.5 PASO 5. INFORME

Se muestra los resultados esperados en las interacciones previas, evidenciado como se pudo realizar el ataque, la fuga de información y la creación del usuario con privilegios de administrador (proceso realizado en el numeral 15, página 61 – evidencia de explotación)

11 ANÁLISIS DE PROBLEMA AL FALLO IDENTIFICADO

En el caso planteado, hay dos puntos que son de gran relevancia para dar solución al problema de la fuga de información

11.1 SISTEMA OPERATIVO

La máquina afectada tiene instalada una versión de Windows 7 – x64, este sistema operativo dejo de recibir actualización de seguridad el 14 de enero de 2020, lo que significa que con el pasar de los días, cada vez va ser más vulnerable a cualquier tipo de ataque.

11.2 REJETTO V. 2.3

Esta aplicación Rejetto HFS es un servidor de archivos, con el cual se puede enviar y recibir todo tipo de archivos[16], al tratarse de un servidor cuando se inicia abre el puerto 80, el problema está en que esta aplicación tiene una vulnerabilidad la cual permite crear una Shell, con lo cual se puede tomar el control del sistema operativo donde esté funcionando.

La aplicación puede que haya sido instalada por el propio departamento de TI de la organización para el proceso de transferencia de archivos, puede que un tercero la haya instalado con ese propósito, o también que haya sido enviada por correo u otro medio, y aplicando algún tipo de ingeniería social el usuario del computador la haya instalado.

12 HERRAMIENTAS UTILIZADAS

Para esta prueba de pentesting se utilizará las siguientes herramientas:

12.1 NMAP

Conocido también como mapeador de redes, es una herramienta muy utilizada por expertos en seguridad informática y pentesting, es de código abierto y permite realizar un análisis de una red encontrando todos los dispositivos que estén conectados a esta, luego con comandos específicos se puede analizar un dispositivo y encontrar información detallada sobre el mismo, y lo más interesante realizar un escaneo de las vulnerabilidades que pueda tener[17].

12.2 METASPLOIT FRAMEWORK

Es una herramienta de código abierto, gratuito, (también existen versiones de pago como el Metasploit Pro) que permite la ejecución de exploits, con el propósito de realizar pruebas de vulnerabilidades a un sistema operativo, dentro de sus principales funciones se puede realizar lo siguiente[18]:

- Escanear y recopilar información de la máquina que se le está haciendo la prueba de pentesting.

---

[16] REJETTO. Description, [Sitio WEB].[07, marzo, 2023]. Disponible en: https://www.rejetto.com/hfs/
[17] NMAP, Guía de referencia de Nmap (Página de manual), [Sitio WEB].[07, marzo, 2023]. Disponible en: https://nmap.org/man/es/index.html
[18] KEEPCODING, ¿Qué es Metasploit?, [Sitio WEB].[07, marzo, 2023]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

- Analizar las vulnerabilidades a nivel se seguridad.
- Escalar privilegios para tener sesiones administradoras.
- Instalar backdoors (puertas traseras) que son códigos maliciosos que permiten sustraer información de la máquina.
- Automatizar procesos (fuzzing) para encontrar fallas de seguridad en el dispositivo.
- Evadir antivirus.
- Eliminar rastros como de huella digital, eliminando logs y registros.

13 INFORME TÉCNICO DE AFECTACIÓN DE UN ATAQUE A UN SISTEMA OPERATIVO

Los ataques a un sistema operativo pueden ser de diversos tipos y con diferentes objetivos, se podrían agrupar de la siguiente manera:

- Daño al sistema: afecta el rendimiento, genera bloqueos y errores en el normal funcionamiento del sistema
- Robo de información: el ciberdelincuente busca robar información como contraseñas de correos, redes sociales, cuentas bancarias, y demás información con la cual pueda obtener algún tipo beneficio.
- Secuestro de información: por lo general el ciberdelincuente busca obtener un beneficio económico a través del rescate de los datos.
- Explotación de vulnerabilidad: el ciberdelincuente se aprovecha de alguna falla o vulnerabilidad de un sistema para ingresar a este y espiar, robar datos y realizar cualquier proceso, ya que tiene control sobre el sistema.

Todos estos ataques se logran con diferentes herramientas, conocidas de forma muy genérica como virus, en la práctica son aplicaciones diseñadas para realizar los ataques mencionados de forma muy general se podrían mencionar los siguientes[19]:

- Malware: aplicación perjudicial para un sistema, en los cuales se encuentras los gusanos y troyanos.
- Virus: Código que afecta a un sistema operativo.
- Gusano: aplicación que una vez infecta un sistema, tiene la capacidad de expandirse sin intervención del usuario.
- Troyanos: permiten abrir puertas para que aplicaciones dañinas ingresen al sistema.

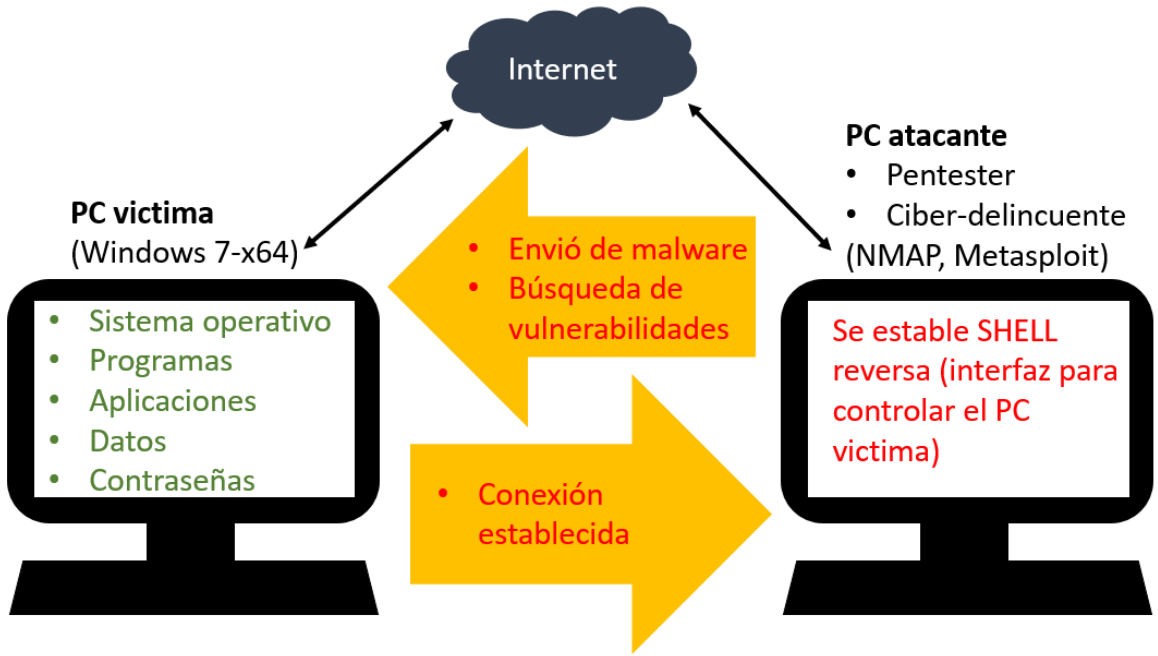
[19] OPTICAL, Ataques informáticos: Causas, Tipos, Consecuencias y Prevenciones, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/

- Spyware: aplicación tipo espía, para robar información del usuario.
- Adware: aplicaciones que muestran publicidad de forma intensiva.
- Ransomware: aplicación que tiene como propósito el secuestro de información.
- Vulnerabilidades: son fallas de un sistema operativo, las cuales son aprovechadas por ciberdelincuentes para ingresar a un sistema, estas fallas por lo general con corregidas con parches de seguridad.

El problema de la fuga de información se debe a vulnerabilidades del sistema operativo Windows 7, que son aprovechadas por los ciberdelincuentes, los cuales con herramientas especificas logran crear una conexión remota hacia la maquina y tomar control de esta, una vez se tenga el control, es como si el ciberdelincuente estuviera de forma presencial en frente de la maquina afectada.

En la figura 16 se representa dos computadores, el (PC victima) para este caso con sistema operativo Windows 7-x64 y el computador que realiza el ataque (PC atacante), que puede ser un profesional en pentesting, o un ciber delincuente, que en ambos casos va a realizar procesos similares, cada uno con sus propias herramientas va a enviar al PC victima malware y búsqueda de vulnerabilidades para poder tomar control de la víctima, una vez se establece la conexión, el atacante puede establecer una SHELL reversa, la cuan es una interfaz con la que se puede controlar el PC victima como si se estuviera operando de forma presencial.

Figura 16. Esquema de ataque a PC victima



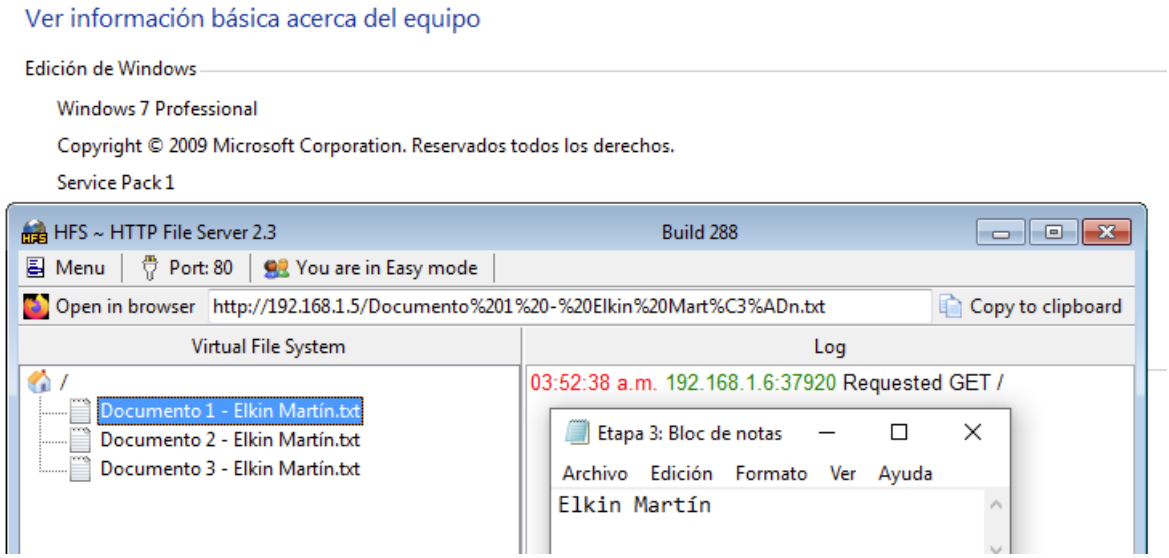
Fuente: autoría propia

14 EXPLOTACIÓN DE VULNERABILIDADES

14.1 PRUEBA DEL SERVIDOR HFS

En la figura 17, se presenta tres archivos de prueba para ser compartidos con la aplicación HFS.

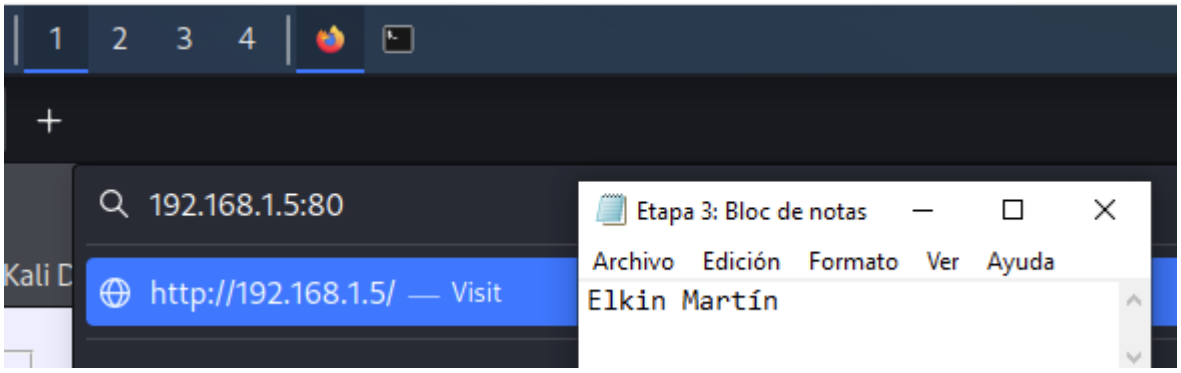
Figura 17. Archivos en servidor HFS



Fuente: autoría propia

La figura 18 muestra una prueba realizada con el navegador Firefox, ingresando la dirección del servidor: 192.168.1.5:80 (80 es el puerto de conexión)

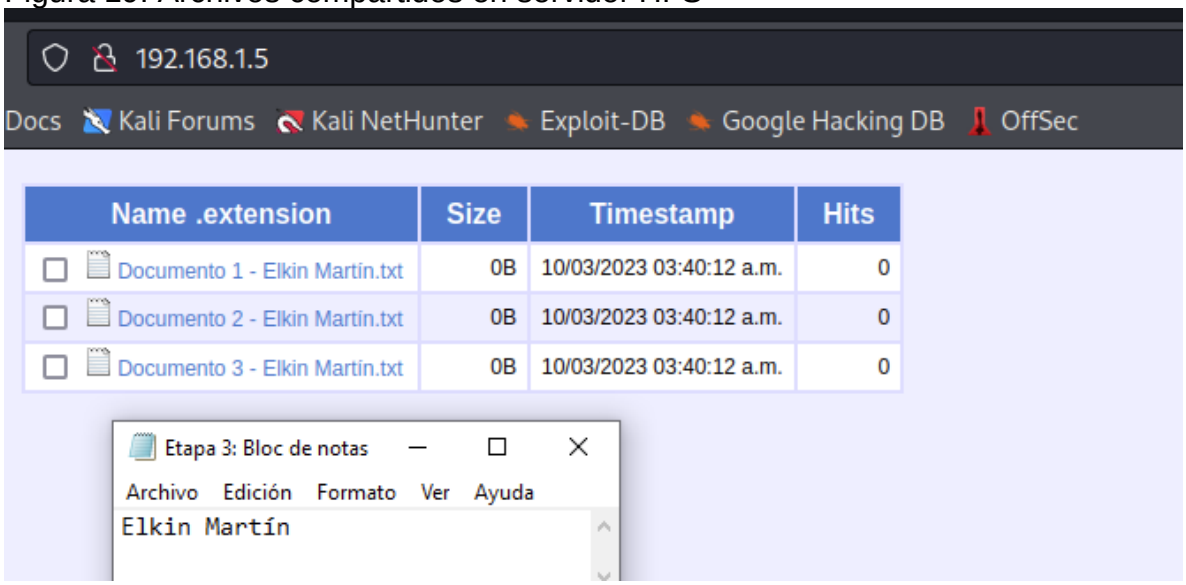
Figura 18. Acceso desde web al servidor HFS



Fuente: autoría propia

La figura 19, muestra el correcto funcionamiento del servidor HFS, mostrando los tres documentos que se han compartido, hasta este punto todo parece estar en orden, un servidor de archivos funcionando sin ningún problema.

Figura 19. Archivos compartidos en servidor HFS



Fuente: autoría propia

14.2 PROCESO DE ANÁLISIS DE VULNERABILIDAD

En este punto se estaría realizando el paso tres (3) de los cinco (5) pasos generales para las pruebas de un pentesting, estamos hablando del “análisis de vulnerabilidades”, para esto se utilizará el programa NMAP ejecutado desde una terminal de Kali Linux con privilegios de administrador “sudo su” (arrancado desde Figura, “Live sistema AMD”)

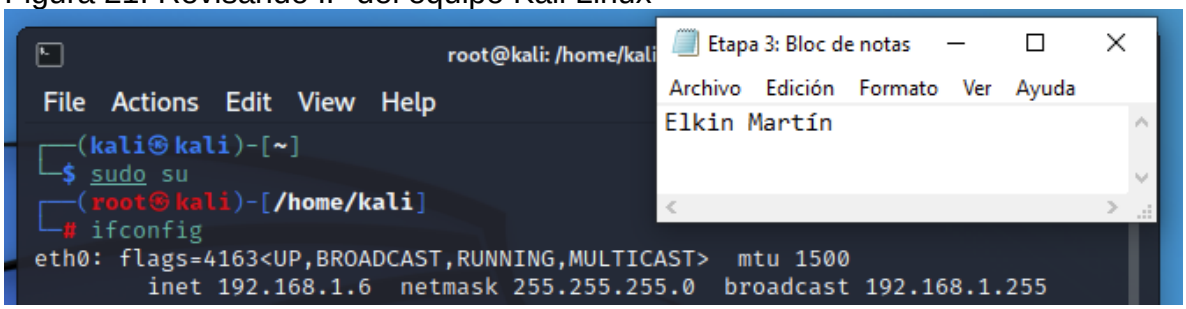
La figura 20 muestra el menú de inicio de Kali Linux, en el cual se selecciona la opción de “Live sistema AMD”

Figura 20. Iniciando Kali Linux

Fuente: autoría propia

En la figura 21 se analiza la IP del equipo Kali Linux para conocer el rango de IP de la red para analizar.

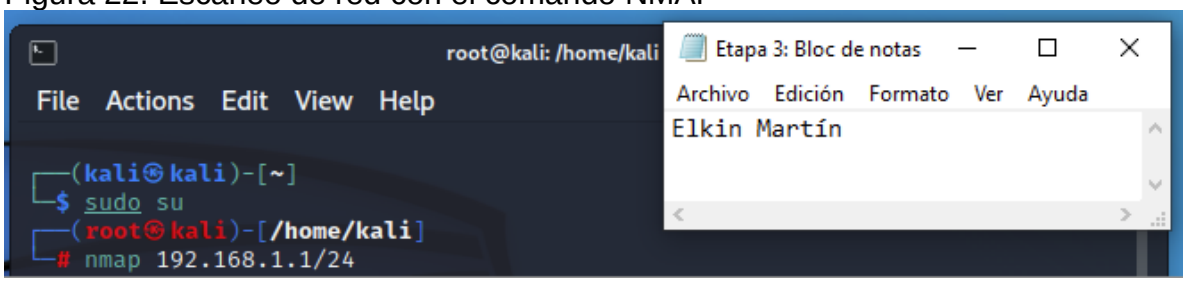
Figura 21. Revisando IP del equipo Kali Linux



Fuente: autoría propia

La figura 22, muestra el proceso de escaneo de red con el comando NMAP y el rango de IP encontrando en el paso anterior 192.168.1.1/24

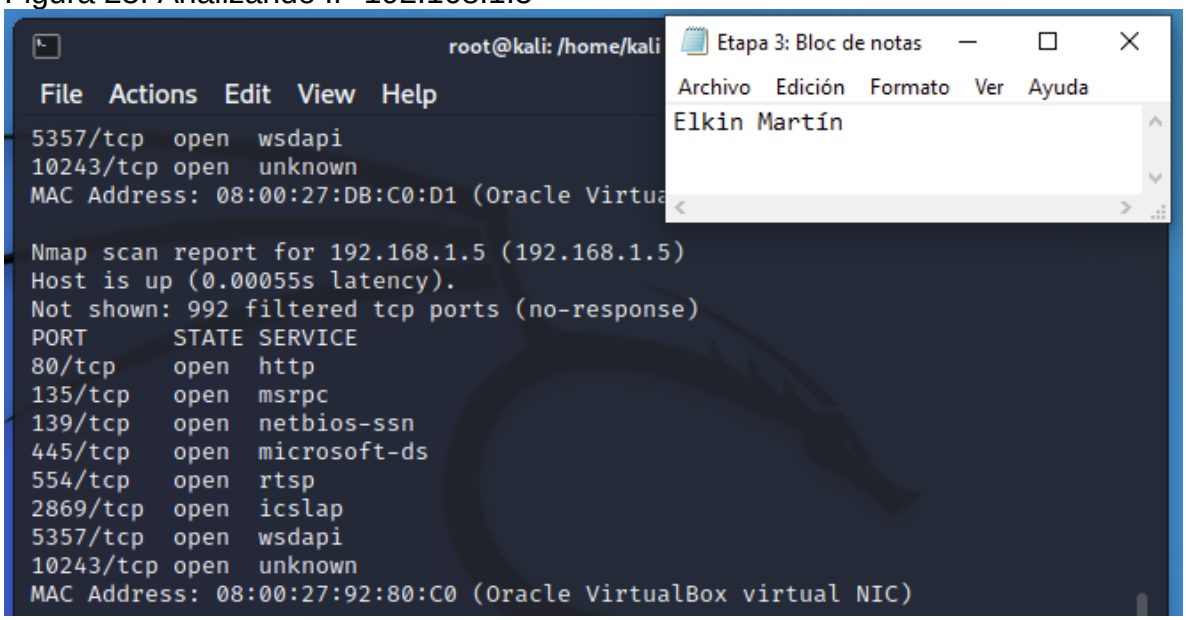
Figura 22. Escaneo de red con el comando NMAP



Fuente: autoría propia

La figura 23, se analiza todos los dispositivos de la red y se observa que la IP 192.168.1.5 tiene abierto el puerto 80, con la información suministrada que el equipo está ejecutando el Rejetto HFS, el cual es un servidor de archivos se podría concluir que esa IP corresponde al equipo que se quiere realizar la prueba.

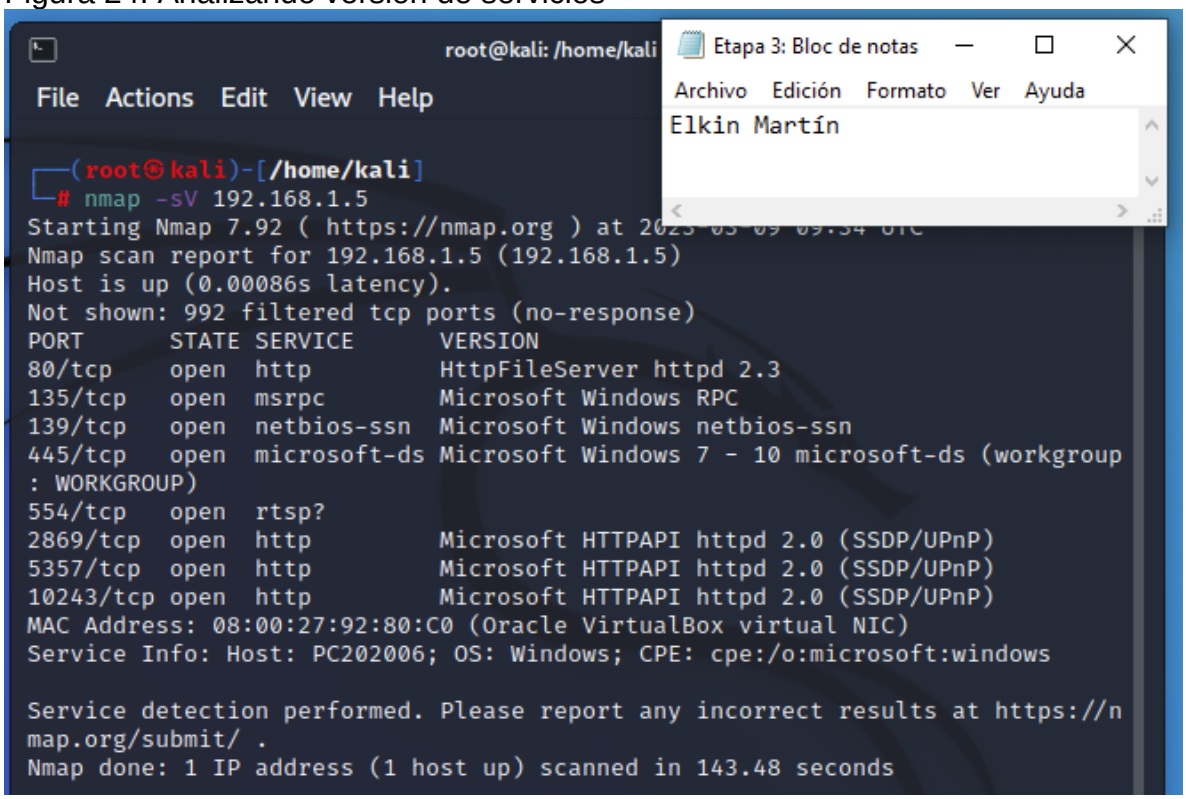
Figura 23. Analizando IP 192.168.1.5



Fuente: autoría propia

En la figura 24, se observa que el puerto 80 está ejecutando una versión de un servidor de archivos versión 2.3, la cual concuerda con la información suministrada del Rejetto HFS v2.3, también se puede observar el nombre del grupo de trabajo “Wordgroup”, grupo por defecto de los sistemas operativos Windows, y que también genera una falla se seguridad en la red, al no tener un nombre de grupo de trabajo personalizado.

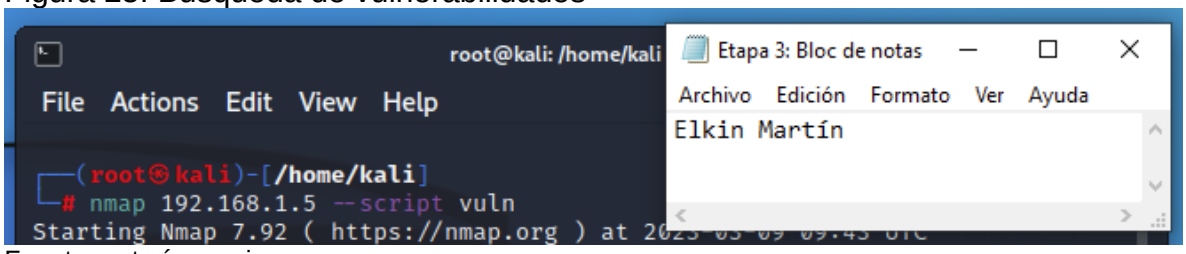
Figura 24. Analizando versión de servicios



Fuente: autoría propia

En la figura 25 se procede a utilizar el comando “NMAP 192.168.1.5 –script vuln” con el cual se va a realizar una exploración de las posibles vulnerabilidades que tenga la máquina.

Figura 25. Búsqueda de vulnerabilidades



Fuente: autoría propia

14.3 VULNERABILIDADES ENCONTRADAS RELACIONADAS CON REJETTO

En el siguiente apartado se procede a realizar un escaneo al equipo que se está revisando el cual tiene dirección IP 192.168.1.5 con el siguiente comando:

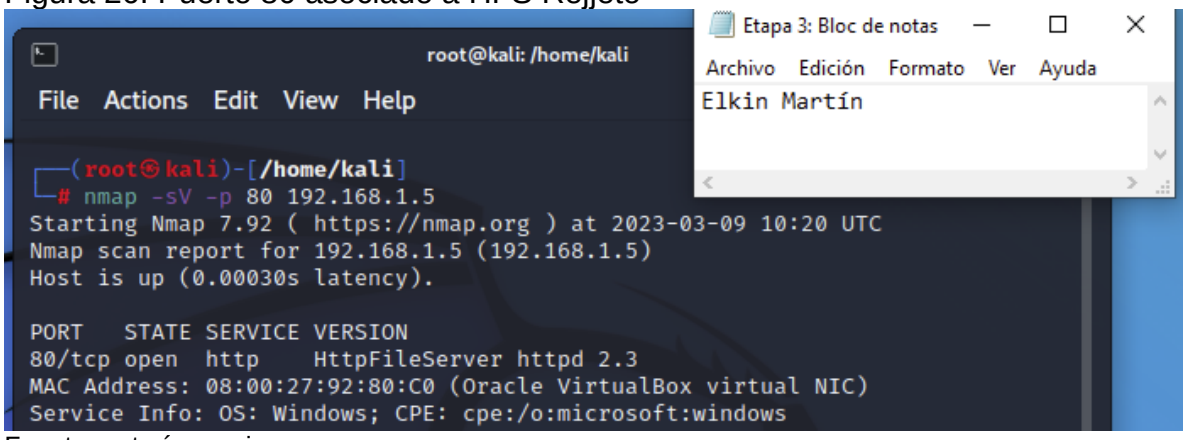
“nmap -sV -p 80 192.168.1.5”

Donde:

“-sV” corresponde a la detección de la versión de servicios [20]
“-p” número de puerto [21]

La figura 26 muestra el puerto 80 abierto y asociando a un servidor de archivos versión 2.3

Figura 26. Puerto 80 asociado a HFS Rejjeto

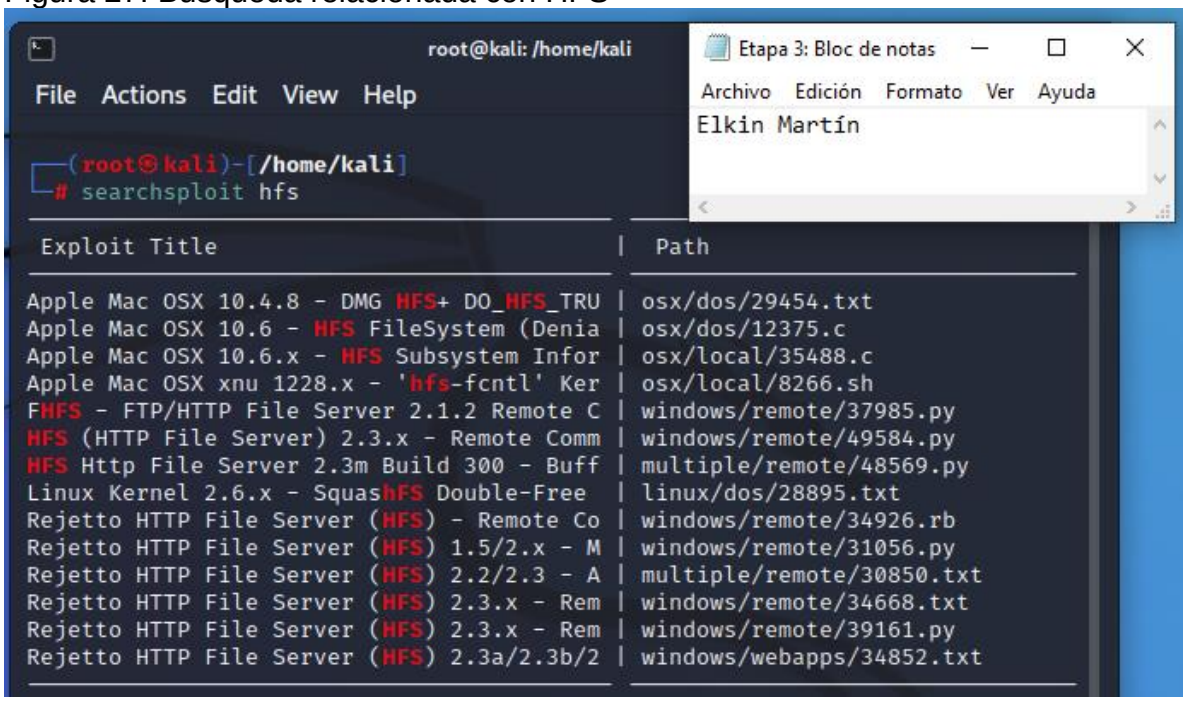


Fuente: autoría propia

En la figura 27 se realiza una búsqueda de exploit relacionados con HFS, y muestra los resultados disponibles.

[20] ELHACKER, Manual y chuleta de comandos con Nmap, [Sitio WEB].[07, marzo, 2023]. Disponible en: https://blog.elhacker.net/2021/10/chuleta-comandos-nmap-opciones-nse.html
[21] Ibid., p 1

Figura 27. Búsqueda relacionada con HFS

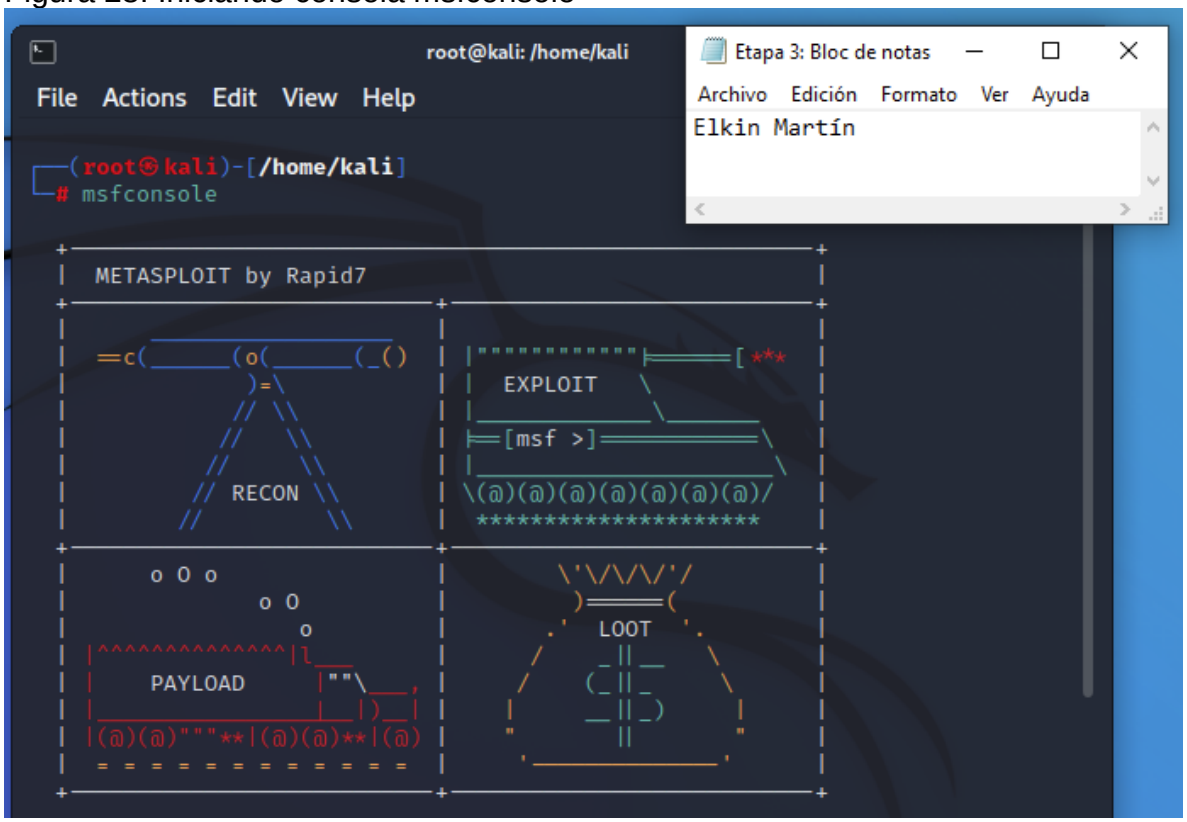


Fuente: autoría propia

14.4 EXPLOTACIÓN VULNERABILIDAD REJETTO

Para realizar la explotación de la vulnerabilidad encontrada, se procede a iniciar la consola con el comando “msfconsole”, esta consola cada vez que inicia muestra una Figura diferente de bienvenida, como se aprecia en la figura 28.

Figura 28. Iniciando consola msfconsole



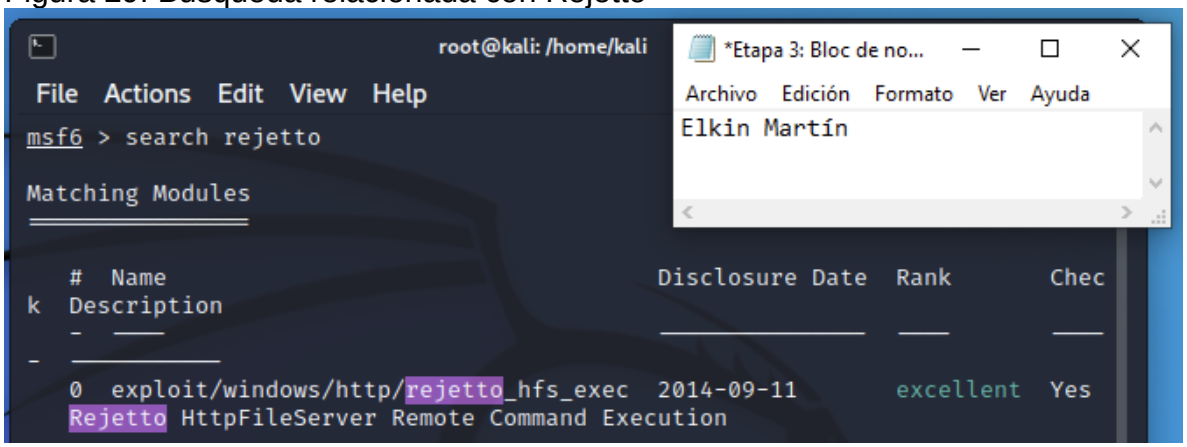
Fuente: autoría propia

Una vez abierta, se comienza con el proceso de explotación de la vulnerabilidad. [22]

En la figura 29 se procede a realizar la búsqueda de exploit relacionada con Rejetto, la cual arroja un resultado.

[22] PENTESTER ACADEMY TV, Basic Exploitation with Metasploit: Windows: HTTP File Server, [Sitio WEB].[05, marzo, 2023]. Disponible en: https://www.youtube.com/watch?v=YQUcyQ4WT6w

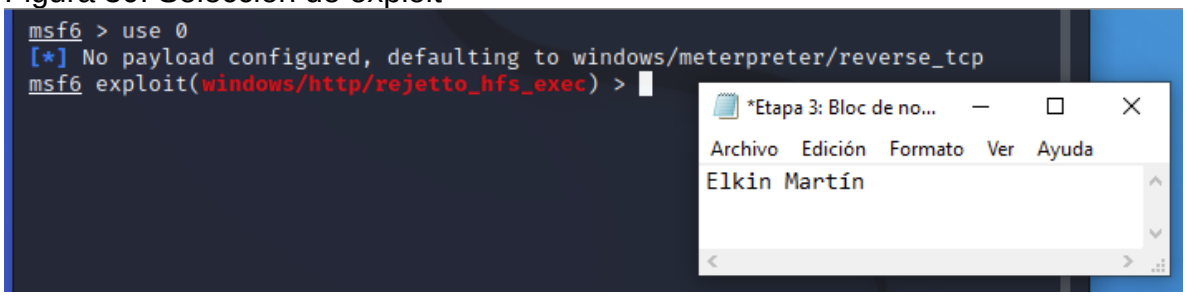
Figura 29. Búsqueda relacionada con Rejetto



Fuente: autoría propia

Luego se procede a seleccionar el exploit disponible, para ese caso con la opción “use 0”, como se evidencia en la figura 30.

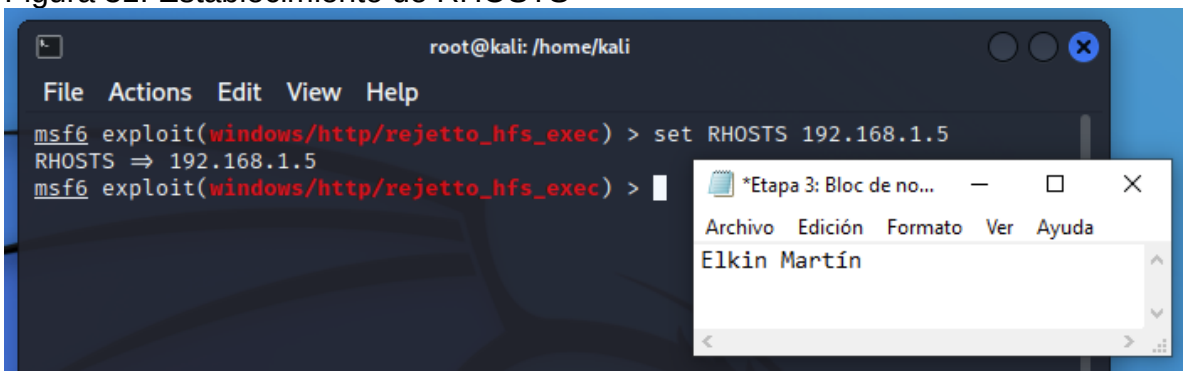
Figura 30. Selección de exploit



Fuente: autoría propia

Se proceda a establecer el RHOSTS con el comando set y la dirección IP, para este caso “set RHOSTS 192.168.1.5”, como se evidencia en la figura 31.

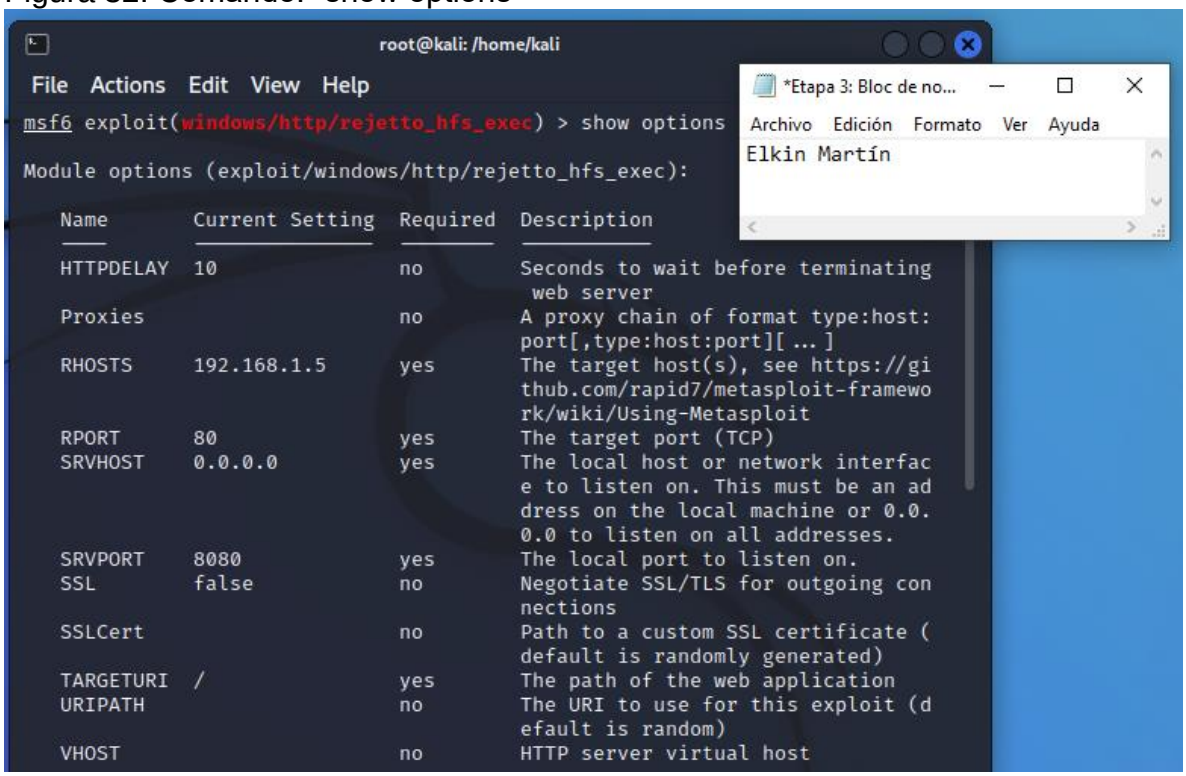
Figura 31. Establecimiento de RHOSTS



Fuente: autoría propia

En la figura 32 se usa el comando “show options” para ver las opciones disponibles para el ataque.

Figura 32. Comando: “show options”

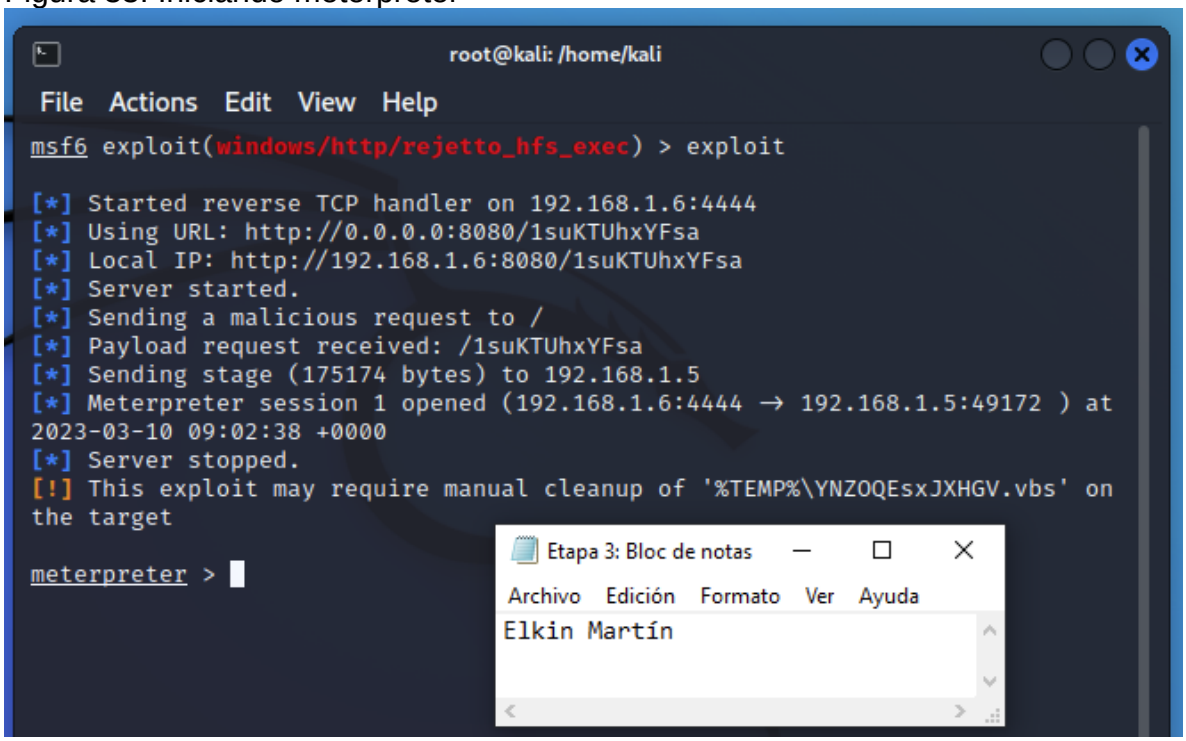


Fuente: autoría propia

Finalmente, en la figura 33 se muestra el paso final para generar el ataque con el comando “exploit”, dependiendo de la conexión y otros factores, puede durar hasta unos minutos, una vez se logra el ataque exitoso, se inicia el “meterpreter” el cual es un payload que permite realizar tareas de forma remota en la máquina víctima[23].

[23] WIDROGO, Metasploit Introduccion: Lo que necesitas saber de Metasploit, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://widrogo.wordpress.com/tag/msfconsole/

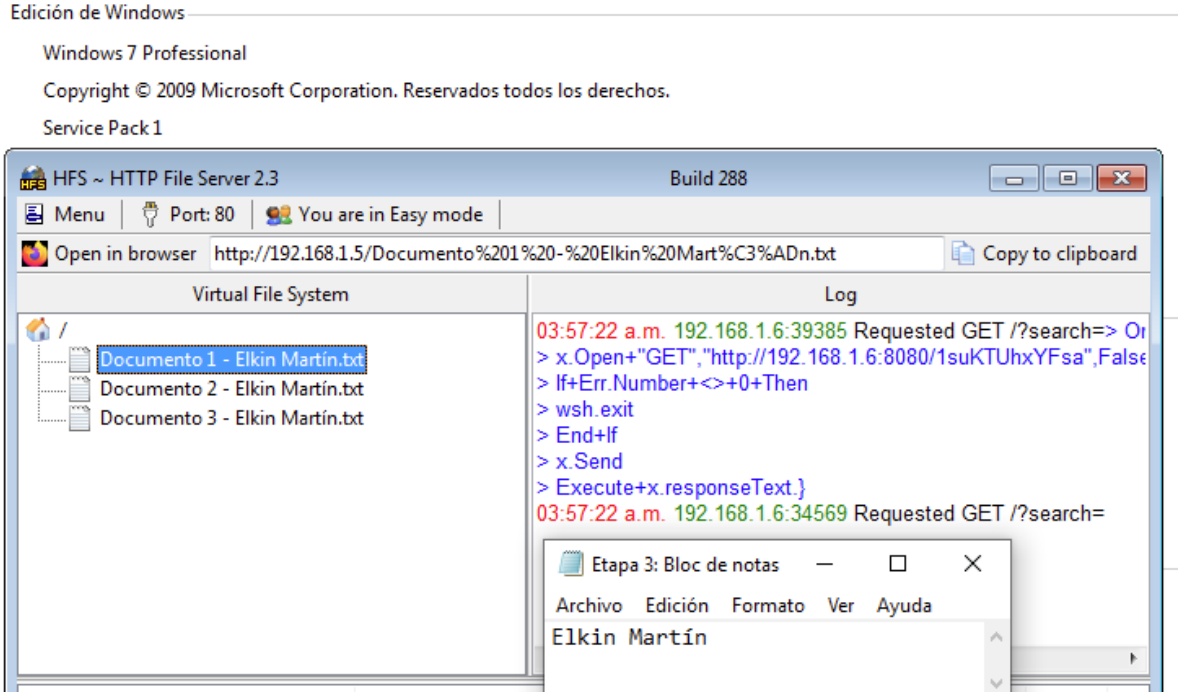
Figura 33. Iniciando meterpreter



Fuente: autoría propia

En la figura 34 se evidencia como el servidor HFS registra los datos (log) mientras se realizaba el ataque desde msfconsole, y se establece la conexión con meterpreter.

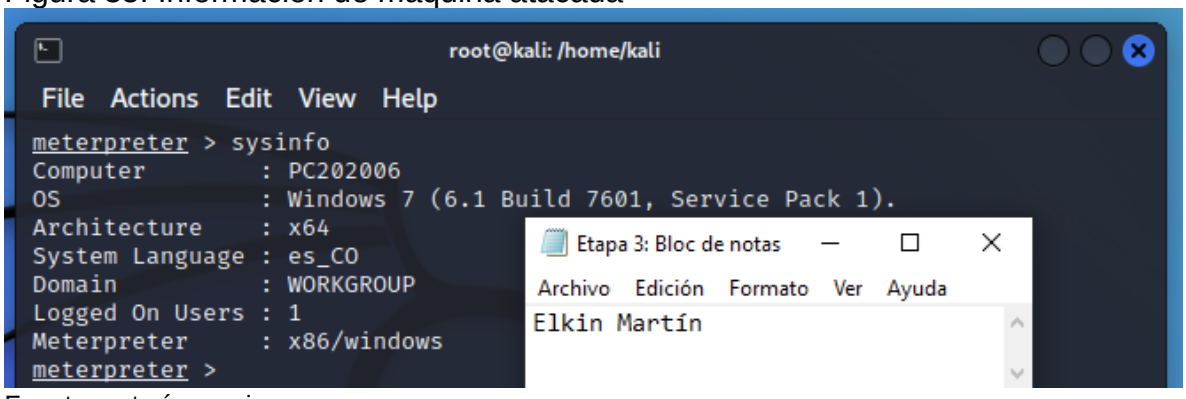
Figura 34. Registro de actividad en HFS



Fuente: autoría propia

En la figura 35 con el uso del comando “sysinfo” se procede a revisar la información básica de maquina atacada, para este caso se aprecia lo siguiente: Nombre del computador, versión del sistema operativo, arquitectura, lenguaje del sistema, nombre del dominio, número de usuarios conectados y la versión del meterpreter.

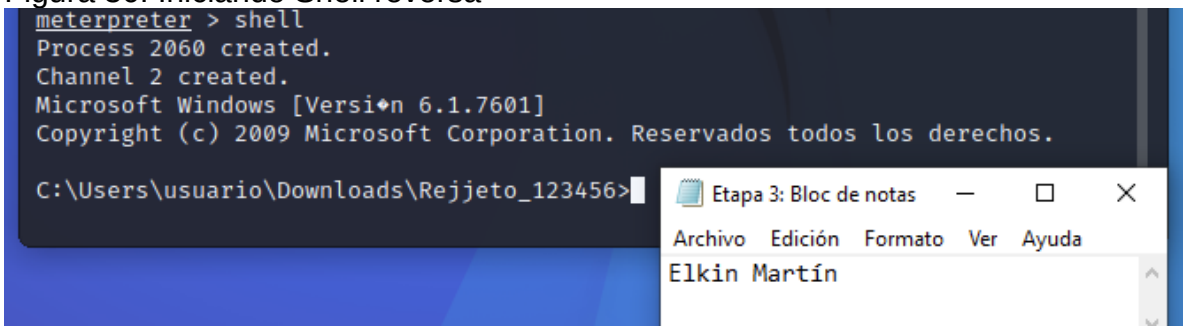
Figura 35. Información de maquina atacada



Fuente: autoría propia

En la figura 36 se procede a iniciar la Shell reversa con el comando “shell”

Figura 36. Iniciando Shell reversa



Fuente: autoría propia

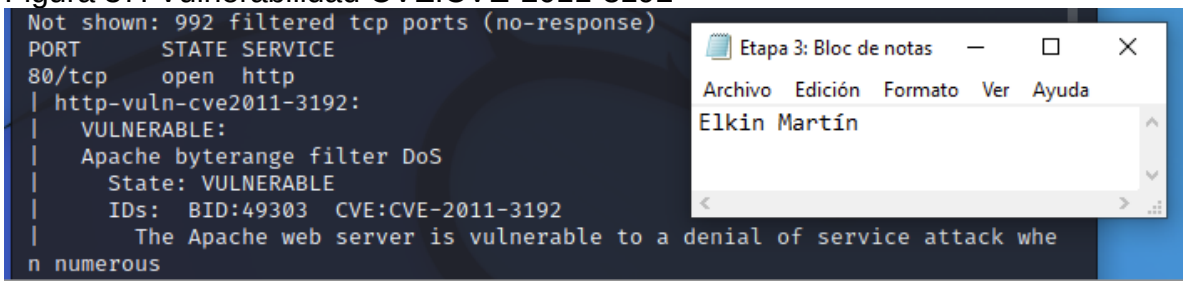
14.5 OTRAS VULNERABILIDADES ENCONTRADAS

Con el uso del comando NMAP 192.168.1.5 –script vuln, mostrado en la Figura 10, se encontraron las siguientes vulnerabilidades:

- Vulnerabilidades relacionadas con el puerto 80

La figura 37 muestra una vulnerabilidad en el puerto 80 CVE:CVE-2011-3192, la cual permite a un atacante remoto generar una denegación de servicio aumentando el consumo memoria RAM y CPU[24].

Figura 37. Vulnerabilidad CVE:CVE-2011-3192



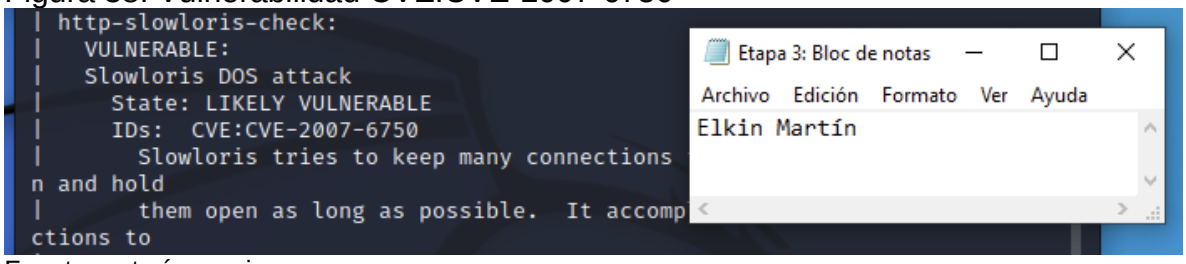
Fuente: autoría propia

La figura 38 muestra una vulnerabilidad en el puerto 80 CVE:CVE-2007-6750, la cual permite a un atacante remoto generar una denegación de servicio (interrupción de demonios) utilizando solicitudes HTTP parciales[25].

[24] CVE. CVE-2011-3192, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2011-3192

[25] CVE. CVE-2007-6750, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750

Figura 38. Vulnerabilidad CVE:CVE-2007-6750

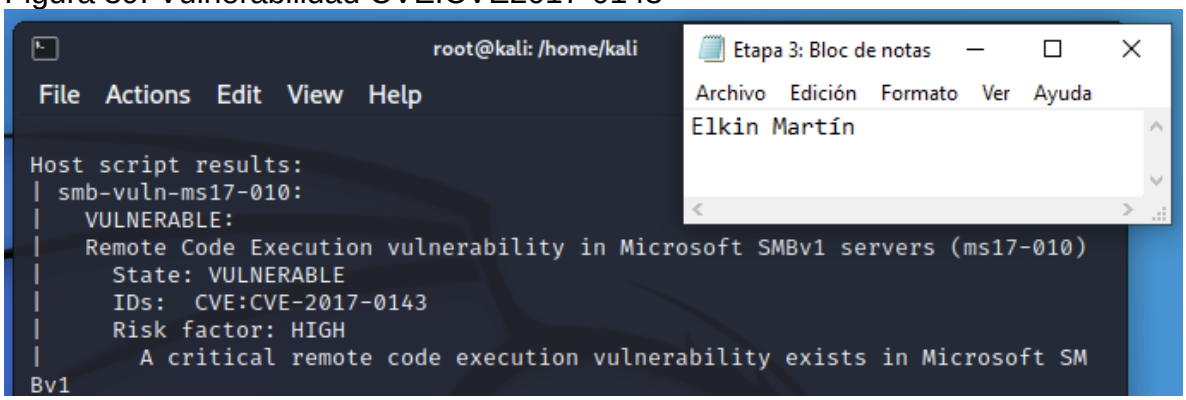


Fuente: autoría propia

- Vulnerabilidades relacionadas con Shell reversa

La figura 39 muestra la vulnerabilidad CVE:CVE2017-0143 la cual permite una ejecución remota de código, generar una Shell reversa[26].

Figura 39. Vulnerabilidad CVE:CVE2017-0143



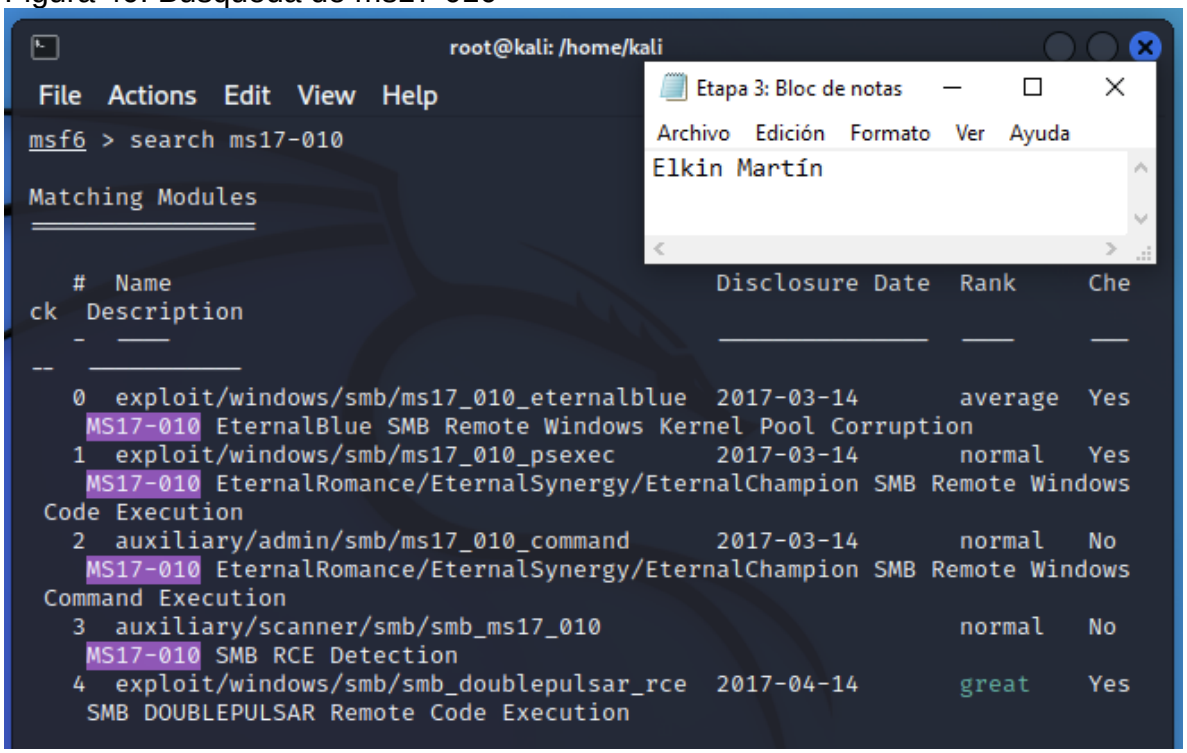
Fuente: autoría propia

14.6 EXPLOTACIÓN VULNERABILIDAD MS17-010

Para iniciar el proceso de explotación de vulnerabilidades, primero se inicia la consola msfconsole, como se aprecia en la figura 13. Una vez iniciada se realiza una búsqueda de la vulnerabilidad encontrada, en este caso así “search ms17-010”, como se evidencia en la Figura 40, mostrando 5 exploit, enumerados del 0 al 4.

[26] CVE. CVE-2017-0143, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

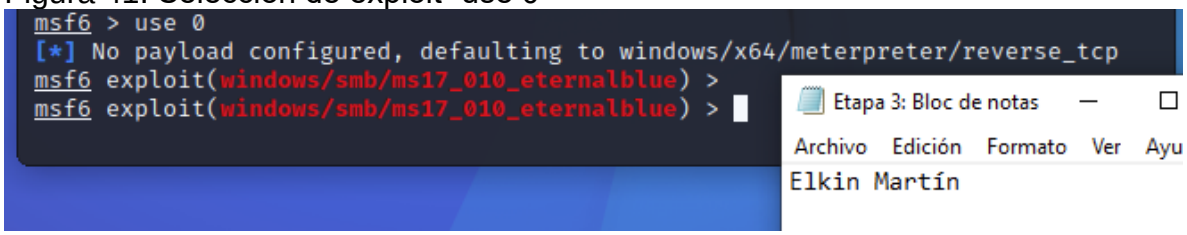
Figura 40. Búsqueda de ms17-010



Fuente: autoría propia

En la figura 41 se selecciona el exploit, para este caso “use 0”

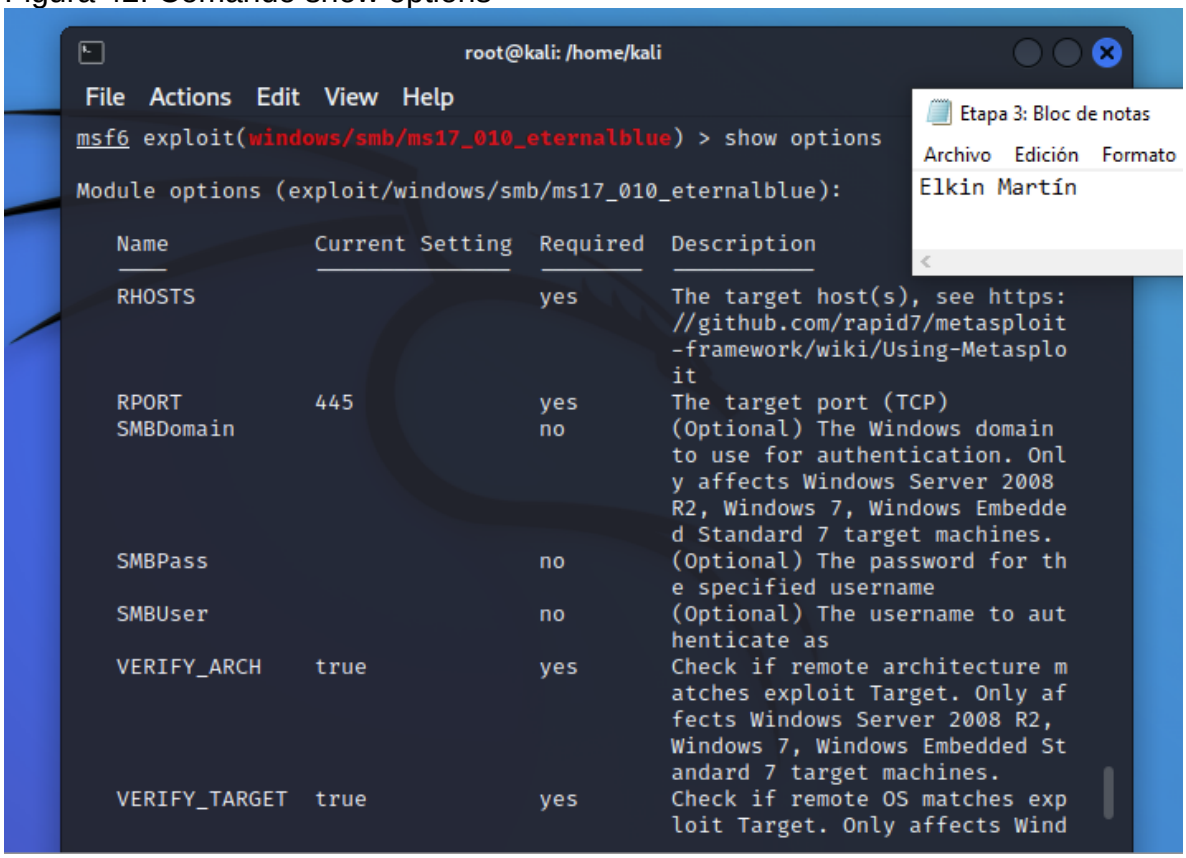
Figura 41. Selección de exploit “use 0”



Fuente: autoría propia

En la figura 42 se procede a ver las posibles opciones con el comando “show options”

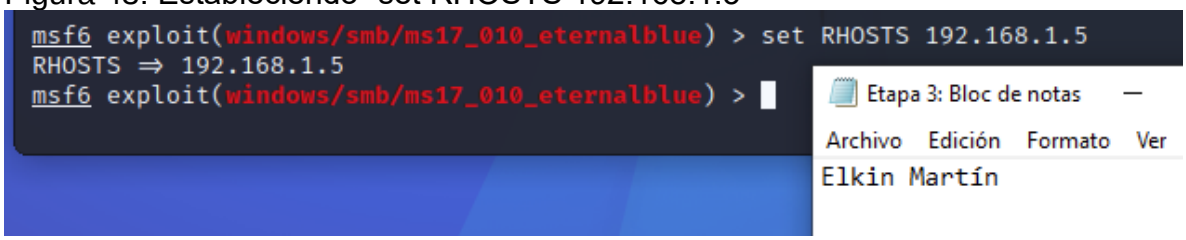
Figura 42. Comando show options



Fuente: autoría propia

En la figura 43 se estable el “set RHOSTS 192.168.1.5”

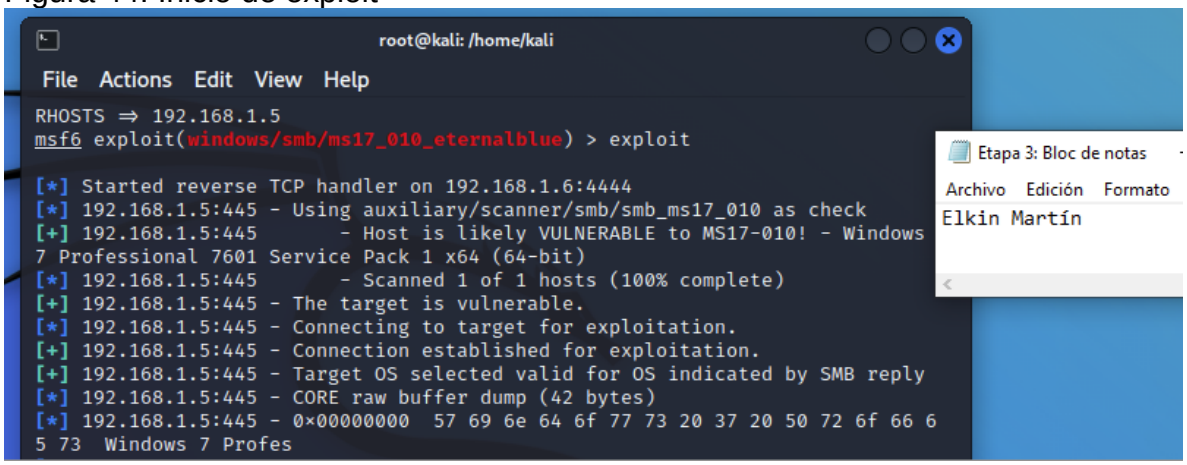
Figura 43. Estableciendo “set RHOSTS 192.168.1.5”



Fuente: autoría propia

En la figura 44 se inicia el exploit, y comienza el proceso para establecer el meterpreter.

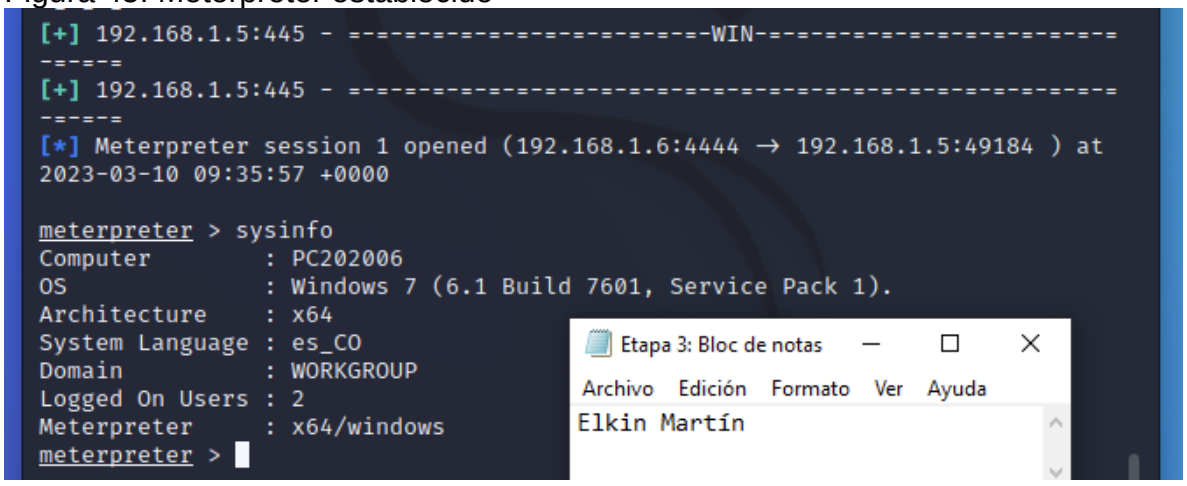
Figura 44. Inicio de exploit



Fuente: autoría propia

La figura 45 se evidencia el meterpreter establecido.

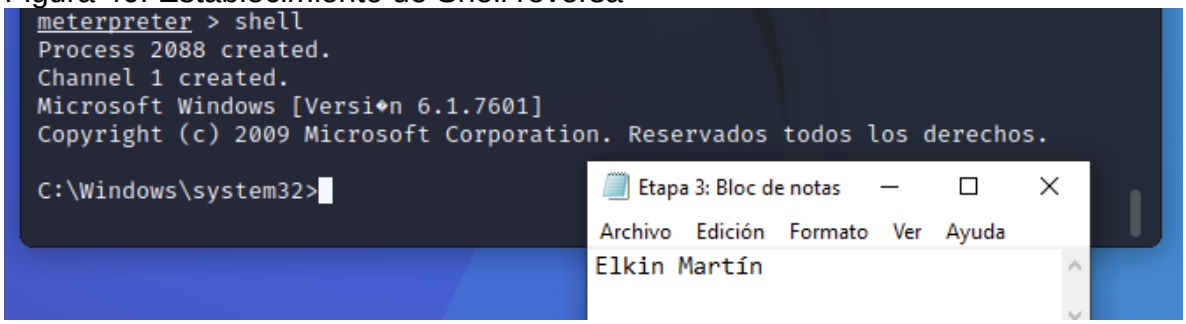
Figura 45. Meterpreter establecido



Fuente: autoría propia

En la figura 46 se evidencia el inicio de la Shell reversa utilizando la vulnerabilidad MS17-010.

Figura 46. Establecimiento de Shell reversa



Fuente: autoría propia

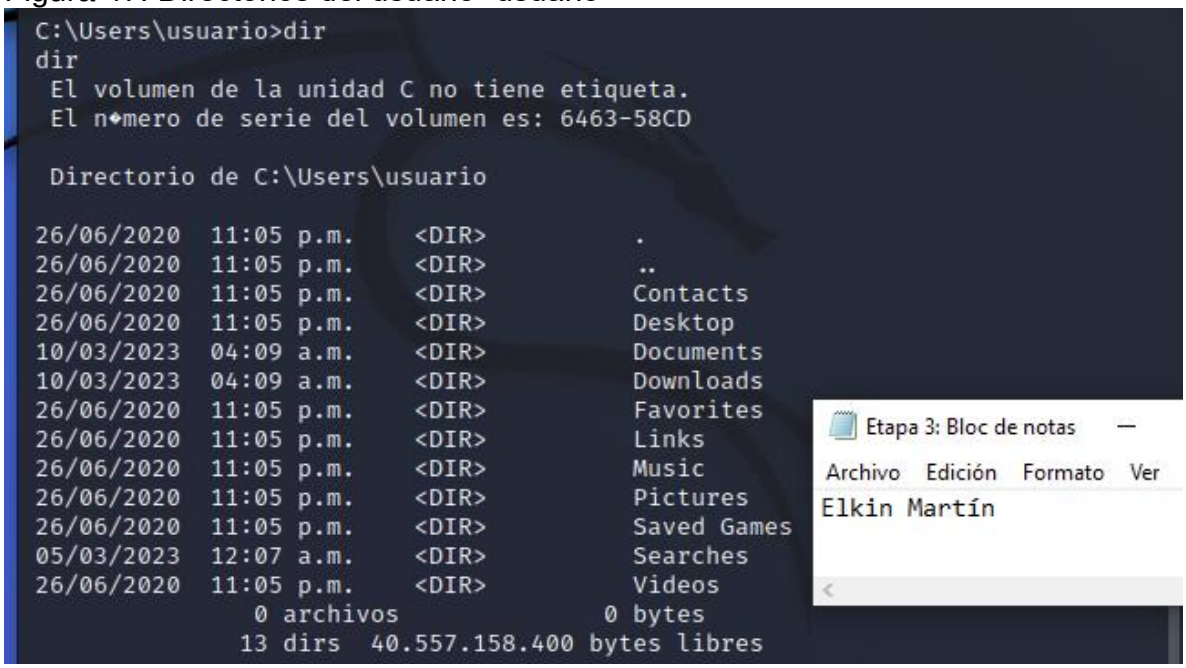
15 EVIDENCIA DE EXPLOTACIÓN

15.1 EVIDENCIA EXPLOTACIÓN VULNERABILIDAD REJETTO

A continuación, se muestra la evidencia de la explotación realizada con la vulnerabilidad el Rejetto

En la figura 47 se evidencia el acceso a la carpeta users/usuario desde la Shell reversa, aca se visualiza los directorios del usuario “usuario” donde se aprecia las carpetas de: escritorio, documentos, descargas, imágenes entre otros.

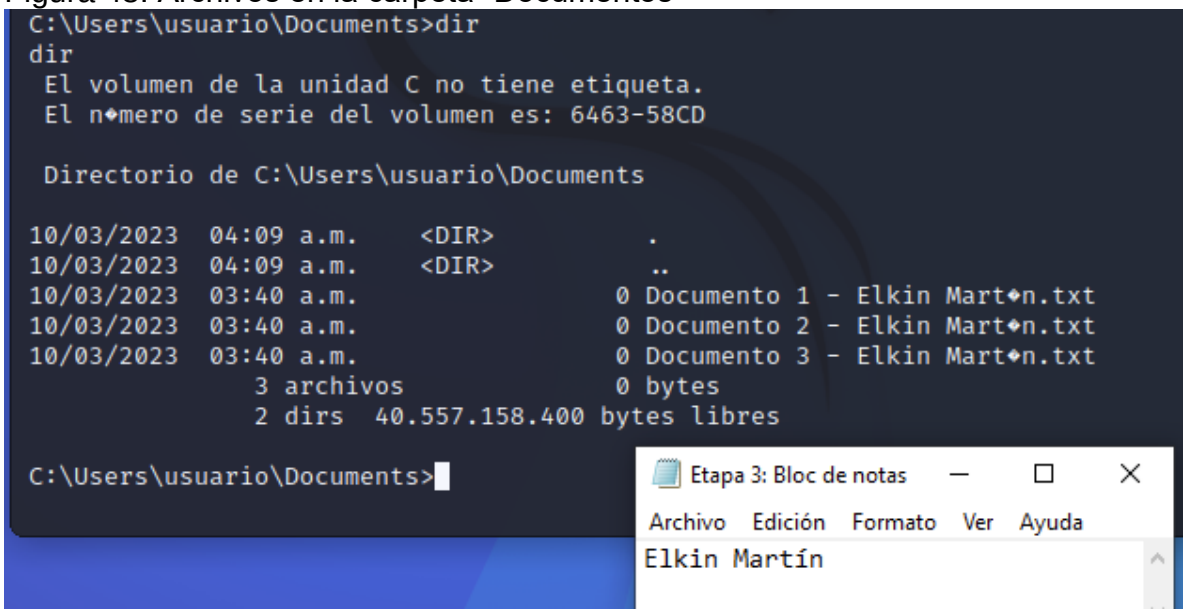
Figura 47. Directorios del usuario “usuario”



Fuente: autoría propia

En la figura 48 se procede a ingresar al directorio documentos, y se visualizan tres archivos del usuario.

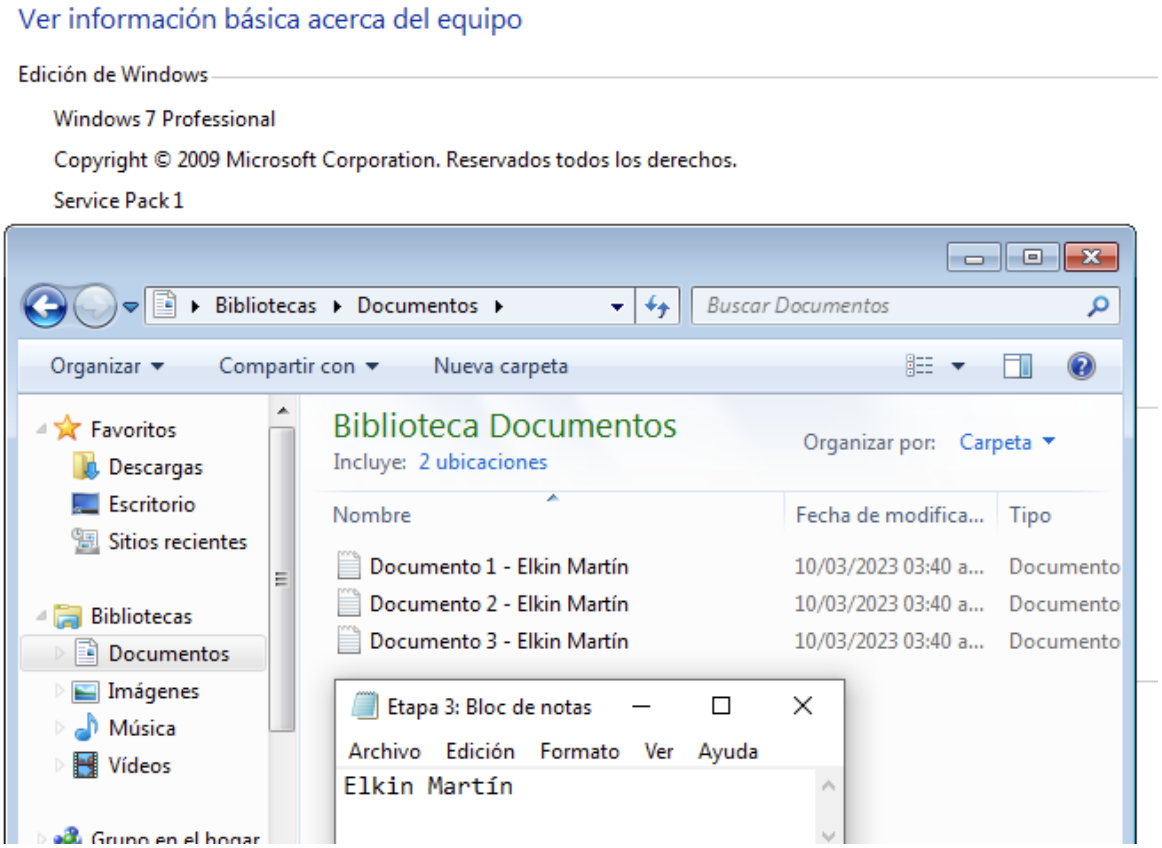
Figura 48. Archivos en la carpeta “Documentos”



Fuente: autoría propia

En la figura 49, se muestra los tres documentos desde el explorador de archivos de Windows 7-64

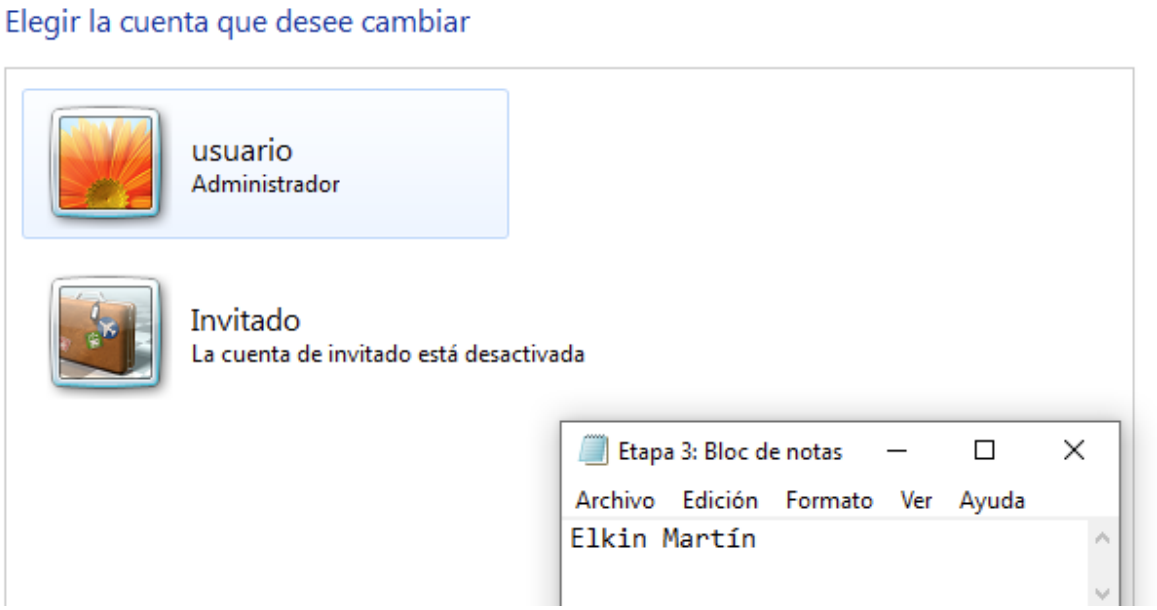
Figura 49. Archivos en la carpeta “documentos” desde Windows 7



Fuente: autoría propia

En la figura 50 se evidencia la existencia de un solo usuario administrador llamado “usuario”.

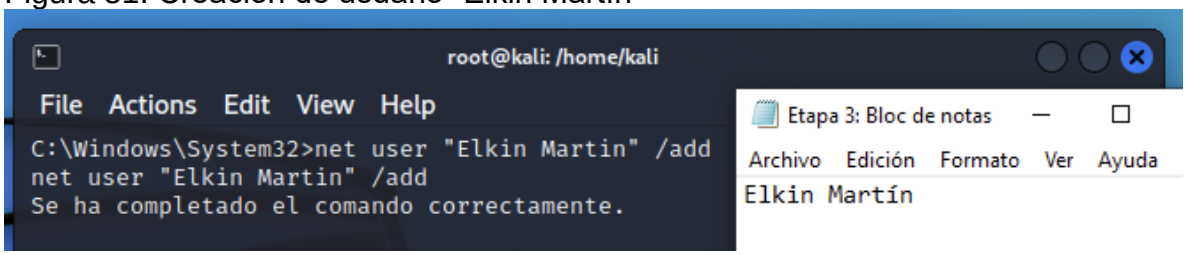
Figura 50. Usuarios en Windows



Fuente: autoría propia

La figura 51 se evidencia la creación de un segundo usuario “Elkin Martín” desde la Shell reversa en Kali Linux, con el comando “net use “nombre usuario” /add [27]”.

Figura 51. Creación de usuario “Elkin Martín”

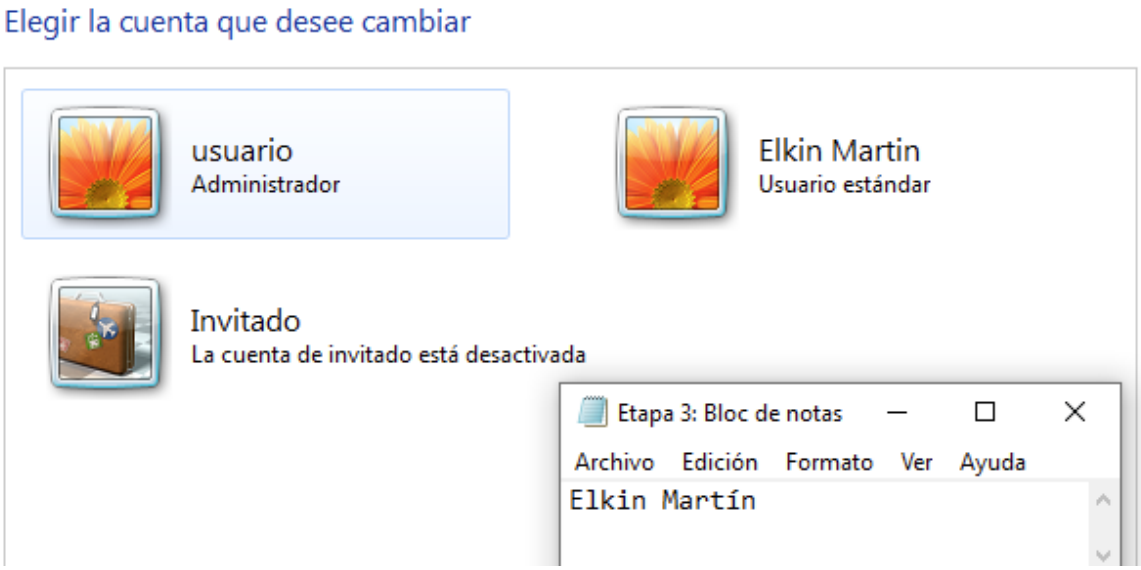


Fuente: autoría propia

En la figura 52 se evidencia la creación del nuevo usuario desde Windows 7.

[27] JCTSOLUCIONES, uso de los comandos net user y net localgroup, [Sitio WEB].[09, marzo, 2023]. Disponible en: https://www.jctsoluciones.com.co/uso-de-los-comandos-net-user-y-net-localgroup/

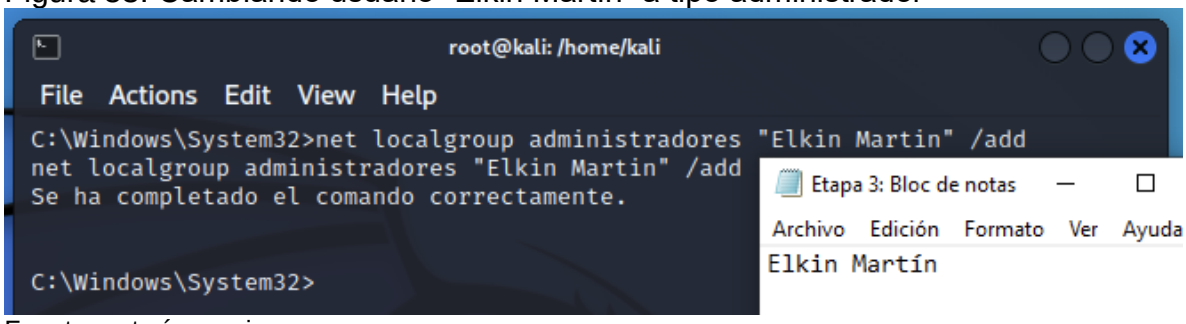
Figura 52. Evidenciado la creación de usuario “Elkin Martín”



Fuente: autoría propia

En la figura 53 se evidencia el escalamiento del usuario “Elkin Martín” a tipo administrador

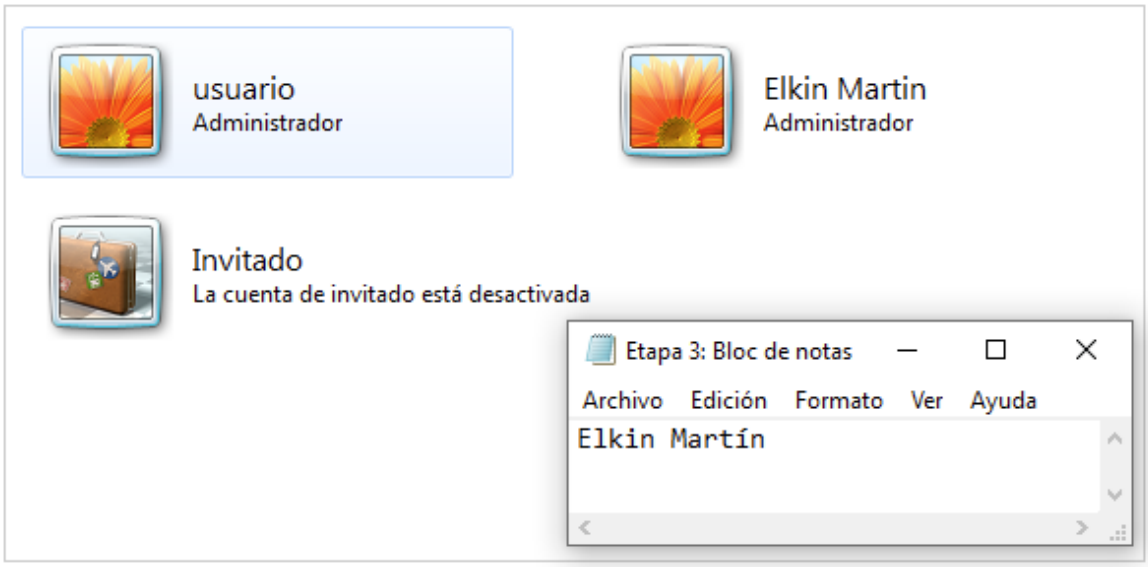
Figura 53. Cambiando usuario “Elkin Martín” a tipo administrador



Fuente: autoría propia

En la figura 54 se evidencia desde Windows como el usuario “Elkin Martín” ahora es usuario administrador.

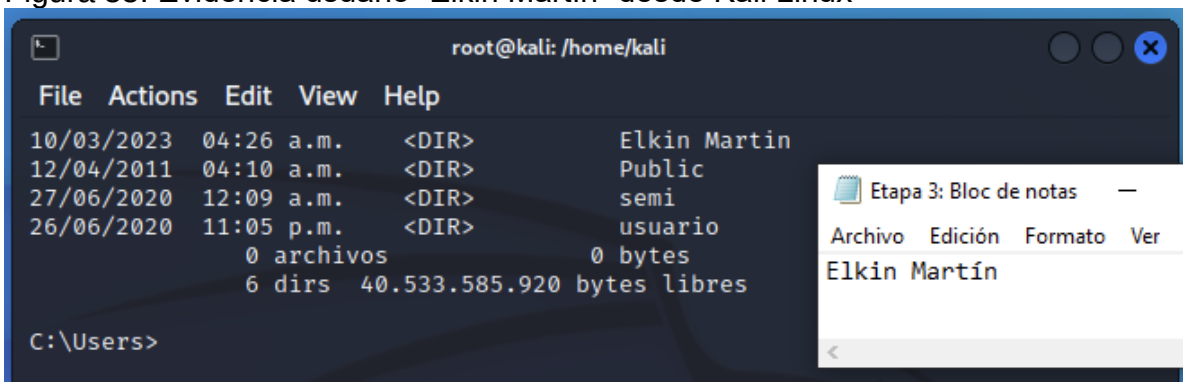
Figura 54. Evidencia usuario “Elkin Martín” como administrador



Fuente: autoría propia

En la figura 55 se evidencia la creación del nuevo usuario “Elkin Martín” desde la Shell reversa en Kali Linux.

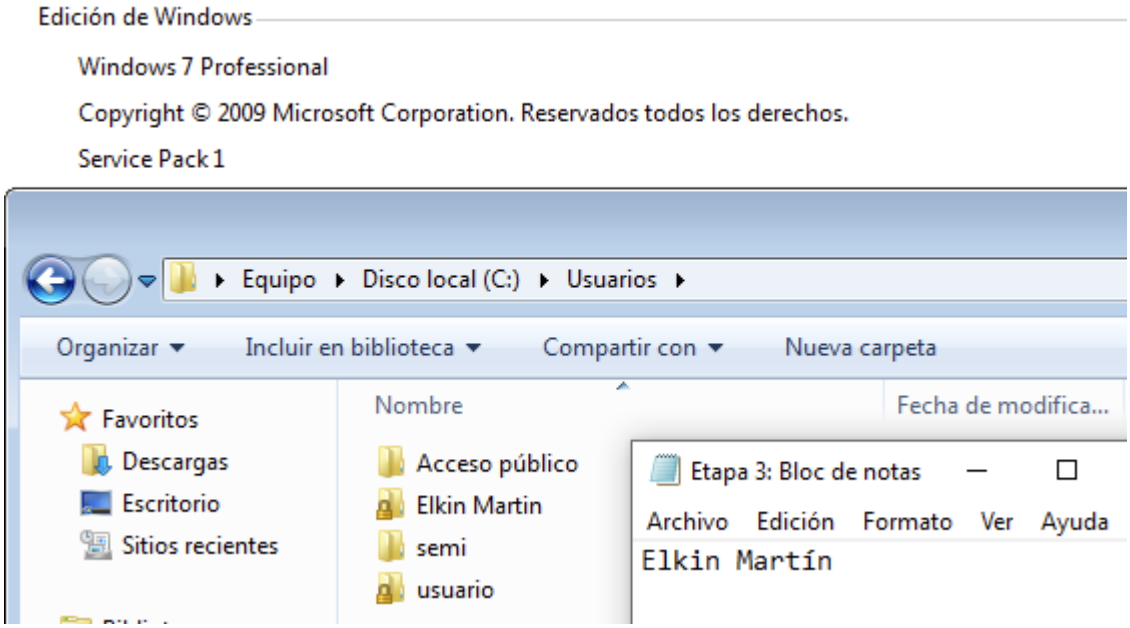
Figura 55. Evidencia usuario “Elkin Martín” desde Kali Linux



Fuente: autoría propia

La figura 56 es la misma evidencia del usuario creado, desde el ambiente de Windows 7.

Figura 56. Evidencia usuario “Elkin Martín” desde Windows 7

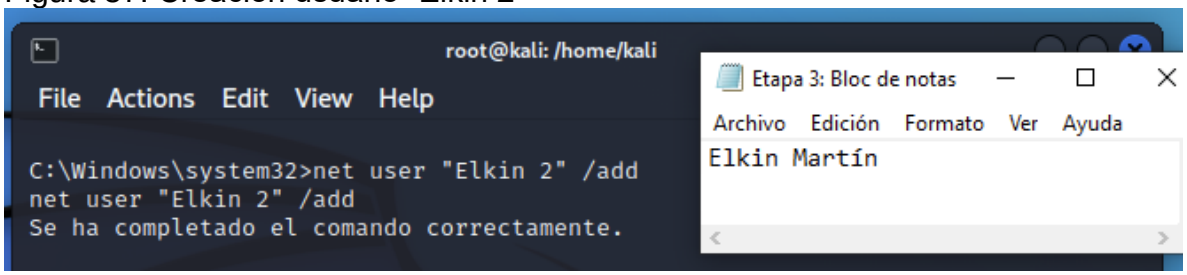


Fuente: autoría propia

15.2 EVIDENCIA EXPLOTACIÓN VULNERABILIDAD MS17-010

Para evidencia la explotación de la vulnerabilidad MS17-010 para crear una Shell reversa, se realiza la misma prueba anterior, de creación de usuario, para este caso “Elkin 2” como se evidencia en la figura 57

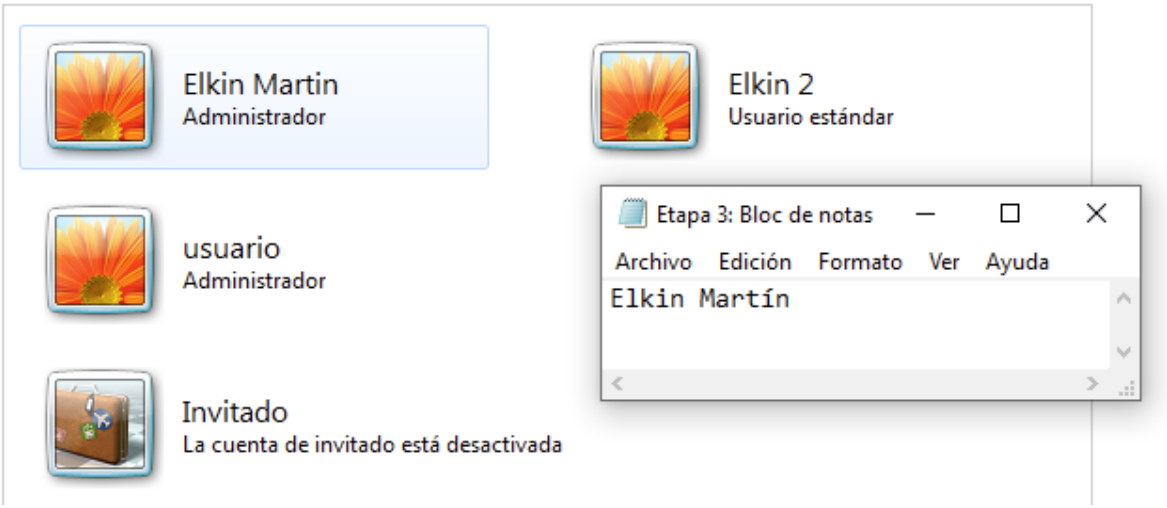
Figura 57. Creación usuario “Elkin 2”



Fuente: autoría propia

La figura 58 evidencia la creación del usuario “Elkin 2” desde el ambiente de Windows 7

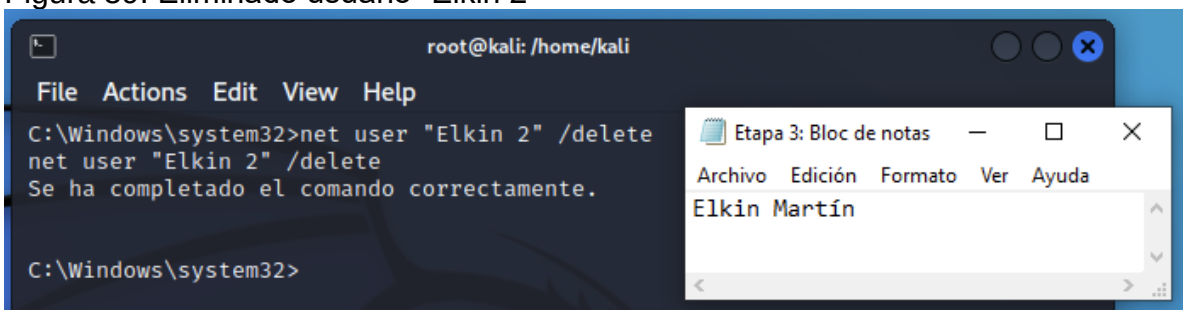
Figura 58. Usuario “Elkin 2” desde Windows



Fuente: autoría propia

Para continuar con la prueba de la Shell reversa se procede a eliminar el usuario “Elkin 2”, como se aprecia en la figura 59.

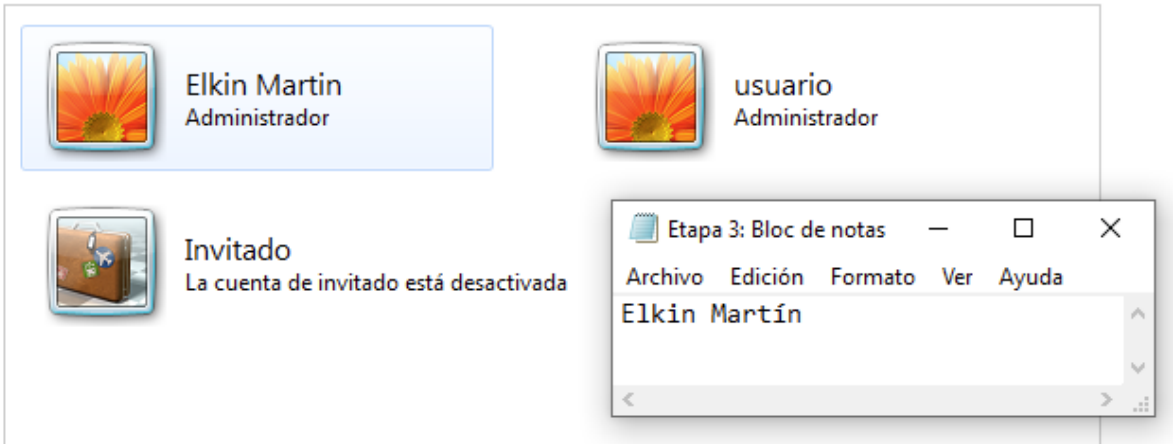
Figura 59. Eliminado usuario “Elkin 2”



Fuente: autoría propia

En la figura 60 se evidencia la eliminación del usuario “Elkin 2” desde el ambiente de Windows.

Figura 60. Prueba de eliminación de usuario “Elkin 2”



Fuente: autoría propia

16 CONTENCIÓN DE ATAQUES INFORMÁTICOS EN TIEMPO REAL

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Teniendo como punto de referencia la maquina con Windows 7-64 y al no contar con ningún programa de seguridad instalado, se sugiere proceder de la siguiente manera:

16.1 INDAGACIÓN

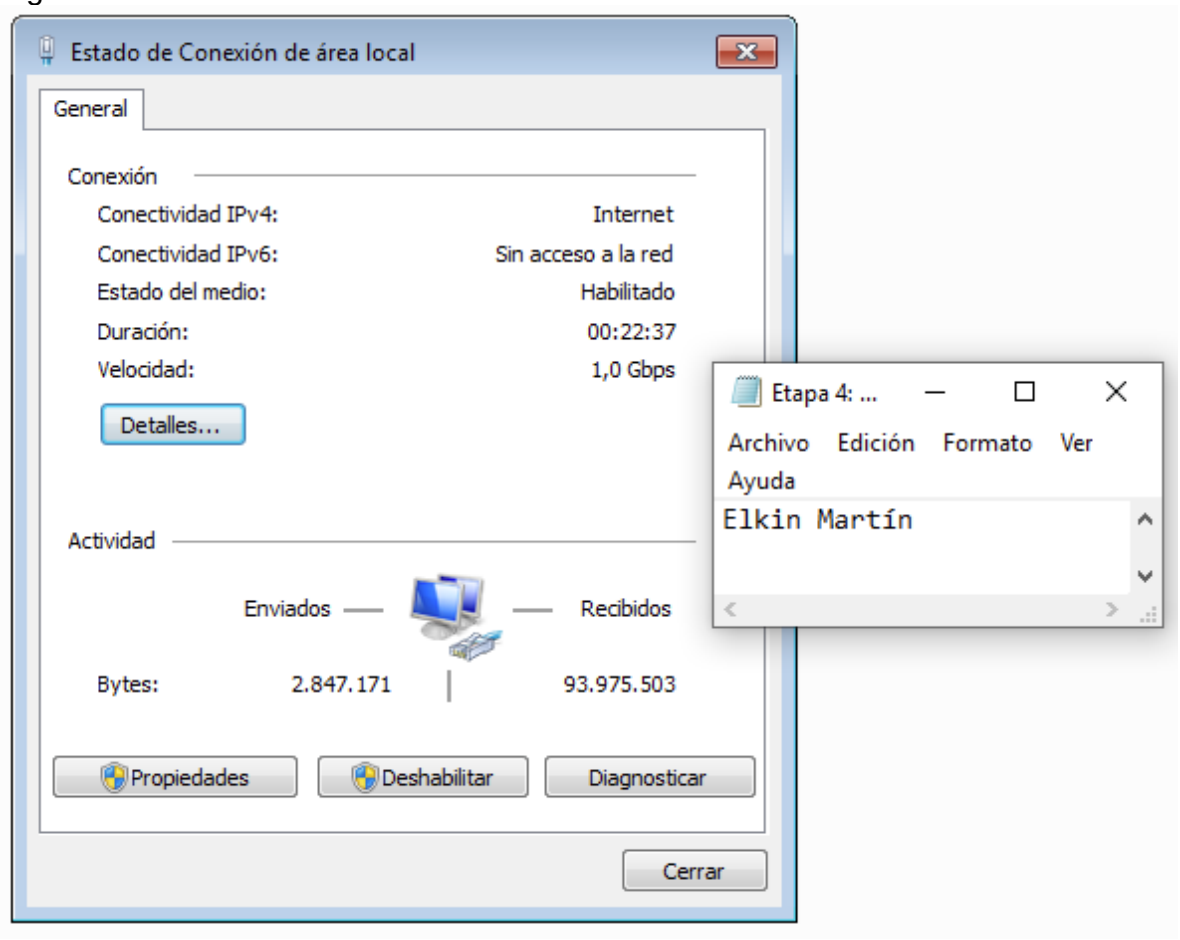
- Verificación por propiedades de la tarjeta de red si es están subiendo datos, al tener todas las aplicaciones web, chat, video y transferencia de archivos cerrados.

Cuando se usa el computador, en el tráfico de red se puede apreciar dos tipos de datos, los datos enviados y los datos recibidos, en el caso de los datos enviados corresponde, por ejemplo, cuando se sube un archivo adjunto a un correo, o se sube algún archivo a una unidad de drive, y los datos recibidos corresponde cuando se navega por cualquier página web o se está visualizando algún contenido en línea por ejemplo videos.

En el uso cotidiano de un computador la cantidad de datos recibidos siempre va a ser mucho mayor que los enviados, a excepción de que sea un servidor, caso en el cual los datos que va a estar enviando siempre va ser mucho mayor que los recibidos.

En la figura 61 se aprecia las propiedades de la tarjeta de red de la maquina Windows 7-64, con un tráfico de red y navegación normal, donde se aprecia que, con 22 minutos de uso, los datos enviados son de 2.847171 bytes y los datos recibidos es de 93.975.503. bytes, casi treinta y tres veces mayor.

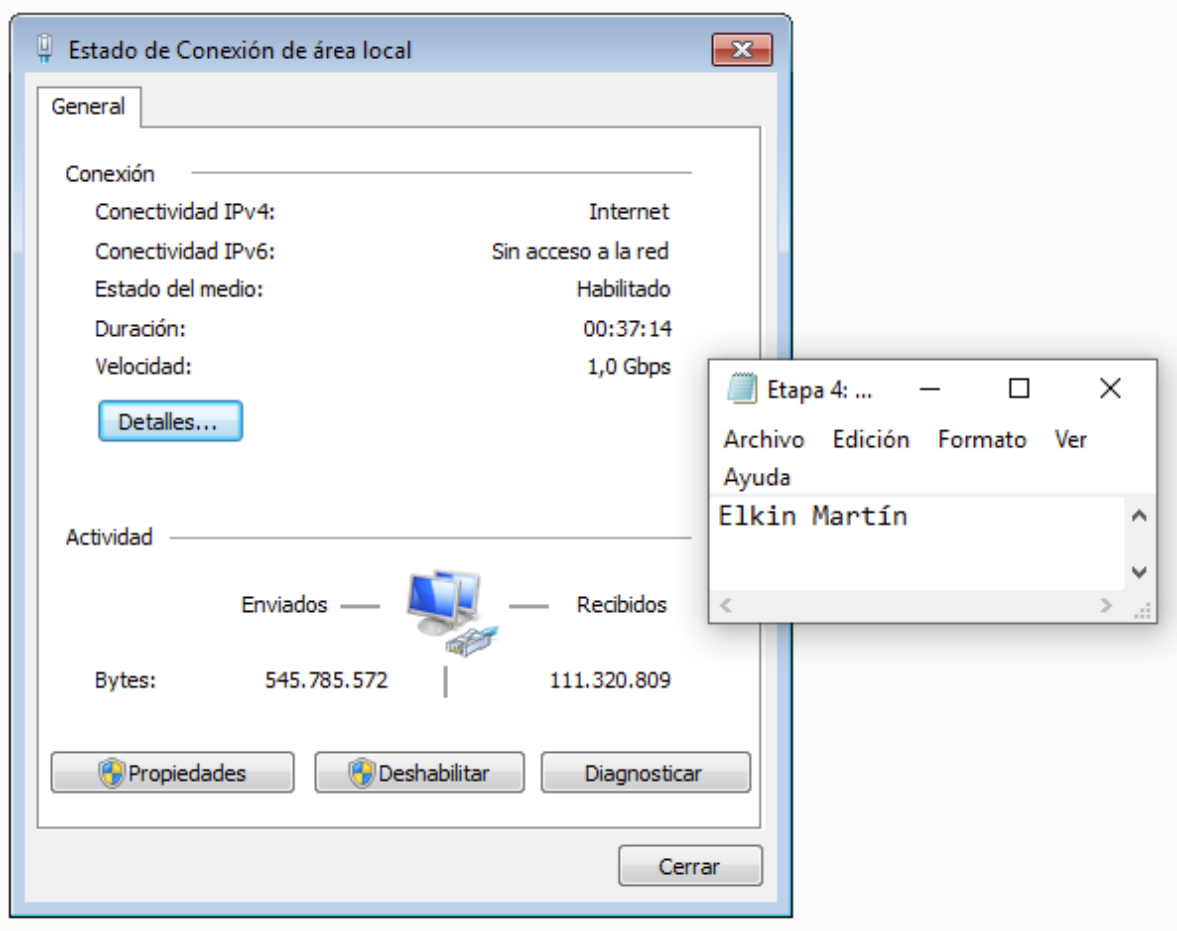
Figura 61. Trafico normal de red



Fuente: autoría propia

Pero si por el contrario al analizar el tráfico de red, los datos enviados son mucho mayor que los recibidos como se aprecia en la figura 62, que con 37 minutos de uso es aproximadamente cinco veces mayor que el recibido, (datos enviados 545.785.572 Bytes, datos recibidos 111.320.829 Bytes) y el usuario indica que no ha iniciado ningún servicio de chat, video llamada o similar, se pasaría a la siguiente indagación.

Figura 62. Trafico anormal de red

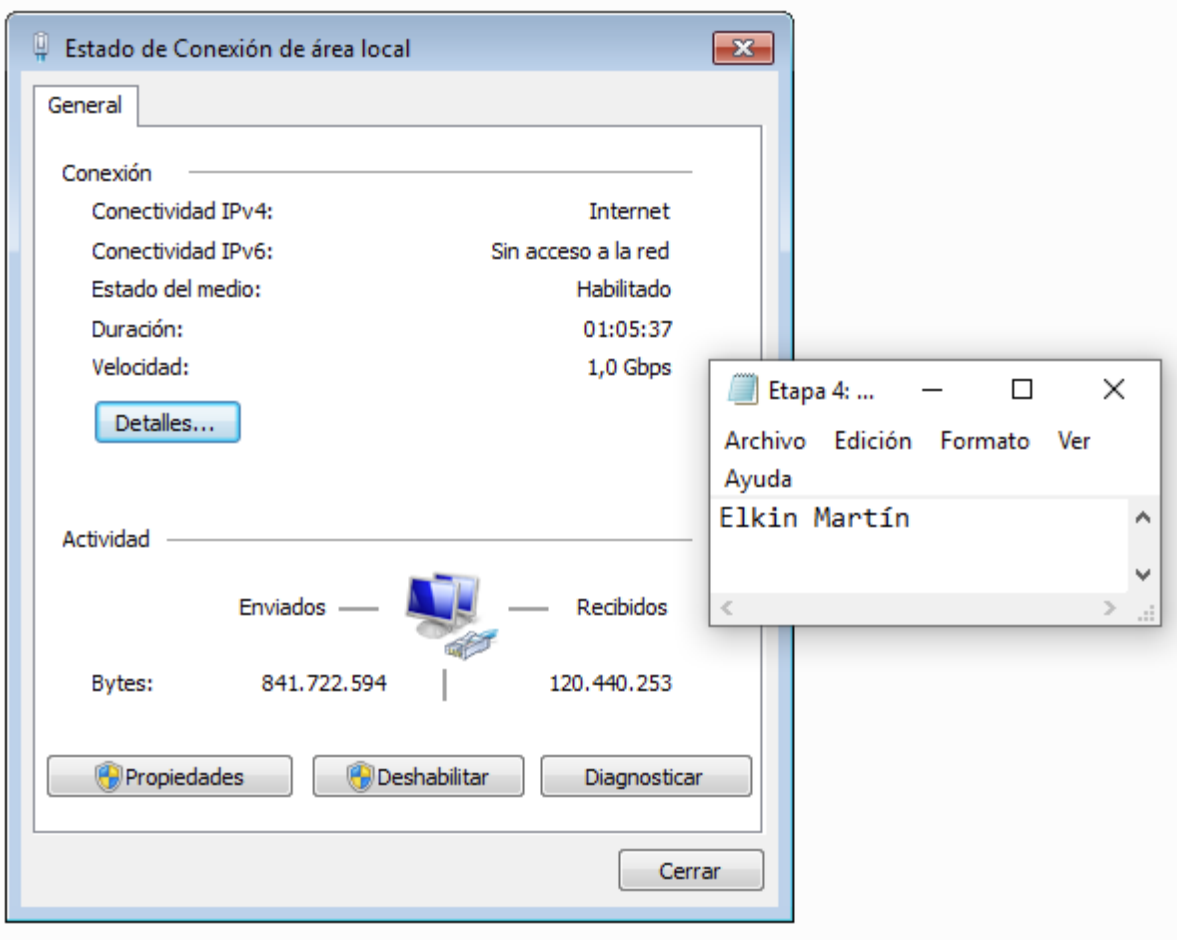


Fuente: autoría propia

- Al verificar que el computador está enviando archivos, verificar si algún usuario está utilizando la aplicación HFS Rejjeto en ese momento, en caso de que no, se asimila que el computador está en pleno ataque.

Para el caso de estudio el usuario indica que no ha utilizado la aplicación HFS Rejjeto, quizás ni siquiera la conoce, pero como se aprecia en la figura 63. Con más de una hora de uso la maquina ha enviado 841.722.594 bytes, mientras que los datos recibidos son de 120.440.253 bytes, lo que indica que la maquina está en pleno ataque.

Figura 63. Windows enviado datos

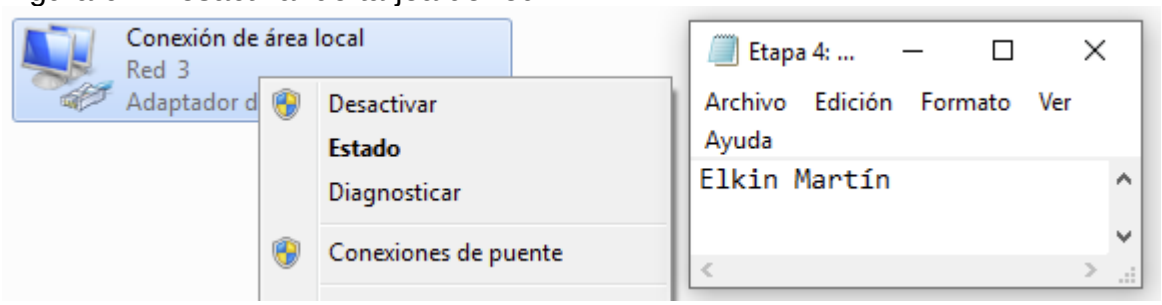


Fuente: autoría propia

16.2 PROCEDIMIENTO

- Una vez identificado que el computador está enviando datos, y ningún usuario lo está usando, lo primero es desconectar la red LAN para impedir el acceso no autorizado del atacante, puede ser descontando el cable de red o deshabilitando la tarjeta de red como se aprecia en la figura 64.

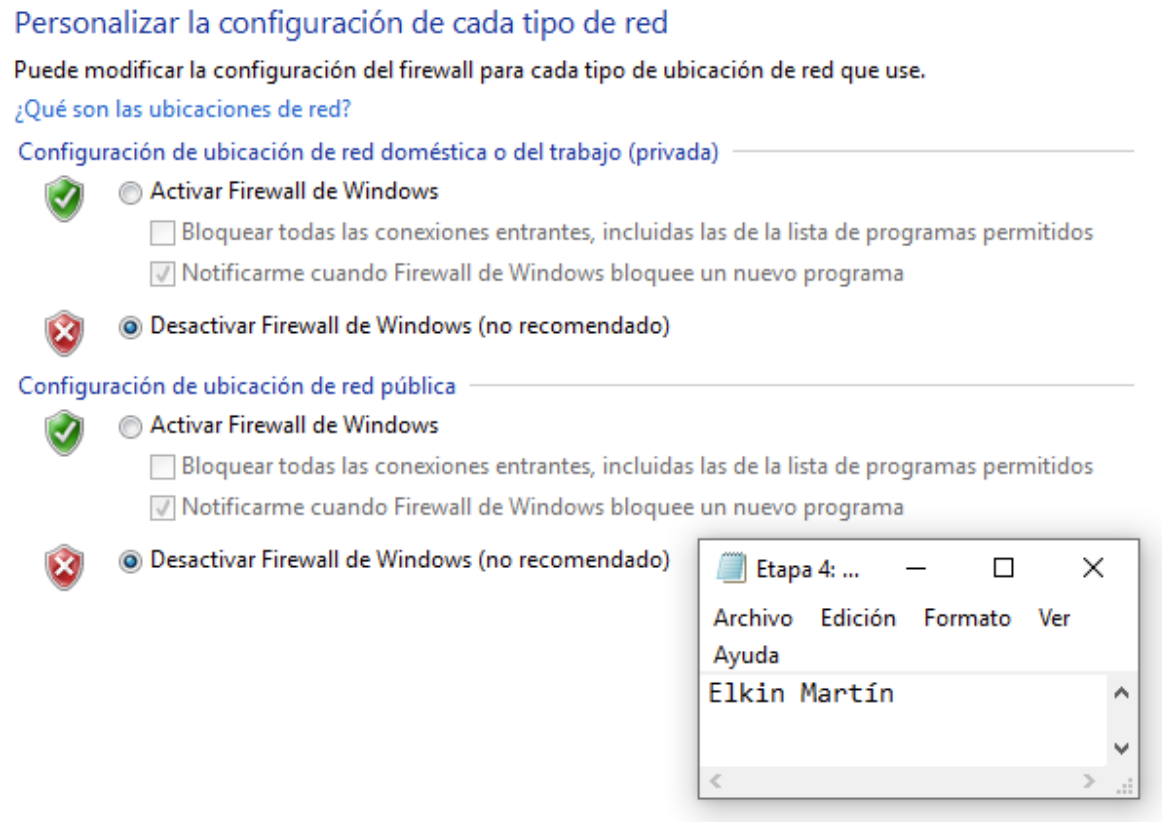
Figura 64. Desactivando tarjea de red.



Fuente: autoría propia

- Revisar configuración de firewall y antivirus, como se aprecia en la figura 65, la maquina Windows 7-64 tenía deshabilitado el firewall tanto para redes privadas como publicas

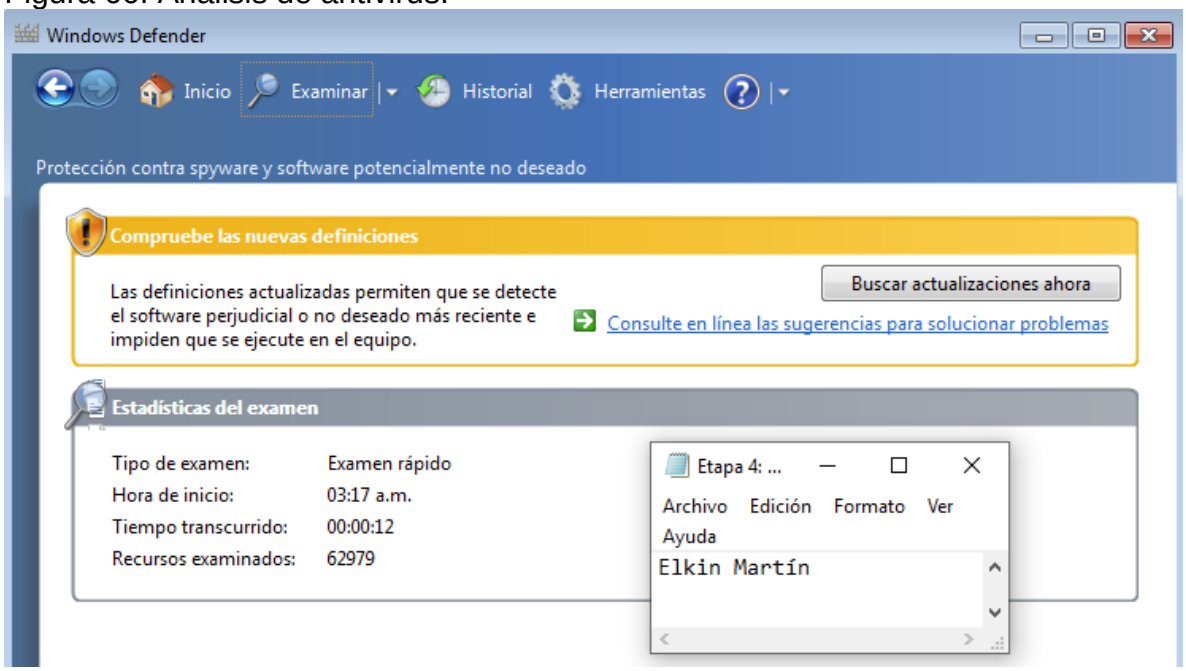
Figura 65. Configuración de firewall de Windows 7-64



Fuente: autoría propia

- Realizar un escaneo de virus y malware, para el caso de estudio la maquina tiene instalado Windows Defender, con lo que se procede a realizar el análisis, como se evidencia en la figura 66

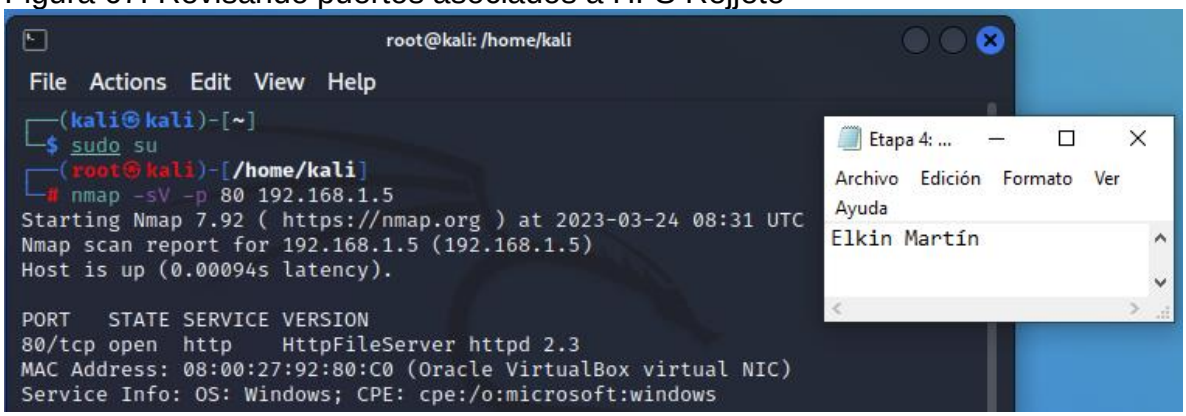
Figura 66. Análisis de antivirus.



Fuente: autoría propia

- Realizar un escaneo de vulnerabilidades, puede ser con NMAP, como se evidencia en la figura 67, desde un Kali Linux del equipo Blue team, se analiza el puerto 80.

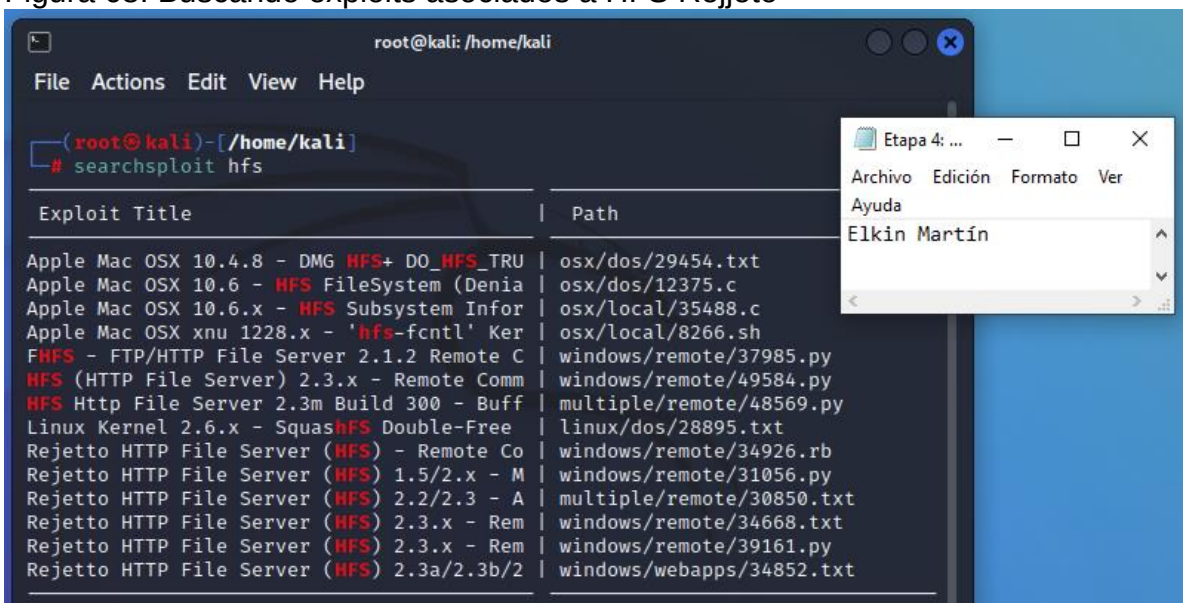
Figura 67. Revisando puertos asociados a HFS Rejjeto



Fuente: autoría propia

En la figura 68 se realiza una búsqueda de las vulnerabilidades relacionadas con HFS Rejjeto

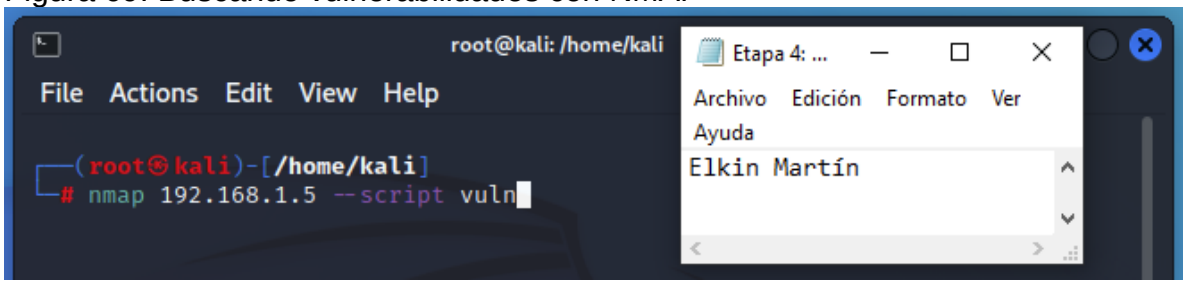
Figura 68. Buscando exploits asociados a HFS Rejjeto



Fuente: autoría propia

Con el comando “NMAP 192.168.1.5 –script vuln” el equipo Blue team procede a buscar vulnerabilidades, como se evidencia en la figura 69.

Figura 69. Buscando vulnerabilidades con NMAP

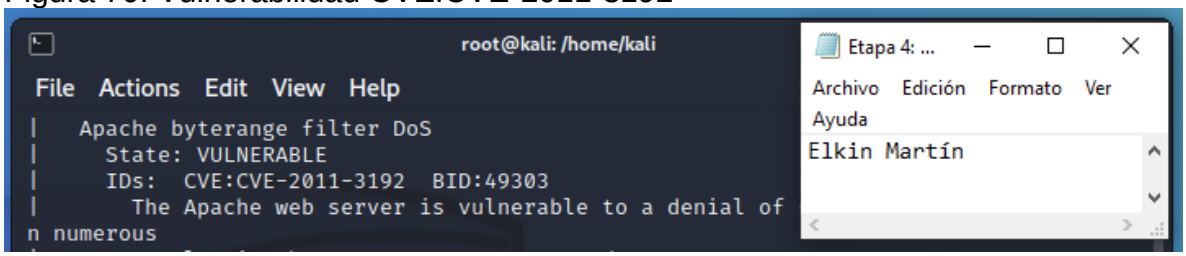


Fuente: autoría propia

Al realizar la búsqueda se encuentran 3 vulnerabilidades más en la maquina Windows 7-64

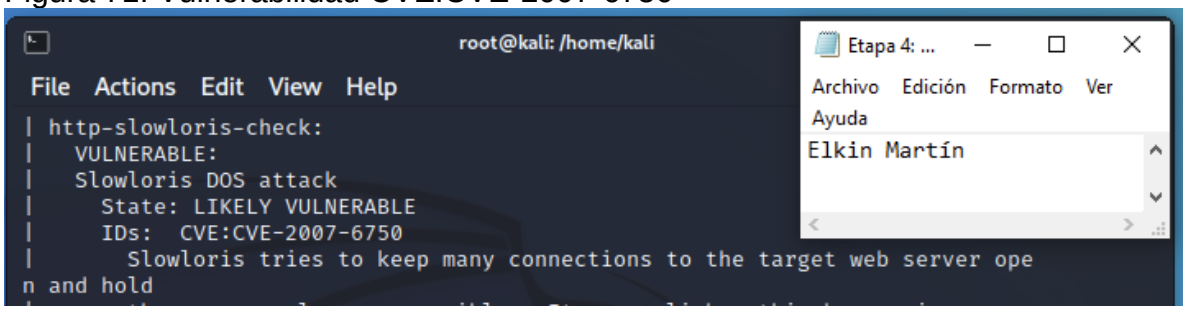
- ✓ Vulnerabilidad CVE:CVE-2011-3192, figura 70
- ✓ Vulnerabilidad CVE:CVE-2007-6750, figura 71
- ✓ Vulnerabilidad CVE:CVE2017-0143, figura 72

Figura 70. Vulnerabilidad CVE:CVE-2011-3192



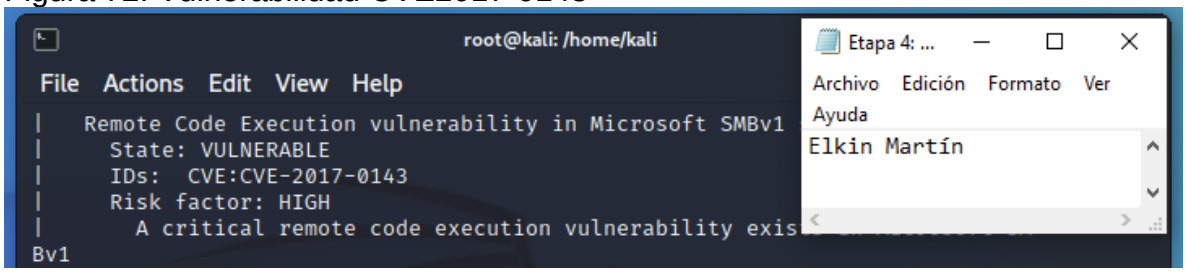
Fuente: autoría propia

Figura 71. Vulnerabilidad CVE:CVE-2007-6750



Fuente: autoría propia

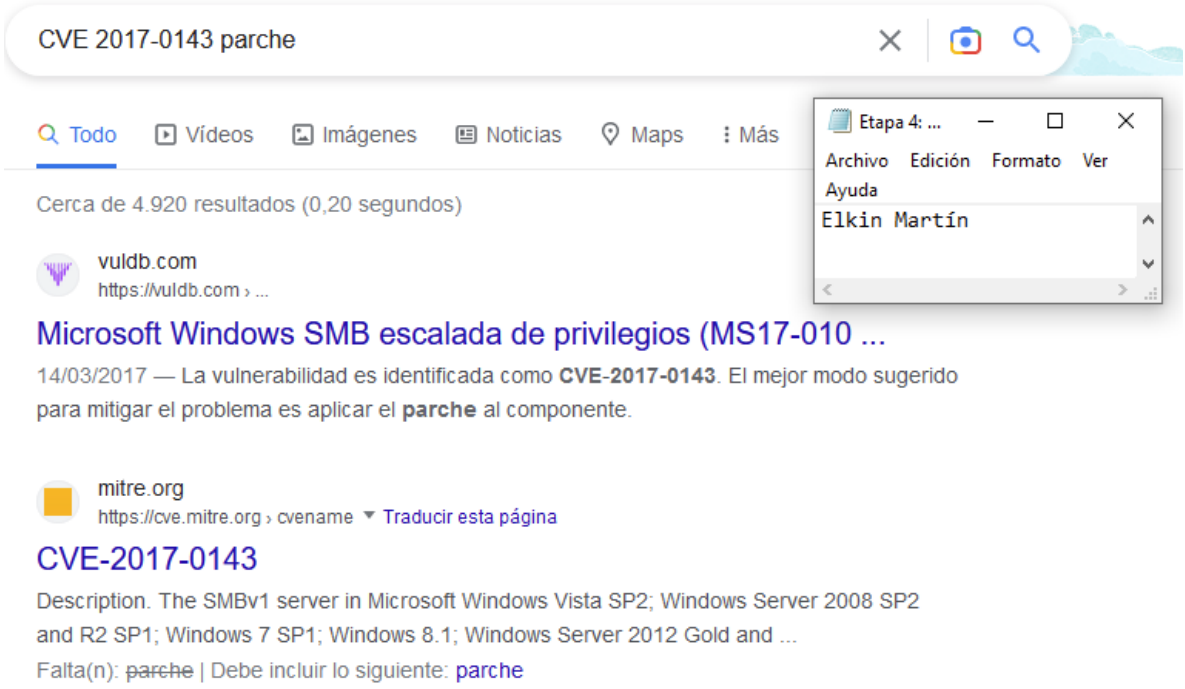
Figura 72. Vulnerabilidad CVE2017-0143



Fuente: autoría propia

- De acuerdo a las vulnerabilidades encontradas, proceder a buscar parches de seguridad o correctivos para solucionar dichas vulnerabilidades, como se aprecia en la figura 73 donde se está realizando una búsqueda de algún parque para la Vulnerabilidad CVE2017-0143

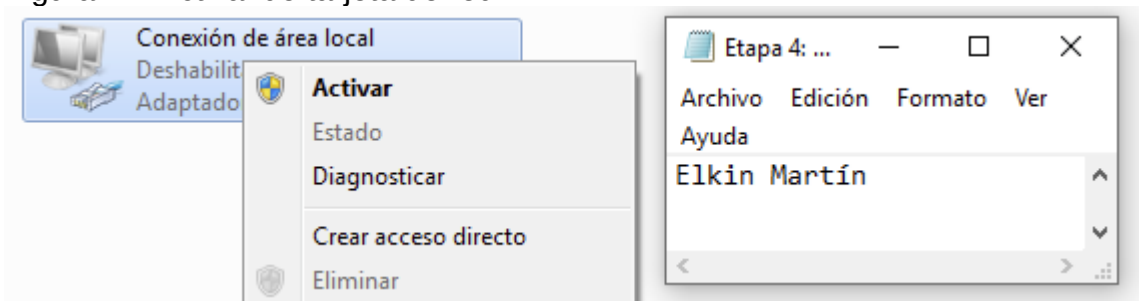
Figura 73. Buscando parche para CVE2017-0143



Fuente: autoría propia

- Una vez realizado el proceso, habilitar nuevamente la conexión LAN, como se aprecia en la figura 74.

Figura 74. Activando tarjeta de red

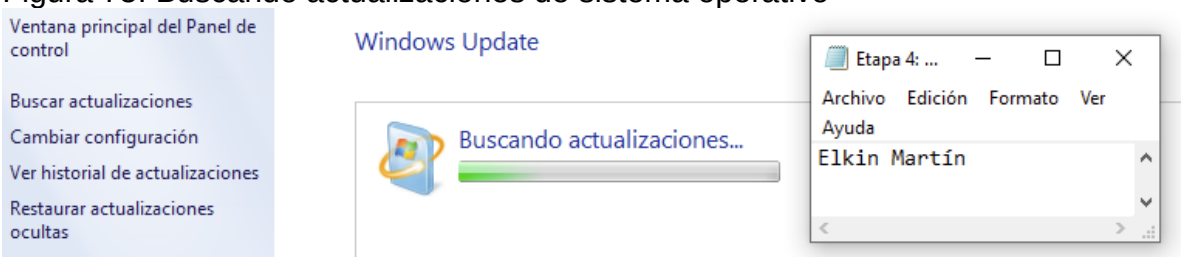


Fuente: autoría propia

- Instalar actualizaciones de seguridad de Windows

Para este proceso se puede realizar desde el Windows Update, como se aprecia en la figura 75.

Figura 75. Buscando actualizaciones de sistema operativo



Fuente: autoría propia

17 HARDENIZACIÓN E IMPLEMENTACIÓN DE ACCIONES FRENTE A UN ATAQUE INFORMÁTICO

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

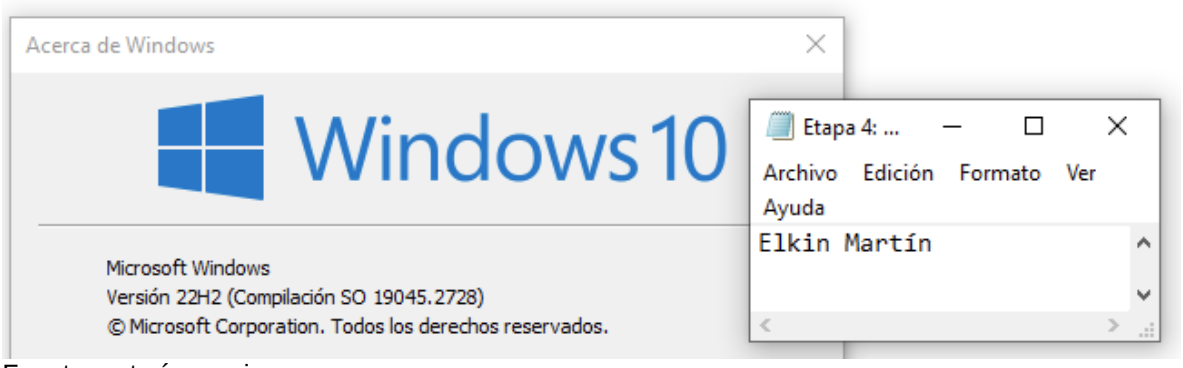
Analizando el ataque, sistema operativo y configuración, se asimila que varios computadores de la organización están en la misma situación, por tanto, se sugiere lo siguiente:

17.1 ACTUALIZACIÓN DE SISTEMA OPERATIVO

Actualizar todos sistema operativo de Windows 7, 8 y 8.1 a Windows 10 u 11 siempre y cuando el computador lo soporte, en caso contrario y si no hay recursos para un reemplazar el computador por uno nuevo o más reciente que si soporte un sistema operativo actual, entonces instalar todas las actualizaciones disponibles para el sistema operativo instalado.

La figura 76 muestra un sistema Windows 10 versión 22H2 actualizado

Figura 76. Sistema operativo actual



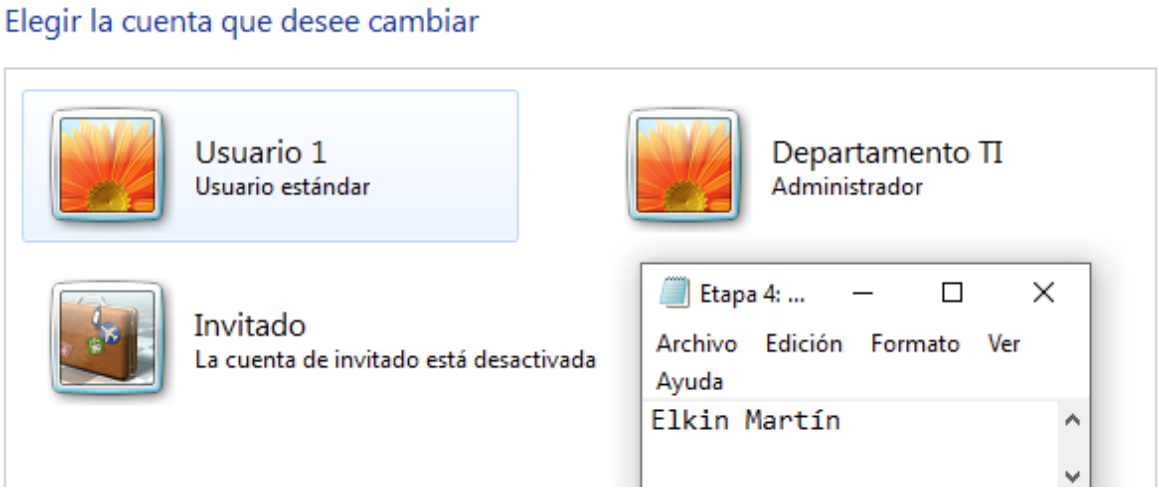
Fuente: autoría propia

17.2 CONFIGURACIÓN DE USUARIOS ADMINISTRADOR Y ESTÁNDAR

En el computador Windows 7-64 analizado se evidencia que solo cuenta con una sesión administradora para todos los usuarios, desde la cual cualquiera puede instalar aplicaciones sin restricciones, para evitar esto, se debe crear una sola sesión administradora con contraseña solo para el personal de TI y otras de tipo estándar de acuerdo al número de usuarios que se requiera para cada puesto de trabajo.

La figura 77 evidencia la creación de un usuario estándar y otro administrador para el departamento TI de la organización.

Figura 77. Configuración de usuarios



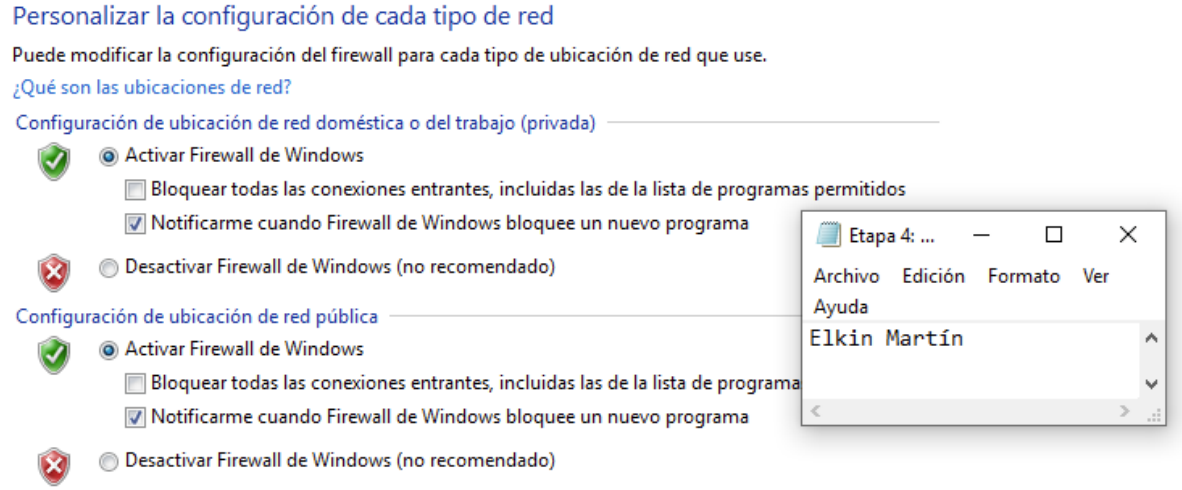
Fuente: autoría propia

17.3 CONFIGURACIÓN DE FIREWALL

Configurar de forma correcta el firewall, ya que al revisar el equipo se evidencio que tenía desactivado el firewall de Windows, como se apreciaba en la figura 5.

En la figura 78 se aprecia configurado de forma correcta el firewall de Windows 7-64.

Figura 78. Configuración correcta de firewall de Windows 7-64



Fuente: autoría propia

17.4 INSTALACIÓN DE SOFTWARE IDS/IPS

Se sugiere instalar software de tipo IDS/IPS, este tipo de software monitorea toda la red en busca de posibles intrusiones, los sistemas de tipo IDS (Sistema de Detección de Intrusiones), en caso de encontrar o detectar alguna intrusión generan una alerta con la cual el personal de TI va a verificar y tomas las medidas necesarias. En el caso de los sistemas de tipo IPS (Sistema de Prevención de Intrusiones) además generar una alerta, pueden bloquear dicha intrusión.

Para el caso de estudio se sugiere instalar cualquiera de las siguientes opciones IDS/IPS, las cuales son de código abierto.

- Snort: es una herramienta de código abierto, de tipo IDS la cual funciona "libpcap" que consiste en la captura de paquetes de biblioteca, y que son analizados con una seria de reglas que pueden ser implementadas de acuerdo a cada necesidad, adema este software permite el rastreo de paquetes [28].

- Suricata: es una herramienta de código abierto desarrollado por OSIF (Open Information Security Foundation) puede funcionar en modo IDS y en modo IPS, para su funcionamiento el software se basa en reglas que ya están predeterminadas para poder identificar cualquier tipo de malware y comportamientos sospechosos [29].

[28] PROTECCIONDATOS. Así es Snort, el sistema de detección de intrusos más popular, [Sitio WEB].[19, marzo 2023]. Disponible en: https://protecciondatos-lopd.com/empresas/snort-deteccion-intrusos/

[29] KEEPCODING. ¿Qué es Suricata en ciberseguridad?, [Sitio WEB].[19, marzo 2023]. Disponible en: https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

17.5 ALTERNATIVAS A HFS REJJETO PARA TRANSFERENCIA DE ARCHIVOS

Para el caso teórico de estudio se debe desinstalar la aplicación HFS Rejjeto, en caso de haber necesidad de compartir archivos, habilitar algún servicio de drive o nube, por ejemplo, Google Drive que en su versión gratuita puede alojar hasta 15 gigas de capacidad[30].

18 DIFERENCIA ENTRE EQUIPO BLUE TEAM Y EQUIPO DE RESPUESTA

¿Describa con sus palabras las diferencias entre un equipo Blue team y un equipo de respuesta a incidentes informáticos?

Lo primero es tener claro los conceptos del equipo Blue Team, equipo de respuesta a incidentes informáticos y luego si explicar la diferencia.

18.1 EQUIPO BLUE TEAM

Es un grupo conformado por profesionales en el área de la seguridad informática y tiene como propósito implementar medidas se seguridad en una red o infraestructura informática para evitar posibles ataques cibernéticos, intrusiones no autorizadas, daño por malware o robo de datos[31].

Para lograr esto el equipo de Blue team debe mantener los sistemas operativos actualizados, utilizar los últimos parches de seguridad, implementar la utilización de firewall, sistemas IPS/IDS y demás protocolos, buenas prácticas y todo lo necesario para evitar cualquier tipo de ataque.

De forma muy general, los equipos Blue team deben tener en cuenta lo siguiente:

- Tener claro toda la infraestructura informática, servidores, número de equipos, software, sistemas de seguridad.
- Identificar cuáles son los sistemas más críticos, como servidores o datos confidenciales.
- Identificar posibles riesgos e impacto de los mismos.
- Analizar posibles amenazas y vulnerabilidades

[30] GOOGLE. ¿Tienes preguntas sobre Google One? Nosotros tenemos las respuestas., [Sitio WEB].[19, marzo 2023]. Disponible en: https://one.google.com/faq/storage?hl=es_419

[31] SECUORA. Blue Team: el equipo que vela por la seguridad defensiva de tu empresa, [Sitio WEB].[19, marzo 2023]. Disponible en: https://secuora.es/blog/blue-team-el-equipo-que-vela-por-la-seguridad-defensiva-de-tu-empresa/

- Realizar un monitoreo constante de la red
- Implementar nuevas medidas de seguridad
- Tener un constante estudio sobre nuevas vulnerabilidades, ataques y demás riesgos informáticos.

18.2 EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

Estos equipos son conocidos como un CSIRT (Equipo de Respuesta frente a Incidencias de Seguridad Informática) en la práctica es un grupo de profesionales en seguridad informática, los cuales una vez se les informa acerca de un incidente informático, como un ciber ataque, robo de datos, caída de servidores por denegación de servicios entre otros, tiene como misión de controlar o mitigar dicha incidencia[32].

Los equipos CSIRT pueden ser parte de grandes organizaciones, universalidades o gobiernos entre otros.

En Colombia los principales CSIRT son:

- CSIRT Gobierno
https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/
- CSIRT Policía Nacional
https://cc-csirt.policia.gov.co/

- CSIRT Asobancaria
https://csirtasobancaria.com/

18.3 DIFERENCIA ENTRE EQUIPO BLUE TEAM Y EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

El equipo Blue team tiene la misión de prevenir un incidente o ataque informático y el equipo de respuesta frente a incidencias de seguridad informática (CSIRT) tiene la misión en caso de que ocurra el incidente o ataque, poder controlar o mitigar dicha situación[33].

---

[32] COMPUTERWEEKLY. Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT), [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.computerweekly.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informatica-CSIRT

[33] MANAGEENGINE. ¿Qué son los controles de CIS?, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

19 CIS “CENTER FOR INTERNET SECURITY” Y BLUE TEAM

¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS “Center For Internet Security” usted lo utilizaría para qué fin?

Primero se debe tener claridad de que es un CIS (Center For Internet Security) para luego ver la necesidad de implementarlo en un equipo Blue team.

19.1 CIS (CENTER FOR INTERNET SECURITY)

Es un conjunto de buenas prácticas relacionadas con la seguridad informática, que ayudan a tomar acciones para prevenir ataques cibernéticos de gran escala y peligrosidad.

En versiones anteriores existían 20 controles, pero la versión 8 establece 18 controles CIS, los cuales son[34]:

- Control CIS 1: Inventario y Control de Activos Empresariales: Son todos los dispositivos de hardware como computadores, portátiles, servidores, switch, router entre otros, para identificar si se conecta un dispositivo no autorizado.

- Control CIS 2: Inventario y Control de Activos de Software: Tanto sistemas operativos como aplicaciones, para identificar si se está ejecutando una aplicación no autorizada.
- Control CIS 3: Protección de datos: Desarrollar procesos y controles para el manejo seguro de la información y datos.

- Control CIS 4: Configuración segura de activos y software empresarial: Realizar configuraciones correctas de todos los dispositivos de la red para garantizar la seguridad de los mismos.

- Control CIS 5: Gestión de cuentas: Utilizar procesos y herramientas para la asignación y administración de las cuentas de usuario, tanto de administradores como de usuarios.

- Control CIS 6: Gestión de control de acceso: Utilizar procesos y herramientas para la asignación, administración y revocación de credenciales tanto de acceso, como de privilegios en usuarios y administradores.

[34] CISECURITY. The 18 CIS Critical Security Controls, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.cisecurity.org/controls/cis-controls-list

- Control CIS 7: Gestión continua de vulnerabilidades: Llevar un registro de todos los incidentes que podrían ayudar a prevenir posibles nuevos ataques.

- Control CIS 8: Gestión de registros de auditoría: Desarrollar planes para analizar y evaluar constantemente posibles vulnerabilidades dentro de la infraestructura.

- Control CIS 9: Protecciones de correo electrónico y navegador web: Aplicar medidas de seguridad para los correos electrónicos y los navegadores, ya que los atacantes se aprovechan de la ingeniería social para atacar a través de estos medios.

- Control CIS 10: Defensas contra malware: Evitar la instalación de malware y software dañino

- Control CIS 11: Recuperación de datos: Realizar copias de respaldo de todos los datos, y tener políticas claras para la recuperación en caso de un incidente.

- Control CIS 12: Gestión de infraestructura de red: Realizar una administración activa de todos los recursos de red, para buscar posibles vulnerabilidades y corregirlas.

- Control CIS 13: Supervisión y defensa de la red: Realizar un monitoreo constante de todos los recursos de red, para mantener un nivel se seguridad optimo en la misma.

- Control CIS 14: Concientización sobre seguridad y capacitación en habilidades: Capacitar a todo el personal de manera constante en temas se seguridad informática, para evitar posibles ataques, ya que el tema de la ingeniería social, es uno de los temas más críticos en cualquier infraestructura.

- Control CIS 15: Gestión de proveedores de servicios: Evaluar todos los proveedores de servicios que tienen información confidencial y critica de la empresa, para analizar si son confiables.

- Control CIS 16: Seguridad del software de aplicación: Administrar y verificar el ciclo de vida de todo el software para evitar y prevenir posibles vulnerabilidades que sean aprovechadas por los atacantes.

- Control CIS 17: Gestión de respuesta a incidentes: Establecer programas y políticas de respuesta frente a posibles incidentes, para poder responder al ataque de forma rápida y eficiente.

- Control CIS 18: Pruebas de penetración: Realizar pruebas de intrusión que simule un ataque real, tanto al personal, dispositivos y toda la infraestructura en general.

19.2 IMPLEMENTACIÓN DE UN CIS (CENTER FOR INTERNET SECURITY) EN UN EQUIPO BLUE TEAM

Teniendo en cuenta que el CIS (Center For Internet Security) es un conjunto de buenas prácticas que ayudan a fortalecer una infraestructura informática y que sus 18 controles son completamente aplicables a la misión que tiene un equipo Blue team, el cual es defensivo frente a posibles ataques, es conveniente y a la vez necesario aplicar este tipo de controles al equipo blue team, ya que como cualquier norma o estándar de seguridad, proporciona un paso a paso para ejercer las funciones de manera organizada y eficiente.

20 FUNCIONES DE UN SIEM

Explique y redacte las funciones y características principales de lo que es un SIEM.

20.1 DEFINICIÓN DE UN SISTEMA SIEM

Un SIEM (Security Information and Event Management) es una solución completa de seguridad que ayuda a la identificación y análisis de amenazas y vulnerabilidades y permite responder de manera rápida y precisa frente a cualquier incidente informático[35].

Para esto los sistemas SIEM deben tener un control total sobre la infraestructura, para poder realizar sus correctos procesos.

Los sistemas SIEM son la combinación de dos sistemas[36]:

- Security Information Management (SIM)
- Security Event Management (SEM)

SIM + SEM = SIEM

[35] MICROSOFT. ¿Qué es SIEM?, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

[36] GEEKFLARE. Las 11 mejores herramientas SIEM para proteger a su organización de ciberataques, [Sitio WEB].[19, marzo 2023]. Disponible en: https://geekflare.com/es/best-siem-solutions/

20.2 VENTAJAS DE UN SISTEMA SIEM

Los sistemas SIEM ofrecen muchas ventajas, dentro de las principales se pueden mencionar las siguientes[37]:

- Centralización de amenazas: los sistemas SIEM permiten tener un control centralizado de todas las posibles amenazas que puede tener la infraestructura.
- Evitar o minimizar las consecuencias de un ataque: Los sistemas SIEM realizan un permanente escaneo de todos los dispositivos de la infraestructura en busca posibles vulnerabilidades y riesgos, para poder prevenirlos o enfrentarlos de manera rápida.
- Capacidad de repuesta en tiempo real: Como los sistemas SIEM realizan un permanente monitoreo de toda la red, en caso de encontrar algún comportamiento anómalo, pueden actuar de inmediato para bloquear y contrarrestar el posible ataque.
- Crear base de incidentes: los sistemas SIEM permiten tener un registro de todos los incidentes que pueden ser utilizados en futuros ataques o incidentes informáticos.
- Reducción de costos: Debido al nivel de automatización que permite los sistemas SIEM permite que el personal de TI se encargue de otras labores, reduciendo costos en talento humano.

20.3 PRINCIPALES CARACTERISTICAS DE UN SIEM

Los SIEM se caracterizan por ofrecer una rápida respuesta frente a incidentes informáticos, para este es importante que un SIEM ofrezca las siguientes características[38].

- Capacidad de respuesta ante incidentes: Además del correcto análisis de vulnerabilidades, los sistemas SIEM debe proporcionar una rápida y efectiva respuesta ante cualquier incidente informático.

- Capacidad de automatización: para eliminar procesos manuales y programar tareas de seguridad y control.

- Escalabilidad: De acuerdo a la necesidad de la empresa poder implementar la solución adecuada y que pueda creer con la empresa según lo requiera.

---

[37] AMBIT-BST. ¿Qué significa SIEM y cómo funciona?, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

[38] GB-ADVISORS. 5 elementos que todo software de SIEM debe tener, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.gb-advisors.com/es/5-elementos-que-todo-software-de-siem-debe-tener/

- Cumplimento de estándares de seguridad: la solución SIEM debe poder cumplir con los diferentes estándares y regulaciones relacionadas con la seguridad informática.

- Monitoreo de infraestructura y nube: los sistemas SIEM no solo deben tener la capacidad de monitorear una infraestructura física, también debe contar con tecnologías para los nuevos estándares basados en la nube.

20.4 PRINCIPALES SOLUCIONES SIEM

Dentro de las principales soluciones SIEM se pueden destacar las siguientes[39]:

- Fusion SIEM
- Graylog
- IBM QRadar
- LogRhythm
- SolarWinds
- Splunk
- Elastic Security
- InsightsIDR
- Sumo Logic
- NetWitness
- AlienVault OSSIM

21 HERRAMIENTAS PARA CONTENER ATAQUES INFORMÁTICOS

Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

21.1 FIREWALL DE NUEVA GENERACIÓN (NGFW)

Los firewalls de nueva generación pueden realizar un proceso de inspección profunda de todos los paquetes, analizando las firmas de actividades dañinas, como también analizar amenazas persistentes, para prevenir posibles instrucciones,

[39] GEEKFLARE. Las 11 mejores herramientas SIEM para proteger a su organización de ciberataques, [Sitio WEB].[19, marzo 2023]. Disponible en: https://geekflare.com/es/best-siem-solutions/

analizar certificados SSL Y SSH, para lograr contener ataques a las capas del modelo OSI, además ofrecen un control de aplicaciones.[40]

21.2 IMPLEMENTACIÓN DE DMZ

Las DMZ (DeMilitarized Zone) o zonas desmilitarizadas permiten crear una configuración en la cual un determinado recurso como puede ser un servidor, va a tener libre acceso desde internet, pero a la vez esto genera una barrera para proteger los recursos internos de la infraestructura.[41]

21.3 SOLUCIÓNES DE IDS/IPS

Estas soluciones monitorean la red en busca de comportamientos anómalos o extraños, las soluciones IDS (Sistema de Detección de Intrusiones) pueden detectar un comportamiento extraño generar una seña de alerta al departamento de TI, y las soluciones IPS (Sistema de Prevención de Intrusiones), además de generar la alerta se pueden realizar bloqueos a dichas conexiones peligrosas.[42]

21.4 SOLUCIONES HONEYPOT

Se le conoce como “trampa dulce” y es un recurso que permite crear una infraestructura virtual paralela a la infraestructura real de la organización, con el objetivo de que, en caso de ataque, el ciber criminal crea que está atacando una infraestructura real, pero está en una falsa y supervisada, desde la cual se puede monitorear todo el comportamiento de ciber criminal para rastrearlo, analizar su tipo de ataque y tomar medidas preventivas para futuros ataques[43].

---

[40] CIBERSEGURIDADPYME, ¿qué es un Firewall de next-genereation?, [Sitio WEB].[20, marzo, 2023]. Disponible en: https://www.ciberseguridadpyme.es/aprende-ciberseguridad/formacion-basica-para-usuarios/que-es-un-firewall-de-next-generation/?cn-reloaded=1

[41] INCIBE, Qué es una DMZ y cómo te puede ayudar a proteger tu empresa, [Sitio WEB].[20, marzo, 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

[42] REDESZONE, Protege tu red con sistemas IDS/IPS y descubre cuáles son los mejores, [Sitio WEB].[20, marzo, 2023]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/sistemas-deteccion-prevencion-intrusiones-ids-ips/

[43] REDESZONE. Qué es y para qué sirve un Honeypot,[Sitio WEB].[20, marzo 2023]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/

CONCLUSIONES

- Como expertos en seguridad informática se debe conocer la normativa legal colombiana referente a delitos informáticos, protección de datos y buenas conductas profesionales, bien sea para asesorar casos de incidentes informáticos, como también realizar pruebas de intrusión dentro de la ley.

  Para delitos informáticos y protección de datos en Colombia existen dos leyes que enfocadas a esto, la primera es la ley 1273 de 2009 denominada “de la protección de la información y de los datos”, la cual tiene dos capítulos, el primero consta de ocho artículos, nombrados del 269A, hasta el 269H, de forma general castigan los accesos no autorizados, la obstaculización de un sistema, la intercepción de datos, el daño informático, el uso de malware y la violación de datos personales entre otros. y el segundo capítulo consta de dos artículos 269I y 269J, que mencionan otros atentados e infracciones informáticas. A excepción del articulo 269C, que tiene una pena de prisión de 36 a 72 meses, todas las demás tienen una pena de prisión de 48 a 96 meses y multas que van desde los 100 hasta los 1000 salarios mínimos legales vigentes.

  La segunda ley es la 1581 de 2012 se centra en la protección de los datos, que son almacenados en bases de datos.

  Además de esto, los expertos en seguridad informática deben tener en cuenta los reglamentos del código de ética COPNIA, los cuales establecen una serie de parámetros que todo profesional debe tener en cuenta para ejercer su profesión de una manera honesta, y profesional.

- Los equipos Red Team tienen la función de simular un ataque a una infraestructura informática, previamente se debe realizar un contrato de confidencialidad en el cual quede claro el alcance de la prueba, y se debe tener especial cuidado en no infringir alguna ley de protección de datos como la 1273 de 2009, por lo general se realiza cinco pasos generas para este tipo de pruebas que son:

  - ✓ Paso 1. Interacciones previas
  - ✓ Paso 2. Recolección de información
  - ✓ Paso 3. Análisis de vulnerabilidades
  - ✓ Paso 4. Explotación de vulnerabilidades
  - ✓ Paso 5. Informe

  Dentro de las herramientas utilizadas por el equipo Red Team se puede destacar herramientas como NMAP y los metasploit framework, entre otras muchas, todas

estas están en las distribuciones de Kali Linux, una distribución diseñada para los profesionales del pentesting, NMAP permite realizar un escaneo de puertos para buscar vulnerabilidades para luego ser aprovechadas con los metasploit framework.

- Los equipos Blue Team tienen la misión de defender una infraestructura informática, dentro de las principales herramientas que utiliza este equipo se pueden destacar la utilización de firewall, configuraciones de tipo DMZ (DeMilitarized Zone), soluciones IDS (Sistema de Detección de Intrusiones), soluciones IPS (Sistema de Prevención de Intrusiones) honeypot (tramas dulces), sistemas SIEM (Security Information and Event Management) estos últimos son una solución completa para el análisis de amenazas y vulnerabilidades. Además de la implementación de estas tecnologías, los equipos Blue Team pueden implementar normativas como la CIS (Center For Internet Security) que con sus 18 controles brindan una guía de buenas prácticas que ayudan a mejorar aún más los entornos de seguridad informática.

RECOMENDACIONES

Como ya se ha mencionado en varias ocasiones, lo más importante para una empresa u organización es la seguridad de los datos, por eso se debe tener buenos sistemas se seguridad para proteger la infraestructura informática, pero es importante tener en cuenta que cada empresa va a tener unos recursos diferentes, y en base a estos recursos el profesional en seguridad informática, deberá sugerir y trabajar con lo que la empresa disponga.

A continuación, se mencionan unas recomendaciones básicas que cualquier empresa puede aplicar y otras recomendaciones ideales para tener un buen sistema de seguridad informático.

Recomendaciones básicas

- Tener instalado la última versión de sistema operativo (siempre y cuando el hardware del pc lo permita)
- Todos los sistemas operativos deben estar actualizados (update activado)
- Se debe trabajar siempre con software legal (por temas legales y porque el uso de ckack y patch son una amenaza a la seguridad)
- Revisar que el antivirus y firewall estén activados y funcionando
- Los sistemas operativos deben contar con mínimo dos sesiones, una sesión administradora para el personal de TI con contraseña y otra para los usuarios
- Capacitación del personal a nivel de ingeniera social, que es una de las principales vulnerabilidades en cualquier infraestructura informática.

Adicional a estas recomendaciones básicas, dependiendo de los recursos y necesidades de cada empresa y se sugieren las siguientes recomendaciones.

Recomendaciones ideales

- Instalación de firewall perimetrales o de nueva generación (NGFW)
- Instalación de antivirus de tipo empresarial
- Instalación de soluciones IDS/IPS
- Instalación de soluciones EDR
- Configuración de zonas desmilitarizadas (DMZ)
- Configuración de sistemas Honeypot
- Implementación de servidores proxy
- Configuración de segmentación de red
- Realizar pruebas de intrusión para colocar a prueba los sistemas de seguridad
- Realizar pruebas de tipo Red Team y Blue Team o en su defecto de tipo Purple Team

LINK VIDEO DE SUSTENTACIÓN

https://youtu.be/TaC7CZ1GlQ0

BIBLIOGRAFÍA

AMBIT-BST. ¿Qué significa SIEM y cómo funciona?, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

CIBERSEGURIDAD. ¿Qué es CVE?. [Sitio WEB].[12, febrero, 2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

CIBERSEGURIDADBIDAIDEA. ¿Cuál son la 5 Fases del Pentesting?. [Sitio WEB].[10, febrero, 2023]. Disponible en: https://ciberseguridadbidaidea.com/fases-del-pentesting/

CIBERSEGURIDADPYME, ¿qué es un Firewall de next-genereation?, [Sitio WEB].[20, marzo 2023]. Disponible en: https://www.ciberseguridadpyme.es/aprende-ciberseguridad/formacion-basica-para-usuarios/que-es-un-firewall-de-next-generation/?cn-reloaded=1

CISECURITY. The 18 CIS Critical Security Controls, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.cisecurity.org/controls/cis-controls-list

COMPUTERWEEKLY. Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT), [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.computerweekly.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informatica-CSIRT

COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares., [Sitio WEB].[18, febrero, 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

CVE. CVE-2007-6750, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750

CVE. CVE-2011-3192, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2011-3192

CVE. CVE-2017-0143, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

ELHACKER, Manual y chuleta de comandos con Nmap, [Sitio WEB].[07, marzo, 2023]. Disponible en: https://blog.elhacker.net/2021/10/chuleta-comandos-nmap-opciones-nse.html

ENTER.CO. Detrás de Buggly: la historia de la fachada Andrómeda, [Sitio WEB].[20, febrero, 2023]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

FUNCIONPUBLICA. LEY ESTATUTARIA 1581 DE 2012. [Sitio WEB].[09, febrero, 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

GB-ADVISORS. 5 elementos que todo software de SIEM debe tener, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.gb-advisors.com/es/5-elementos-que-todo-software-de-siem-debe-tener/

GEEKFLARE. Las 11 mejores herramientas SIEM para proteger a su organización de ciberataques, [Sitio WEB].[19, marzo 2023]. Disponible en: https://geekflare.com/es/best-siem-solutions/

GOOGLE. ¿Tienes preguntas sobre Google One? Nosotros tenemos las respuestas., [Sitio WEB].[19, marzo 2023]. Disponible en: https://one.google.com/faq/storage?hl=es_419

IMSALUD. ABC Ley 1581 de 2012 Protección de Datos Personales. [Sitio WEB].[09, febrero, 2023]. Disponible en: https://www.imsalud.gov.co/web/sin-categoria/abc-ley-1581-de-2012-proteccion-de-datos-personales/

INCIBE, Qué es una DMZ y cómo te puede ayudar a proteger tu empresa, [Sitio WEB].[20, marzo 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

JCTSOLUCIONES, uso de los comandos net user y net localgroup, [Sitio WEB].[09, marzo, 2023]. Disponible en: https://www.jctsoluciones.com.co/uso-de-los-comandos-net-user-y-net-localgroup/

KEEPCODING, ¿Qué es Metasploit?, [Sitio WEB].[07, marzo, 2023]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

KEEPCODING. ¿Qué es ExploitDB?. [Sitio WEB].[12, febrero, 2023]. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/#Que_es_ExploitDB

KEEPCODING. ¿Qué es Suricata en ciberseguridad?, [Sitio WEB].[19, marzo 2023]. Disponible en: https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

MANAGEENGINE. ¿Qué son los controles de CIS?, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

MICROSOFT. ¿Qué es SIEM?, [Sitio WEB].[19, marzo 2023]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

NMAP, Guía de referencia de Nmap (Página de manual), [Sitio WEB].[07, marzo, 2023]. Disponible en: https://nmap.org/man/es/index.html

OPENWEBINARS. Para qué sirve OpenVAS. Sitio WEB].[11, febrero, 2023 https://openwebinars.net/blog/que-es-openvas/

OPTICAL, Ataques informáticos: Causas, Tipos, Consecuencias y Prevenciones, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/

PENTESTER ACADEMY TV, Basic Exploitation with Metasploit: Windows: HTTP File Server, [Sitio WEB].[05, marzo, 2023]. Disponible en: https://www.youtube.com/watch?v=YQUcyQ4WT6w

PROTECCIONDATOS. Así es Snort, el sistema de detección de intrusos más popular, [Sitio WEB].[19, marzo 2023]. Disponible en: https://protecciondatos-lopd.com/empresas/snort-deteccion-intrusos/

REDESZONE, Protege tu red con sistemas IDS/IPS y descubre cuáles son los mejores, [Sitio WEB].[20, marzo 2023]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/sistemas-deteccion-prevencion-intrusiones-ids-ips/

REDESZONE. Qué es y para qué sirve un Honeypot,[Sitio WEB].[20, marzo 2023]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/
REJETTO. Description, [Sitio WEB].[07, marzo, 2023]. Disponible en: https://www.rejetto.com/hfs/

SECRETARIASENADO. LEY 1273 DE 2009, [Sitio WEB].[18, febrero, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SECRETARIASENADO. LEY 1273 DE 2009. [Sitio WEB].[08, febrero, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SECUORA. Blue Team: el equipo que vela por la seguridad defensiva de tu empresa, [Sitio WEB].[19, marzo 2023]. Disponible en: https://secuora.es/blog/blue-team-el-equipo-que-vela-por-la-seguridad-defensiva-de-tu-empresa/

VIEWNEXT. Las 8 herramientas imprescindibles de pentesting [Sitio WEB].[11, febrero, 2023]. Disponible en: https://www.viewnext.com/8-herramientas-imprescindibles-pentesting/

VIEWNEXT. Las 8 herramientas imprescindibles de pentesting [Sitio WEB].[Sitio WEB].[11, febrero, 2023]. Disponible en: https://www.viewnext.com/8-herramientas-imprescindibles-pentesting/

WIDROGO, Metasploit Introduccion: Lo que necesitas saber de Metasploit, [Sitio WEB].[08, marzo, 2023]. Disponible en: https://widrogo.wordpress.com/tag/msfconsole/