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

JORGE LUIS VILLEGAS MAGUIÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
SAN JUAN DE PASTO
2023

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

JORGE LUIS VILLEGAS MAGUIÑA

DOCUMENTO DE GRADO DEL SEMINARIO ESPECIALIZADO: “EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM”

TUTOR: JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
SAN JUAN DE PASTO
2023

CONTENIDO

LISTA DE FIGURAS

RESUMEN

El presente documento es un informe técnico describe de forma técnica el desarrollo de 5 etapas de una situación planteada en una organización, en donde se hace necesario realizar por parte del equipo de seguridad Red Team & Blue Team, una serie de actividades y estrategias para encontrar la solución de un problema y falla de seguridad al interior de la organización. El presente informe se resume en las siguientes etapas

ETAPA 1: CONCEPTOS EQUIPOS DE SEGURIDAD
En esta etapa se realiza la identificación, análisis y configuración del banco de trabajo basado en el problema de seguridad planteado por la organización

ETAPA 2: ACTUACIÓN ÉTICA Y LEGAL
En esta etapa se realiza la identificación del problema teniendo en cuenta los temas éticos y legales aplicables al escenario planteado por la organización.

ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN
En esta etapa se realiza la aplicación de pruebas prácticas de intrusión(Pentesting), realizadas por el equipo.

ETAPA 4: CONTENCIÓN DE ATAQUES INFORMÁTICOS
En esta etapa se realiza la contención del ataque informático develado por el equipo Red Team & Blue Team, en donde se hace todo lo posible y necesario para la contención y corrección de vulnerabilidades del sistema.

ETAPA 5: SOCIALIZACIÓN DE INFORME TÉCNICO
En esta epata se presenta el informe final con toda la información relevante a las etapas anteriores, incluyendo conclusiones y recomendaciones para la organización

GLOSARIO

DELITO INFORMATICO: El delito informático es toda acción ilegal que se realiza en el entorno digital.

DATOS PERSONALES: Los datos personales s||on toda aquella información de una persona, organizada por datos privados, semiprivados y públicos, que contienen información como datos físicos, creencias religiosas, historial médico, laboral, educativo entre otros.

MAQUINA VIRTUAL: Una máquina virtual es la Isolación de recursos de hardware y software de un servidor y/o computador en fracciones que se recrean dentro un sistema completamente independiente capaz de ejecutar otro sistema operativo y aplicaciones independientes al servidor que lo contiene.

PENTESTING: Es un método práctico de pruebas de seguridad, a través del cual se intenta vulnerar los sistemas, redes, equipos, aplicaciones para comprobar el nivel de seguridad y protección de estos.

VIRTUALBOX: Es un software de virtualización creado para las arquitecturas x86/amd64, desarrollado por la compañía Oracle Corporation.

ATAQUE INFORMATICO: Un ataque informático es el intento de la vulneración de un sistema, equipo, red, aplicación, que consiste en aprovechar algún hueco de seguridad y/o vulnerabilidad, principalmente con el fin de obtener algún tipo de beneficio, que suele ser principalmente económico

METERPRETER: Meterpreter es una aplicación que permite realizar y ejecutar tareas de forma remota en una máquina, siendo un software que se ejecuta en un nivel bajo de la máquina, siendo muy difícil de detectar.

PAYLOAD: Es una aplicación que realiza la carga que se ejecuta en una vulnerabilidad encontrada en un sistema.

SIEM: SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es una categoría de software, la cual establece como objetivo entregar información y datos útiles sobre las potenciales amenazas de seguridad, en sus redes críticas, a través de la técnica de estandarización de datos y priorización de amenazas.

INCIDENTE DE SEGURIDAD: Un incidente de seguridad es la materialización de un riesgo, el cual ocurre cuando se juntan una amenaza y una vulnerabilidad del sistema.

CONTENCION DE ATAQUES: Es la aplicación de una serie de medidas y estrategias de software y hardware que permiten contener ataques en tiempo real de un sistema, aplicación, red, servidor.

DETECCION DE ATAQUES: Es la aplicación de un software o hardware que permite la detección de malware, virus y posibles ataques a un sistema, aplicación, red, servidor.

SHELL: Es una interfaz de comunicación entre el usuario y el sistema operativo, que generalmente cuenta con una serie de comandos definidos para su comunicación.

PUERTA TRASERA: Backdoor o puerta trasera se le conoce a la entrada secreta a los sistemas y/o dispositivos, que se usan generalmente con fines maliciosos para acceder a los sistemas y tomar control sobre ellos.

1. INTRODUCCIÓN

Ante el continuo crecimiento de la tecnología, se plantean verdaderos retos por parte de los equipos de seguridad de la empresas, dado que el crecimiento exponencial de los delitos informáticos y los ataques a todo tipo de sistemas informáticos es un dolor de cabeza para todas las empresas, se hace necesario establecer equipos de trabajo enfocados a la seguridad perimetral de las empresas, estos equipos de trabajo deben estar constantemente actualizados y dedicados a realizar pruebas de seguridad y monitoreo constate de los sistemas, siendo esto un verdadero reto, ante el continuo cambio de la tecnología y la masificación de las comunicaciones y el acceso a internet.

La seguridad hoy en día se torna en el pilar fundamental de todas entidades que valoran verdaderamente su información, por ende necesitará todas las ayudas y estrategias que le permitan estar al día y a la vanguardia de los avances tecnológicos, siendo en este punto donde los equipos Red Team & Blue Team, se vuelven en un pieza fundamental del engranaje que va fortalecer la seguridad, siendo entonces fundamental tanto para las entidades y empresas estar al día y alineados con las regulaciones éticas y legales a nivel nacional e internacional, para no trasgredir y pasar los límites del Hackin Ético.

Somos conscientes que la defensa de la ciberseguridad se debe dar en todos los frentes y es por eso que hoy en día existen grupos dedicados a combatir la ciberdelincuencia, y gracias al trabajo en conjunto hoy se tienen muchas herramientas y aplicaciones que nos permiten simular escenarios de prueba, que nos permitan a toda la comunidad informática aprender y dar pasos positivos, además de aunar esfuerzos en un mundo tecnológico que crece día a día a pasos agigantados, en pro de la seguridad informática, por tanto como parte fundamental interesada nos corresponde el estudio constante y el aprendizaje de nuevas técnicas, el uso y desarrollo de nuevos métodos y la actualización permanente, de tal forma que en el momento que nos toque, podamos dar lo mejor del conocimiento y experiencia.

El constante avance tecnológico es una premisa que toda empresa tiene en sus objetivos de crecimiento, ya que se ha convertido en una estrategia fundamental a la hora de marcar la diferencia, al tener sus procesos optimizados, sin embargo el uso de nuevas tecnologías, y herramientas tecnológicas no supervisadas y revisadas por un adecuado equipo de seguridad, los pone en peligro y riesgo constante con vulnerabilidades que pueden ser detectadas y utilizadas por

atacantes malintencionados, generando graves consecuencias y un impacto desastroso para las empresas por las pérdidas económicas y de información que se puedan generar.

Es así como se hace necesario para todas las empresas contar con equipos de seguridad como los equipos Blue Team & Red Teams, que puedan apoyar de forma preventiva y correctiva cualquier situación de seguridad que se pueda presentar en las empresas y organizaciones

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Evaluar las estrategias y acciones de los equipos Red Team & Blue Team, que hacen parte de una organización, en el marco de los criterios éticos y legales, demostrando técnicamente las vulnerabilidades y debilidades en un sistema informático, a partir del uso de metodologías y técnicas de intrusión, para así poder formular estrategias optimas y efectivas de contención mediante el análisis de los riesgos y las vulnerabilidades en una infraestructura de Tecnologías de la Información.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar el análisis de la legislación relacionada con delitos informáticos.
- Realizar el análisis sobre el ejercicio de Pentesting.
- Realizar la explicación de las herramientas y servicios utilizados en la ciberseguridad.
- Evidenciar la implementación de un “banco de trabajo” en un entorno local para realizar el Pentesting
- Brindar una guía para la identificación de un problema específico en temas éticos y legales
- Analizar un problema ético legal en un acuerdo de confidencialidad
- Utilizar herramientas y procedimientos para dar solución al escenario propuesto de acuerdo con los pasos del Pentesting.
- Análisis del problema de seguridad que permita dar solución al fallo identificado al interior de una organización.
- Usar herramientas de seguridad para dar identificar fallos en el escenario propuesto.
- Analizar el ataque del escenario propuesto y realizar la explotación de vulnerabilidades en el escenario propuesto.
- Evidenciar de forma práctica la explotación de la vulnerabilidad identificada
- Analizar y plantear acciones necesarias para contener un ataque en tiempo real.
- Realizar el informe de acciones de Hardening a implementar para poder evitar que sucedan ataques de seguridad informática.
- Analizar las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos

- Análisis sobre la pertinencia de trabajar con CIS “Center For Internet Security” como propuesta de aseguramiento por parte de un equipo de Blue Team.
- Análisis sobre las funciones y características principales de un SIEM.
- Informe de elección de 3 herramientas que permitan contener ataques informáticos.
- Formular Aspectos que aporten al desarrollo de estrategias de RedTeam &
- BlueTeam.
- Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización.
- Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

3. CONCEPTOS EQUIPOS DE SEGURIDAD

3.1 ANÁLISIS DE LA LEGISLACIÓN RELACIONADA CON DELITOS INFORMÁTICOS

3.1.1 DELITOS INFORMATICOS EN COLOMBIA

En Colombia se cuenta con la Ley 1273 del 2009, ley orientada a la protección de la información digital, "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"[1], que comprende un capítulo dedicado lo los delitos que se incurran en atentados contra la integridad, confidencialidad y disponibilidad de la información y un segundo capítulo que se incurran en atentados informáticos y otras infracciones, de tal forma que a partir de la promulgación de la Ley, se comienza a penalizar los delitos informáticos con sanciones privativas de la libertad que van desde los 36 meses hasta los 120 meses y con sanciones económicas que van desde los 100 a 1.500 salarios mínimos legales mensuales vigentes, teniendo además una situación de agravación de la pena que va desde la tercera a la mitad cuando los delitos se cometieren en situaciones particulares como podrían ser delitos cometidos en redes y sistemas del sector público, servidores públicos, fines de terrorismo entre otros.

3.1.2 PROTECCION DE DATOS PERSONALES

En Colombia se cuenta con la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”[2], para dar los lineamientos y directrices orientadas a la protección de los datos personales, ley que se promulga para ser aplicada en todas las entidades públicas y privadas que recopilen datos personales de los ciudadanos, permitiendo así a la ciudadanía poder conocer, actualizar, rectificar y de ser necesario también autorizar el uso de estos datos, como un derecho fundamental, que debe se debe respetar y cumplir, garantizando así también el acceso y/o restricción a la información y a la transparencia de la misma en el momento que se requiera.

3.2 FASES DEL PENTESTING

Hoy en día los ataques informáticos son una constante diaria y un verdadero problema para todos, sin embargo pese a las constantes noticias de ataques informáticos, aún muchas de la empresas privadas y públicas no han tomado conciencia de la importancia de proteger

[1] SIC. (2009). Ley 1273 de 2009 (pp. 1) Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
[2] FUNCION PUBLICA. Ley 1581 de 2012 (pp. 1) Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

los datos y su información, sin embargo ese número de empresas y entidades va creciendo día a día, para lo cual una de las principales actividades es realizar Hacking Ético, que consiste en realizar pruebas de seguridad conocidas como Pentesting de Seguridad, que se realiza a los sistemas informáticos con los que se cuenta, estas pruebas de seguridad se pueden realizar siguiendo metodologías que guían y orientan la ejecución y documentación de las mismas. Entre las metodologías más usadas podemos encontrar: Open Source Security Testing Methodology Manual- OSSTMM, Open Web Application Security Project – OWASP, Information Systems Security Assement Framework – ISSAF,
En el presente trabajo se describe de forma general las etapas de las pruebas de penetración basadas en el Hacking Ético siguiendo la guía técnica de la NIST SP 800-115, en la que encontramos 4 etapas:

3.2.1 PLANEACIÓN

En esta fase de la prueba de penetración se realiza la definición y limitación del alcance y los escenarios de la prueba, se defines los grupos y equipo de trabajo, además se realizan los acuerdos de privacidad y confidencialidad, basados en los aspectos legales y normativos que puedan aplicar y regir la ejecución de la prueba de penetración planeada.

En esta fase no se aplica ningún ejercicio que requiera una herramienta o aplicación de seguridad.

3.2.2 DESCUBRIMIENTO

La fase de descubrimiento consiste en obtener la mayor cantidad de información posible del objetivo a atacar, en esta etapa se realiza a través de la recolección y el escaneo de información y búsqueda de vulnerabilidades, para ello se pueden usar por ejemplo diferentes técnicas como puede ser la Ingeniería social, que consiste en obtener información y datos sensibles a través del engaño y suplantación de identidad a los usuarios con métodos como el Phishing, Visghing Smishing, entre otros, herramientas como por ejemplo Nmap que sirve para el escaneo y rastreo de puertos abiertos en los sistemas informáticos, de tal forma que se pueda identificar puertos y servicios abiertos para pasar a una etapa final de descubrimiento en busca de vulnerabilidades del sistema, para lo cual se puede usar la herramienta Nessus, que permite realizar una análisis profundo de vulnerabilidades de diversos sistemas operativos. La Fase de descubrimiento es una fase de vital importancia para realizar una prueba de penetración exitosa.

3.2.3 ATAQUE

En esta fase se realiza el ataque y vulneración de los sistemas informáticos, en esta etapa se evidencia que tan efectivas fueron las fases de Planeación y Descubrimiento, en esta etapa también es posible que se pueda generar un loopback para retroalimentar la fase de

Descubrimiento, con el objetivo de plantear un nuevo ataque probablemente más efectivo. El ataque busca como objetivos primordiales el acceso y elevación de privilegios en el sistema informático, de tal forma que en el primero objetivo realizará la aplicación o ejecución de un Exploit, el cual es un software informático que aprovecha la vulnerabilidad del sistema para ingresar al sistema, esta etapa podrá requiere de un experto con conocimiento en lenguajes de programación para utilizar un Exploit que puede ser conseguido desde internet o construir uno en base a las vulnerabilidades detectadas; y el segundo objetivo será finalmente la elevación de privilegios para tomar control total de administración sobre el sistema atacado.

3.2.4 REPORTE

La fase de reporte consiste en entregar un informe ejecutivo de tallado con todas las actividades y pruebas realizadas, las vulnerabilidades encontradas, los riesgos y las recomendaciones para ser aplicadas con el objetivo de corregir las debilidades, brechas de seguridad y minimización de riesgos de los sistemas informáticos.

El reporte debe ser realizado y preparado en un lenguaje que la alta gerencia pueda comprender, para así tomar las decisiones más acertadas.

3.3 HERRAMIENTAS DE CIBERSEGURIDAD

3.3.1 HERRAMIENTAS

3.3.1.1 METASPLOIT

Metasploit es un programa de seguridad, que contiene un Framework de código abierto muy usado en las pruebas de penetración, cuenta con una amplia gama de Exploits que permite realizar Pentesting confiables gracias a su amplia comunidad que brinda constantes actualizaciones. Metasploit además puede ser usada en todas las fases del Pentesting, dado que cuenta con opciones para escanear puertos y vulnerabilidades, elevación de privilegios, entre otras muchas ventajas.

3.3.1.2 NMAP

Nmap es un programa de seguridad, de código abierto que permite realizar escaneo de puertos, redes y dispositivos conectados a la red, con el objetivo de obtener información de los dispositivos, ver que puertos y servicios están habilitados y encontrar vulnerabilidades.

3.3.1.3 OPENVAS

OpenVas es un programa de código abierto que permite realizar escaneo multiplataforma de vulnerabilidades en los sistemas informáticos, la herramienta cuenta con una amplia base de datos de vulnerabilidades conocidas y crece día a día con el apoyo de la comunidad. OpenVas es una herramienta fundamental en toda prueba de penetración de seguridad.

3.3.2 SERVICIOS EN LINEA

3.3.2.1 EXPLOITDB

ExploitDB es un servicio web en línea que recopila bases de datos públicas con Exploits para vulnerabilidades conocidas, de tal forma que dichos Exploits se pueden descargar y utilizar en las pruebas de penetración. Las bases de datos de ExploitDB crecen continuamente gracias a la inmensa comunidad que la alimenta.

3.3.2.2 CVE

El CVE o Common Vulnerabilities and Exposures, es un código único que permite la identificación de las vulnerabilidades y exposiciones comunes, cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, con el objetivo de documentar y llevar uns base de datos que permita identificar las vulnerabilidades.

3.4 BANCO DE TRABAJO

Para armar el banco de trabajo se requiere de la instalación de Virtualbox para Windows, de tal forma que se pueda construir un escenario de pruebas local de acuerdo con la guía práctica y escenario.

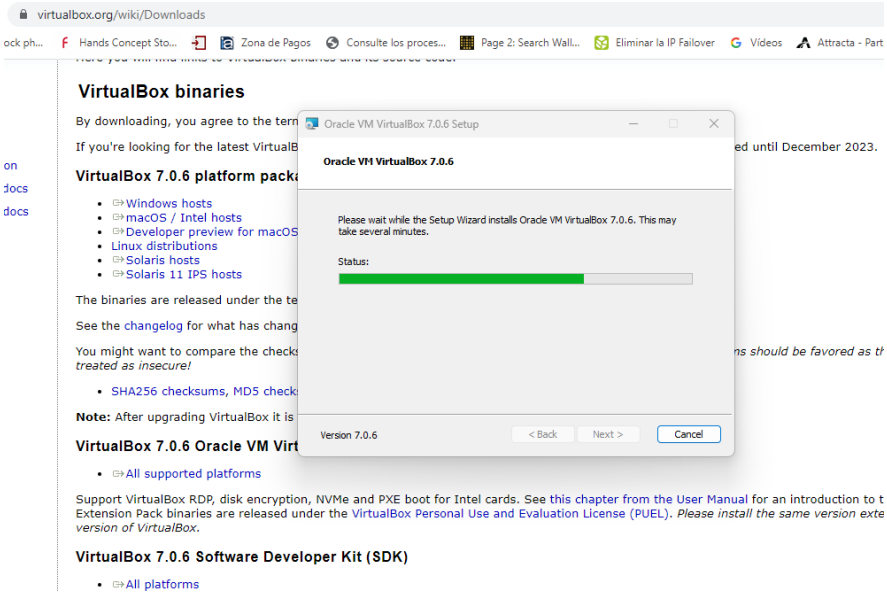
3.4.1 DESCARGA DE VIRTUALBOX

De acuerdo con lo anterior, se procede a realizar la descarga de VirtualBox del sitio oficial: https://www.virtualbox.org/wiki/Downloads la versión para sistemas Windows

Figura 1. Descarga de VirtualBox

Fuente: Elaboración propia

Figura 2. Instalación VirtualBox

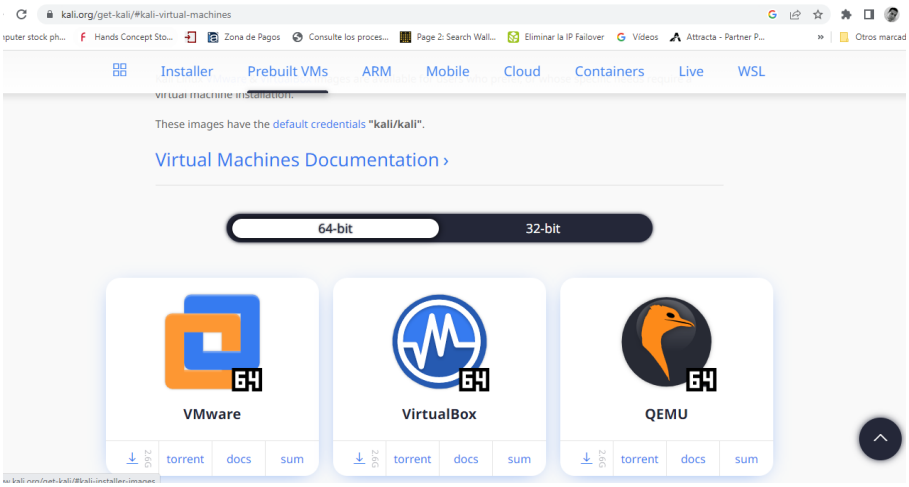


Fuente: Elaboración propia

3.4.2 DESCARGA DE KALI LINUX

Se realiza la descarga de Kali Linux para Virtualbox preconfigurado desde https://www.kali.org/get-kali/#kali-virtual-machines

Figura 3. Descarga de Máquina Virtual Kali Linux Preconfigurada

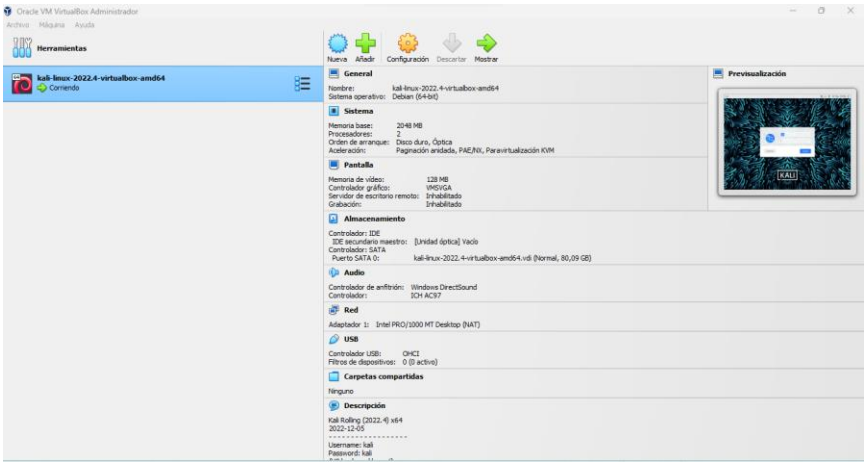


Fuente: Elaboración propia

3.4.3 MONTAJE KALILINUX EN VIRTUALBOX

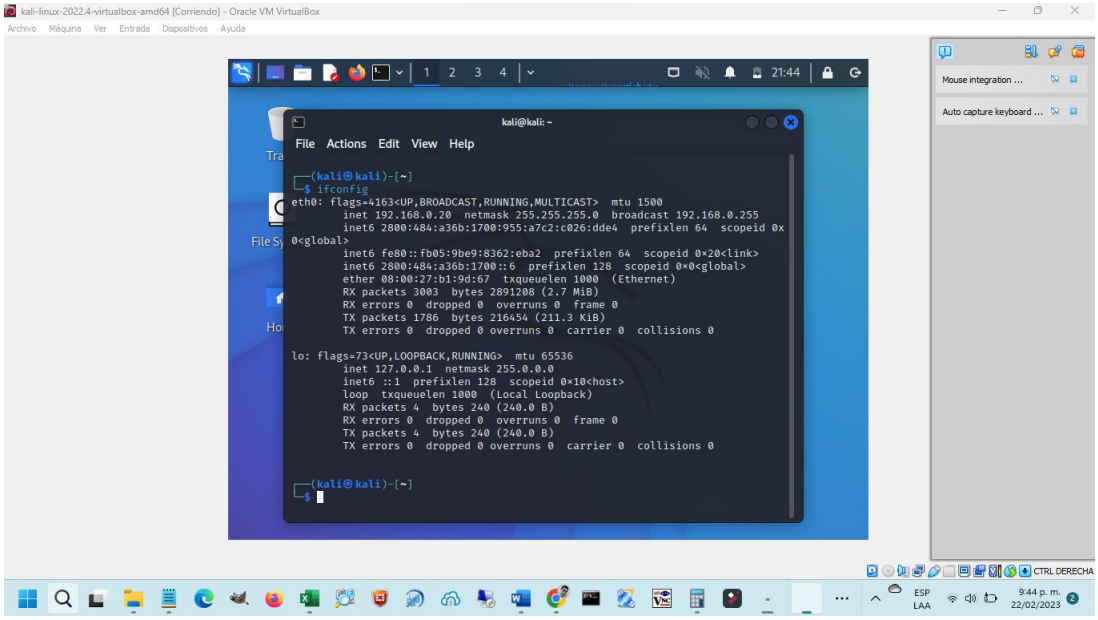
Montamos la máquina virtual preconfigurada de Kali en VirtualBox, e iniciamos la VPS. El usuario por defecto es kali y la contraseña kali para nuestro banco de trabajo.

Figura 4. Montaje de la Máquina Virtual de Kali Linux



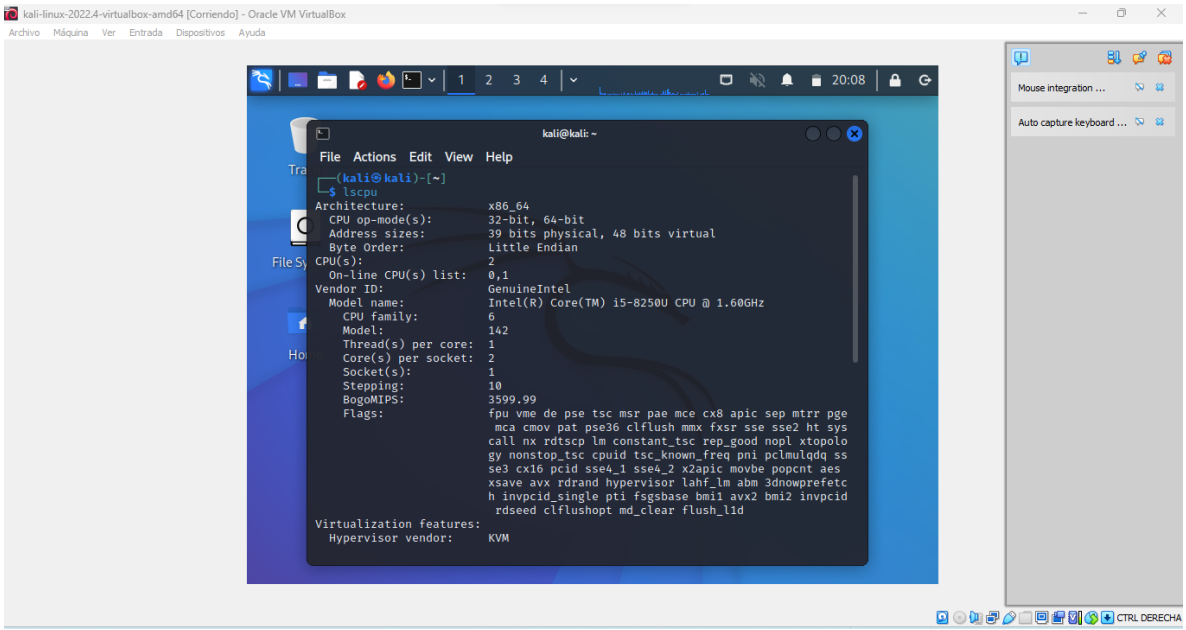
Fuente: Elaboración propia

Figura 5. Configuración de Red de la máquina virtual Kali Linux dentro del mismo segmento con IP: 192.168.0.20



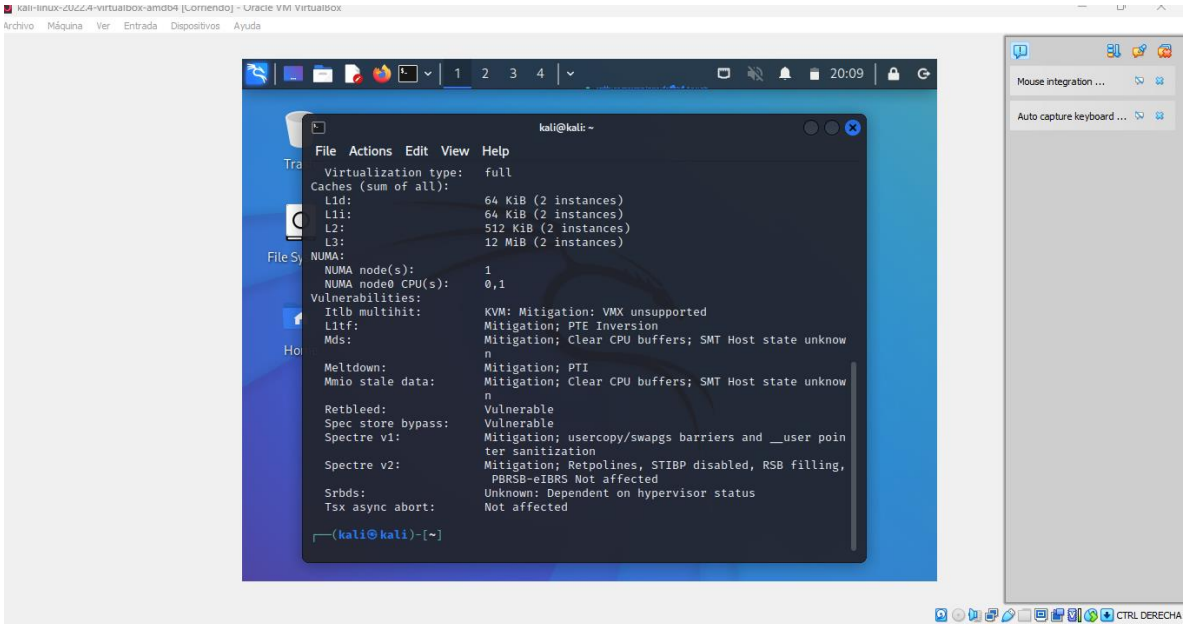
Fuente: Elaboración propia

Figura 6. Configuración de Hardware con el comando lscpu de la máquina virtual



Fuente: Elaboración propia

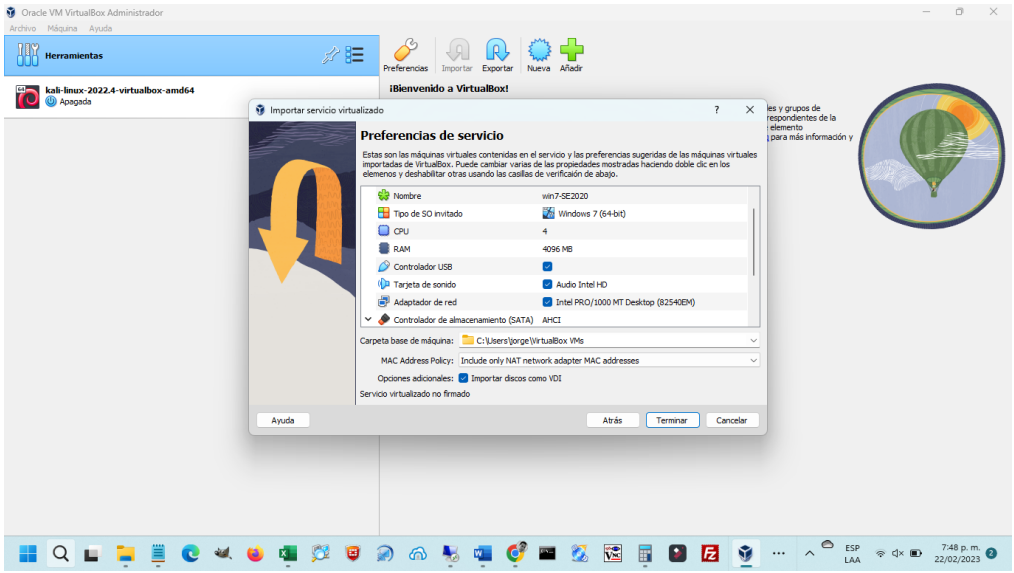
Figura 7. Continuación configuración de Hardware con el comando LSCPU de la máquina virtual



Fuente: Elaboración propia

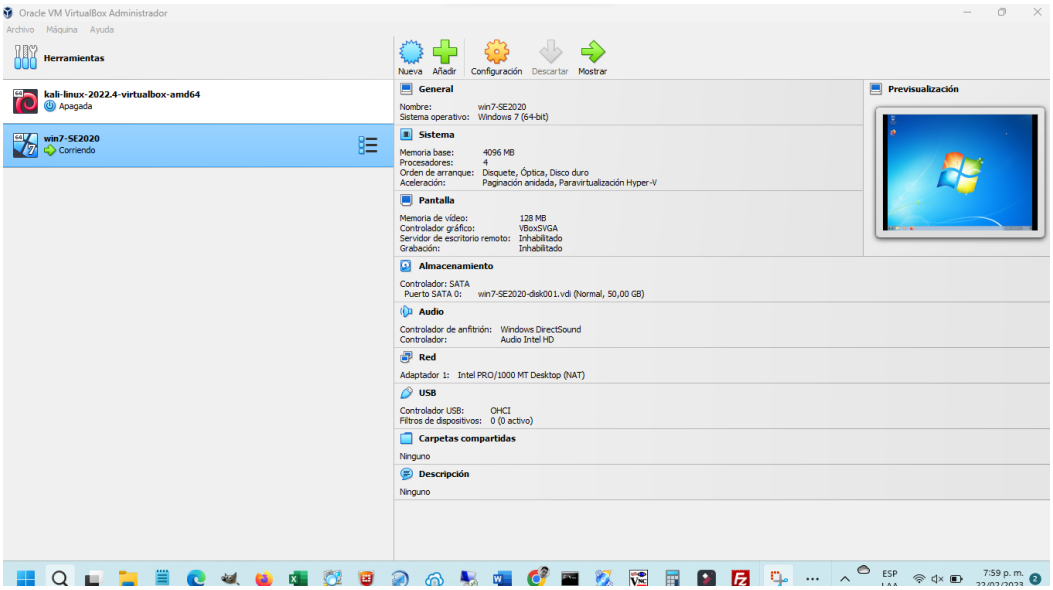
3.4.4 MONTAJE WINDOWS 7 A 32 BITS EN VIRTUALBOX

Figura 8. Se procede a importar las imágenes OVA de Windows 7 a 32 bits



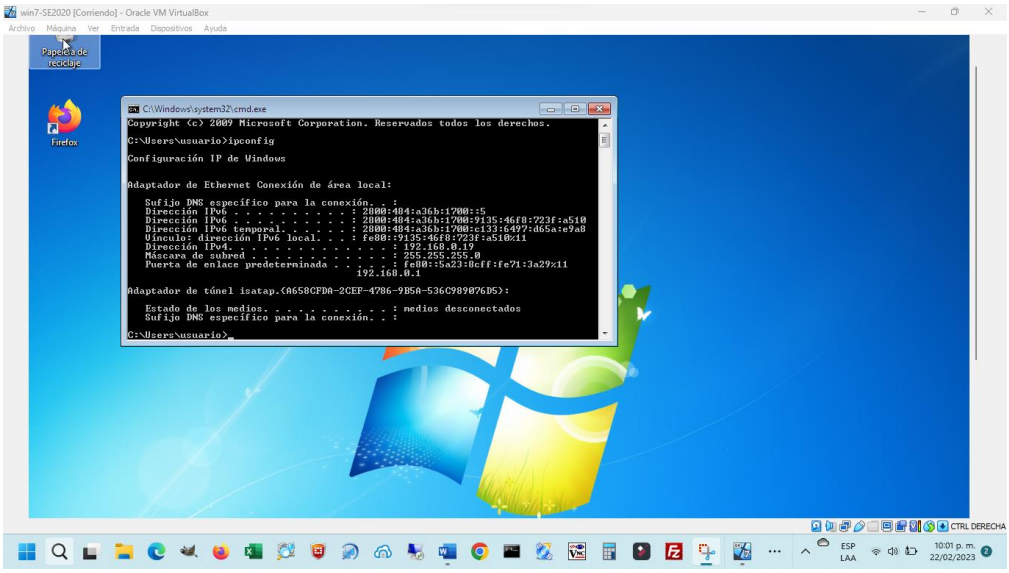
Fuente: Elaboración propia

Figura 9. Se procede a configurar los parámetros del sistema e iniciar la máquina virtual



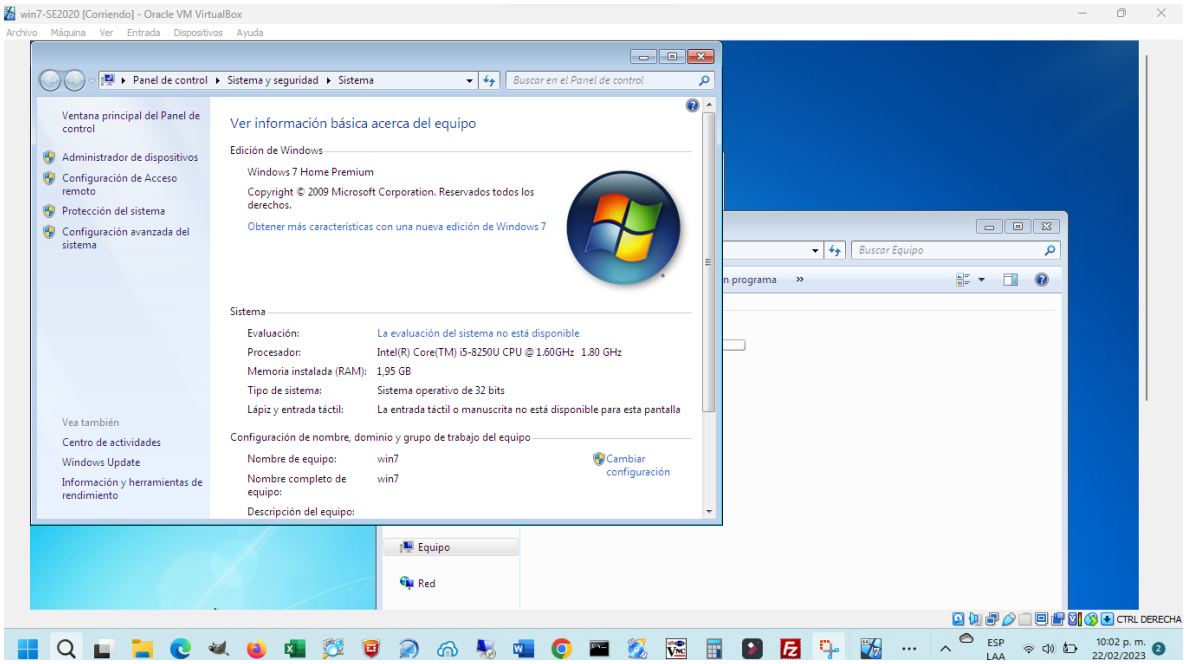
Fuente: Elaboración propia

Figura 10. Configuración de red dentro del mismo segmento con IP: 192.168.0.19



Fuente: Elaboración propia

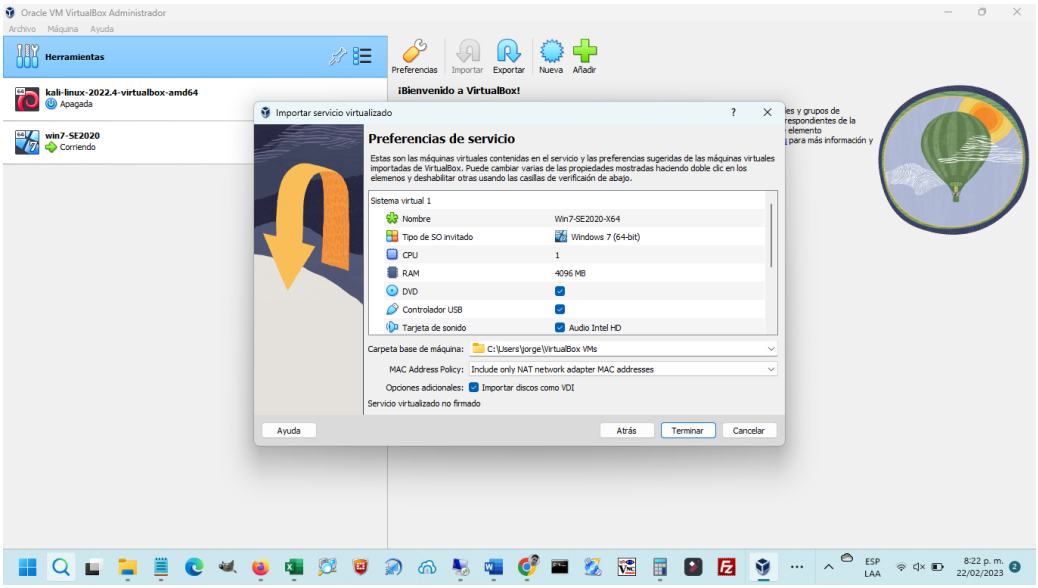
Figura 11. Configuración y hardware de la máquina con Windows 7 a 32 bits



Fuente: Elaboración propia

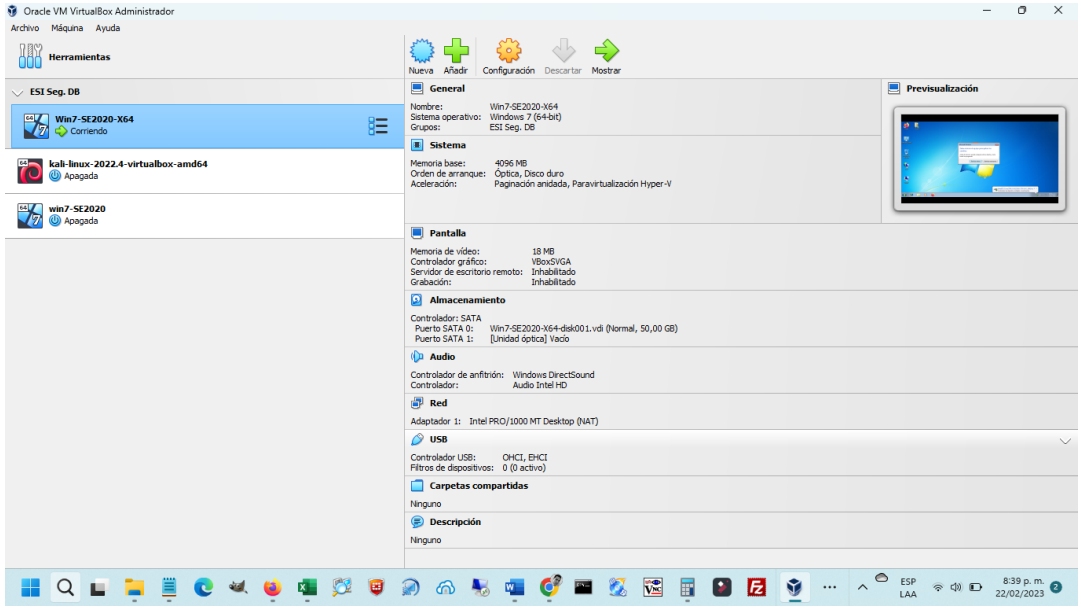
3.4.5 MONTAJE WINDOWS 7 A 64 BITS EN VIRTUALBOX

Figura 12. Se inicia máquina virtual satisfactoriamente



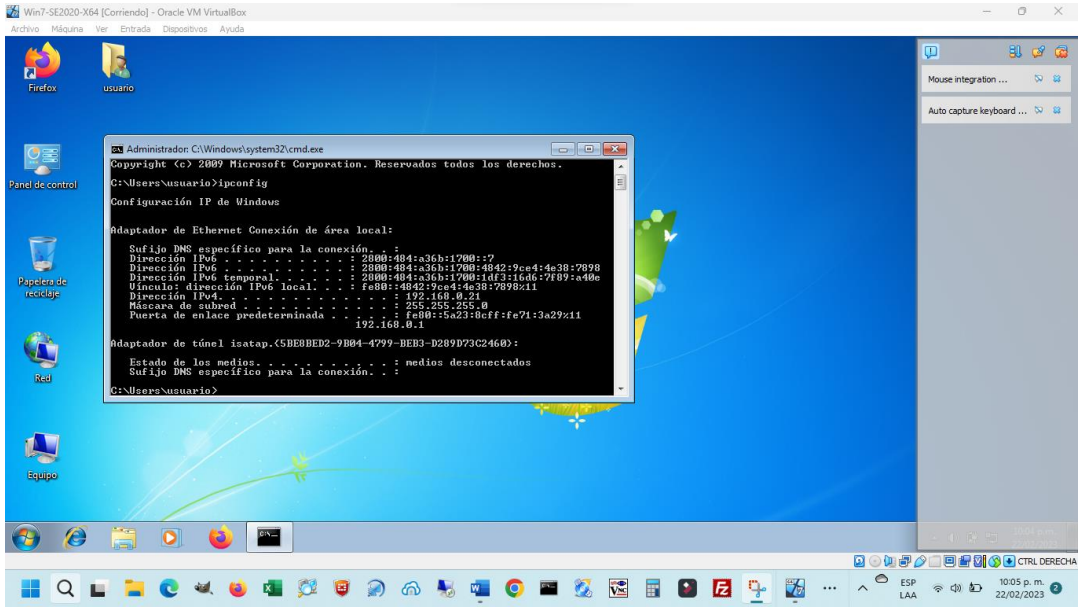
Fuente: Elaboración propia

Figura 13. Se importa imagen Windows 7 a 64 bits en VirtualBox. Se procede a configurar los parámetros del sistema e iniciar la máquina virtual



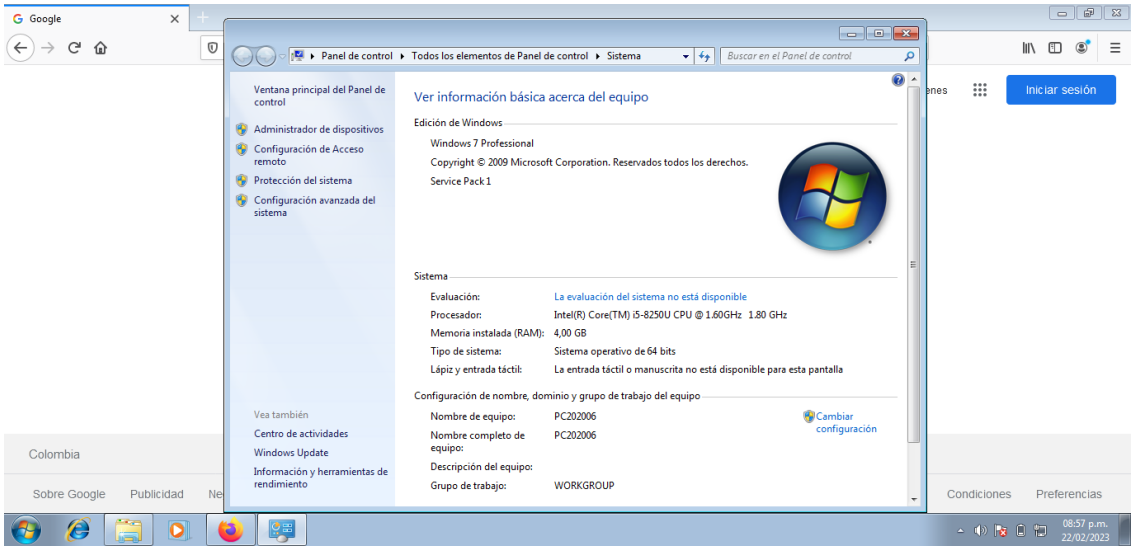
Fuente: Elaboración propia

Figura 14. Configuración de Red dentro del mismo segmento con IP: 192.168.0.21



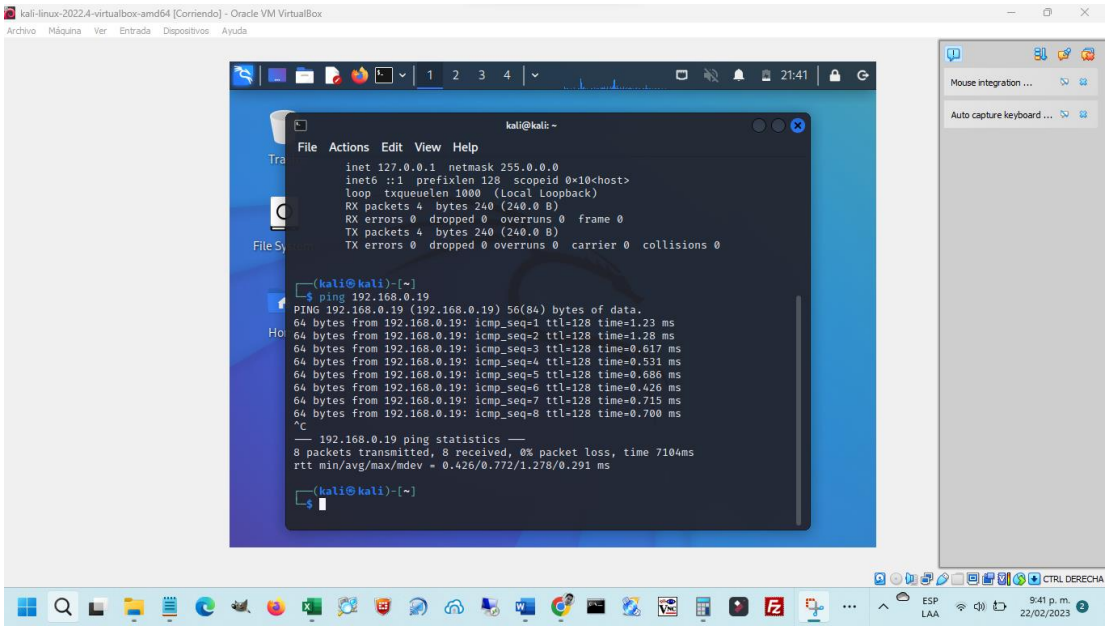
Fuente: Elaboración propia

Figura 15. Hardware de la máquina Windows 7 a 64 Bits



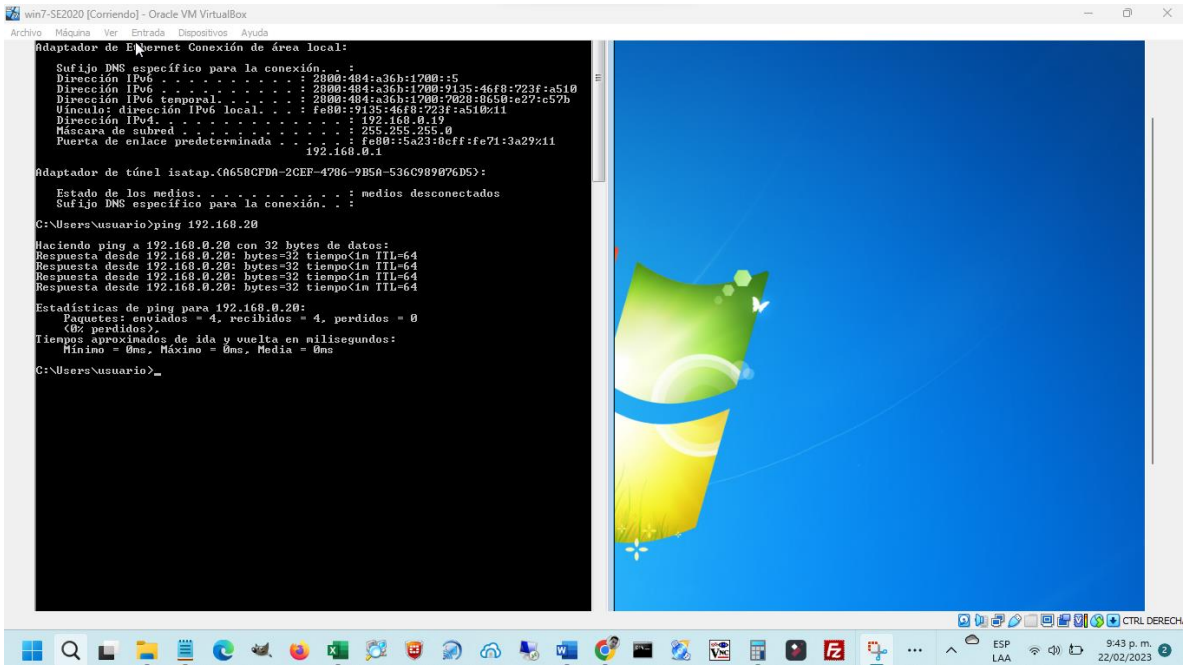
Fuente: Elaboración propia

Figura 16. Comunicación entre las máquinas Kali y Windows 7 32 bits



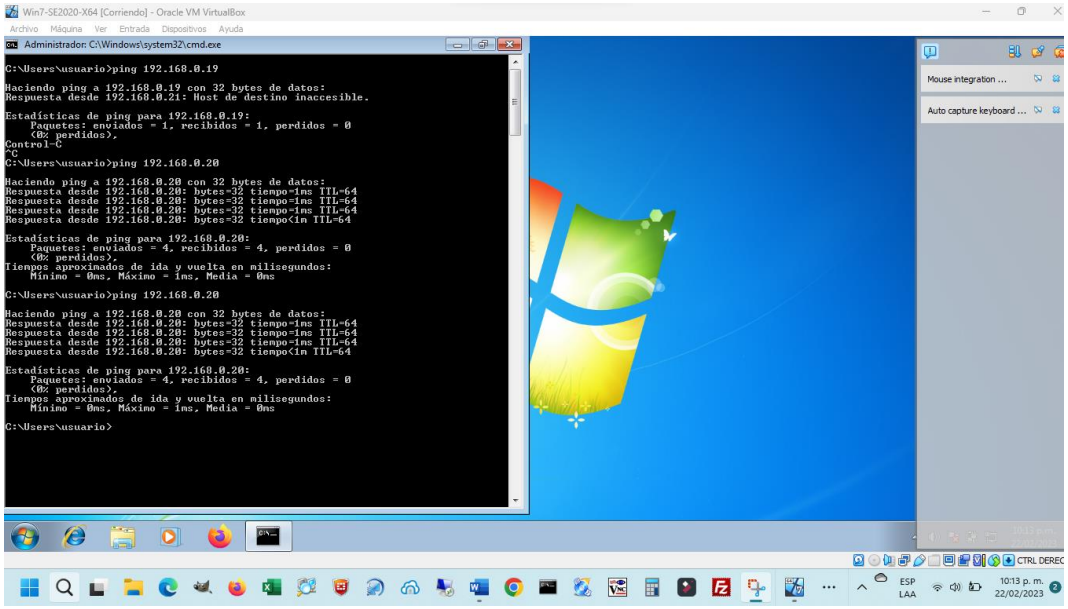
Fuente: Elaboración propia

Figura 17. Comunicación entre las máquinas Windows 7 32 bits y Kali Linux



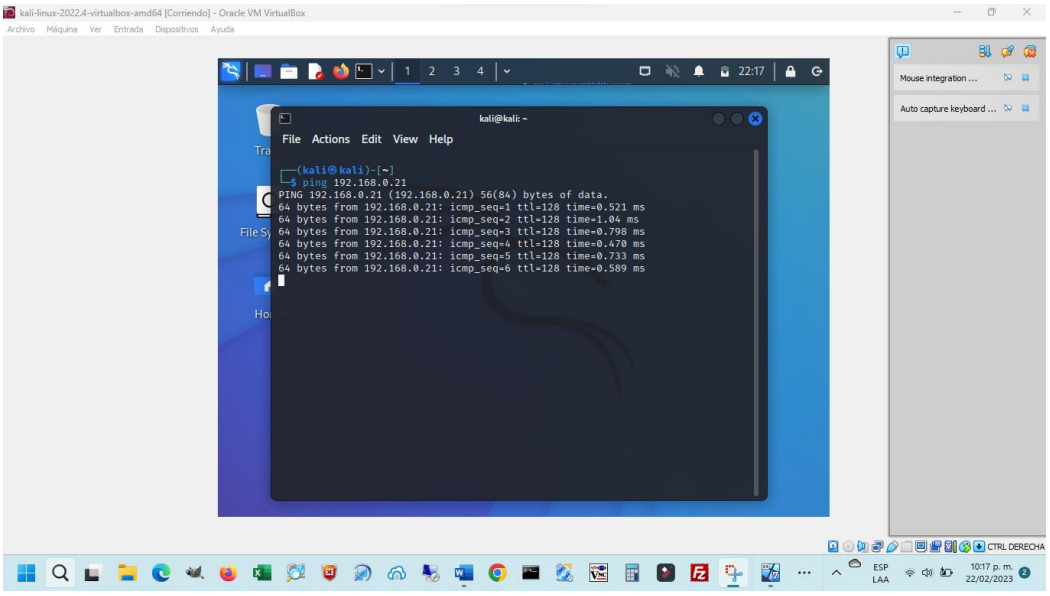
Fuente: Elaboración propia

Figura 18. Comunicación entre las máquinas Windows 7 64 bits y Kali Linux



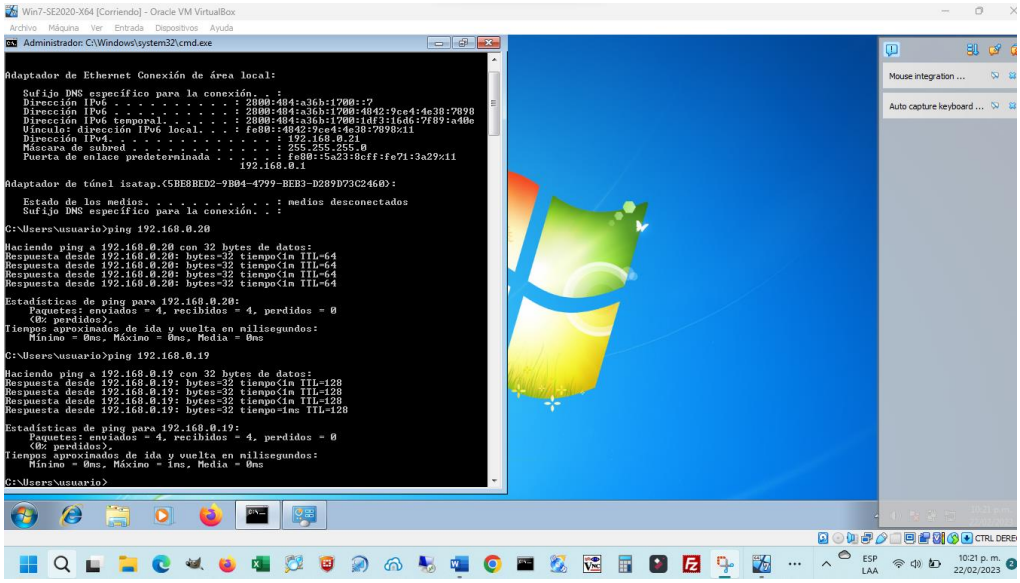
Fuente: Elaboración propia

Figura 19. Comunicación entre las máquinas Kali Linux y Windows 7 64 bits



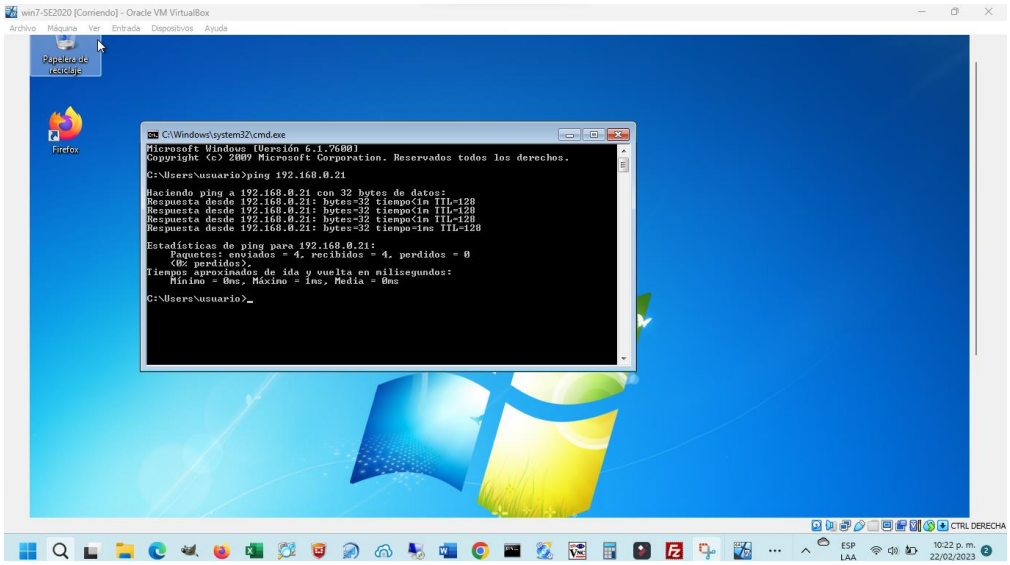
Fuente: Elaboración propia

Figura 20. Comunicación entre las máquinas Windows 7 64 bits y Windows 32 bits



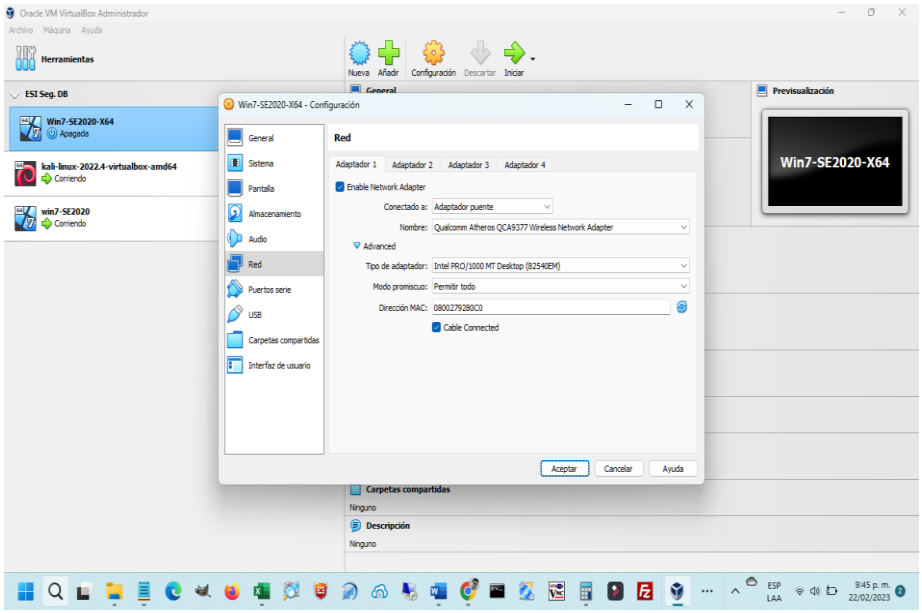
Fuente: Elaboración propia

Figura 21. Comunicación entre las máquinas Windows 32 bits y Windows 7 64 bits



Fuente: Elaboración propia

Figura 22. Configuración de Red en VirtualBox para todas las máquinas tipo Adaptador de Puente:



4. ACTUACIÓN ÉTICA Y LEGAL

4.1 DESARROLLO DE CUESTIONARIO

4.1.1 UNA VEZ LEÍDO EL ANEXO 2 – ESCENARIO 2 Y EL ANEXO 3 – ACUERDO, ¿USTED LOGRA EVIDENCIAR ALGÚN PROCESO ILEGAL Y NO ÉTICO QUE SE ESTÉ ESTIPULANDO EN DICHO ACUERDO?

Una vez leído el escenario del problema y el acuerdo de confidencialidad entre la empresa White House Security y los integrantes de los equipos Red Team & Blue Team, se puede evidenciar que si existen procesos ilegales dentro del acuerdo de confidencialidad en los a siguientes apartes:

- “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 Whitehouse Security no podrán ser divulgados”

  En el Objeto del Acuerdo se encuentra que los integrantes de los equipos de seguridad deberán guardar un acuerdo de confidencialidad sobre procesos ilegales, lo cual viola la ley 1273 sobre los delitos informáticos en Colombia

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

  Dentro de las obligaciones del acuerdo, específicamente en la obligación 3 se viola la ley 1273 sobre de delitos informáticos.

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

  Dentro de las obligaciones del acuerdo, específicamente en la obligación 4 se obliga a los integrantes a guardar reserva sobre información de carácter ilegal, lo cual, lo cual va en contra de la ley 1273 sobre delitos informáticos en Colombia

- “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.”

Dentro de las obligaciones del acuerdo, específicamente en la obligación 9 se obliga a los integrantes a ocultar información de carácter ilegal, lo cual, lo cual también va en contra de la ley 1581, sobre la protección de los datos personales y ley 1273 sobre delitos informáticos en Colombia

4.1.2 ARTÍCULOS DE LA LEY 1273 QUE SE ESTARIAN VULNERARANDO EN EL ACUERDO Y PORQUÉ

4.1.2.1 TODOS LOS ARTICULOS DE LA LEY 1273

De acuerdo con el acuerdo de confidencialidad la empresa Whitehorse Security, en su Objeto, en el que se habla de guardar confidencialidad sobre cualquier proceso ilegal que se esté dando dentro de la organización y al no hablar de cuales son dichos procesos, a mi parecer por ende se podría presentar en cualquier momento durante la ejecución del contrato laboral la violación cualquiera de los artículos de la ley 1273.[3]

4.1.2.2 ARTICULOS DE LA LEY 1273 CON MAS RIESGO

De acuerdo con las obligaciones de confidencialidad existen algunos artículos de la Ley 1273 que tienen mayor riesgo de vulneración:

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO, debido a que se pueda presentar esta vulneración para apropiarse de datos e información de terceros (Obligación No 3 del acuerdo de confidencialidad)

- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS, dado que en el ejercicio de sus actividades puedan realizar esta práctica no al interior de la organización, si no más bien hacia el exterior con fines ilegales

- Artículo 269F. VIOLACIÓN DE DATOS PERSONALES, que como parte de sus actividades dentro de la organización puedan también realizar actividades ilegales que vayan en contra vía de este artículo, que se pone en riesgo en las obligaciones del acuerdo (Obligación No 9 del acuerdo de confidencialidad)

- Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, debido a que se puede presentar agravación del delito cuando se cometiere particularmente en este

[3] SIC. (2009). Ley 1273 de 2009 (pp. 1-4) Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

acuerdo de confidencialidad por incurrir en “Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este", "Revelando o dando a conocer el contenido de la información en perjuicio de otro", "Obteniendo provecho para si o para un tercero"

4.1.3 USTED APLICARÍA A ESTE TRABAJO EN THE WHITEHOUSE

Definitivamente no aplicaría ni aceptaría trabajar con ninguna compañía que tenga un acuerdo de confidencialidad como el que se plantea en el ejercicio, debido a muchas razones, como son los principios éticos y morales adquiridos a lo largo de mi vida y en los que no aplicaría a trabajos que vayan en contravía de dichos principios, además de no poner en riesgo la estabilidad personal y familiar, mi carrera profesional.

Adicionalmente a los anterior, como ingeniero de sistemas, e inscrito en el Concejo profesional de Ingeniería - COPNIA, órgano del estado encargado de controlar inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, quien en diversos apartes define en cumplimiento de la Ley 842 de 2003 “Código de Ética Profesional COPNIA”[4] los deberos y prohibiciones que tenemos como ingenieros, como son las responsabilidades”:

- Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados;

- 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

- Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones

Y las prohibiciones:

- Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley
- 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

[4] COPNIA. Código de Etica para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. (pp. 1-20) Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

4.1.4 OPERACIÓN ANDROMEDA BUGGLY

La operación Andrómeda fue una operación encubierta y secreta, realizado por la inteligencia militar de Colombia, que se destapó en el año 2014 por la revista Semana[5], la operación que consistió en crear una fachada en una casa conocida como Buggly, que invitaba y reunía a toda una comunidad de interesados y expertos informáticos a participar en diversos eventos y actividades aparentemente legales que buscaban principalmente compartir el conocimiento entre la comunidad, siendo un lugar de concentración de muchos expertos sobre todo relacionados con el Haking Ético, sin embargo una vez se destapó la fachada se conocieron acusaciones y detalles de las actividades realizadas en con contra múltiples objetivos, filtrándose información confidencial y hasta conspiraciones en contra de los negociadores de la Paz de aquel momento entre las FARC y el Gobierno de Colombia, en la Habana Cuba, destacándose también la venta por parte de los militares, de información al Hacker Colombiano Andres Sepulveda con una gran cantidad correos confidenciales. La operación Andrómeda desató un escándalo mediático en Colombia, que ocasionó la baja y retiro de múltiples integrantes de la fuerza militar hasta detención y capturas de algunos de ellos. La operación Andrómeda también mostró que no hubo control y seguimiento de los integrantes y que estos incumplieron su compromiso de confidencialidad y reserva, al vender y suministrar información a terceros, violándose las leyes 1273 y 1581 de 2009, dado que se compartió información con fines de lucro, en beneficio de terceros y que se agravan al ser realizados por militares servidores públicos en ejercicios de sus funciones.

[5] REVISTA SEMANA (2015). El informe que sacudió el caso de la fachada Andrómeda. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

5. EJECUCIÓN PRUEBAS DE INTRUSIÓN

5.1 DESCRIPCION DE LAS HERRAMIENTAS UTILIZADAS POR FASES DEL PENTESTING

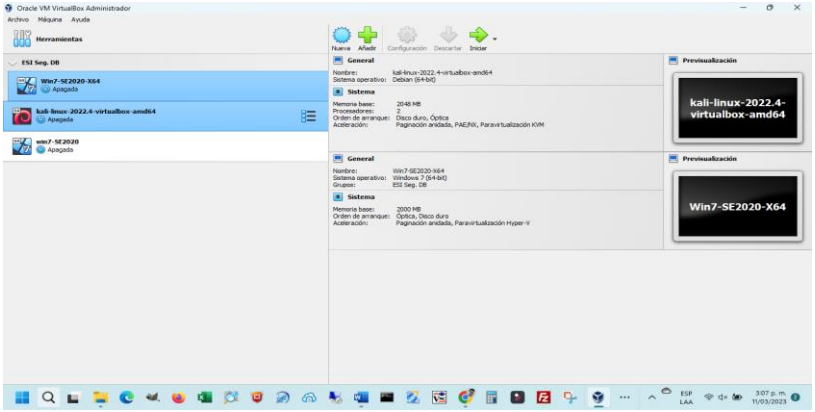
5.1.1 FASE DE PLANEACION

En esta fase no se usan herramientas, sin embargo de acuerdo con el escenario planteado en el anexo 4, escenario 3 se define el alcance tomando como elementos clave para realizar la planeación de la Prueba de seguridad los siguiente:

- Se sabe que se está generando fuga de información al interior de la organización en uno de sus equipos de cómputo.
- El equipo donde se genera la fuga de información tiene instalada una aplicación llamada Rejetto v 2.3
- La aplicación al parecer tiene asociado un Exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.

A partir de lo anterior se plantea aplicar un Pentesting para encontrar el fallo y vulnerabilidad que se está presentando, para lo cual se recreará el escenario haciendo uso de 2 máquinas anteriormente implementadas en el Banco de Trabajo del Equipo, siendo una de ellas una imagen de Windows 7 64 Bits, y la otra una con Kali Linux, la cual tiene las herramientas necesarias para realizar las pruebas del Pentesting.

Figura 23. Banco de trabajo Con Windows 7 x64 y Kali Linux



Fuente: El Autor

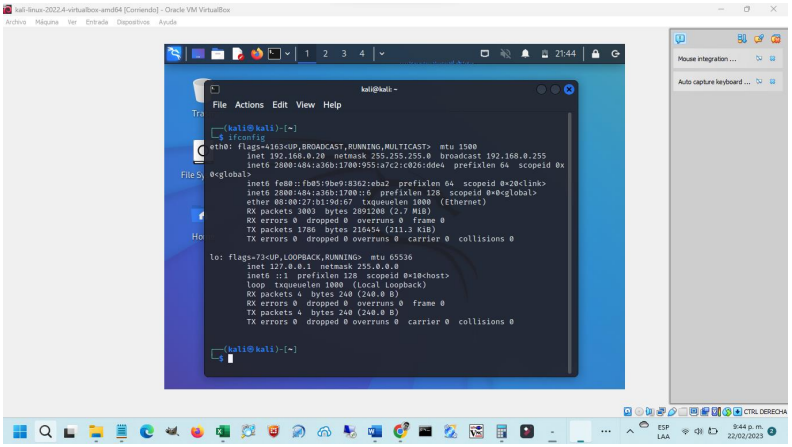
5.1.2 FASE DE DESCUBRIMIENTO Y ANALISIS DE VULNERABILIDADES

5.1.2.1 HERRAMIENTAS UTILIZADAS

5.1.2.1.1 COMANDOS PARA OBTENCION DIRECCIONES IP

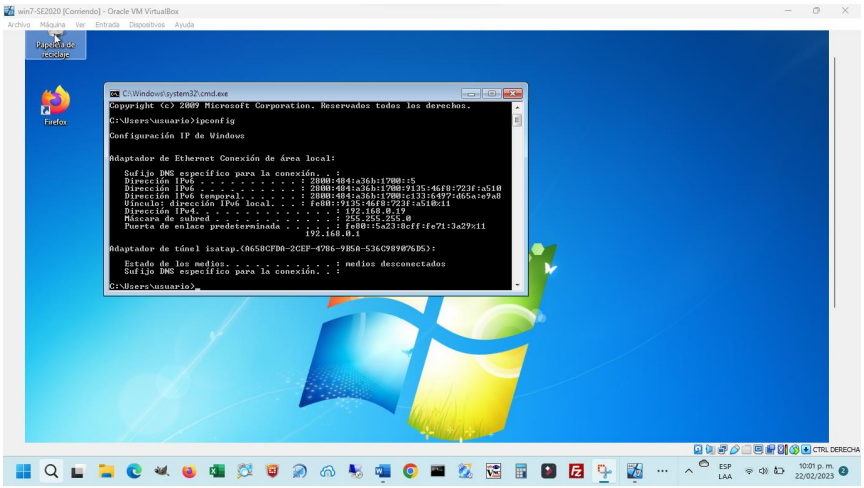
Se utilizan los comandos Ipconfig en Windows y Ifconfig en Kali Linux para obtener las direcciones IP de las máquinas.

Figura 24. Identificación Dirección Ip equipo con Kali Linux 192.168.0.20



Fuente: El Autor

Figura 25. Identificación Dirección IP Windows 7 X64 192.168.0.19

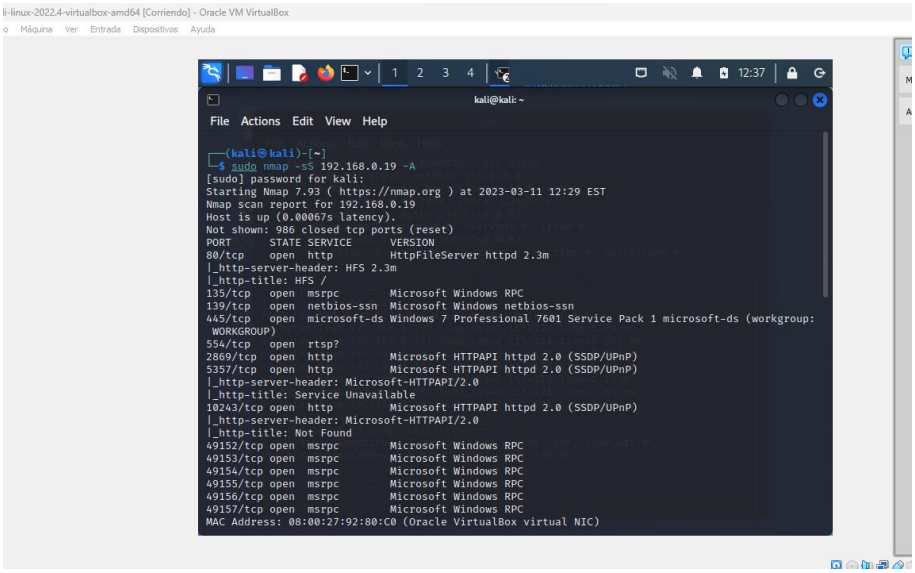


Fuente: El Autor

5.1.2.1.2 HERRAMIENTA NMAP

Nmap es una herramienta que sirve para el escaneo y rastreo de puertos abiertos en los sistemas informáticos, brindándonos información muy útil como puertos abiertos, nombres de aplicaciones, versión de las aplicaciones, entre otros.
Usamos para nuestro ejercicio el comando nmap -sS 192.168.0.19 para descubrir puertos abiertos en la máquina víctima con Windows 7 X64, con dirección ip 192.168.0.19

Figura 26. Resultado escaneo de puertos con Nmap



Fuente: El Autor

Resultado: Una vez se ha completado la ejecución de la herramienta se puede visualizar los puertos y servicios abiertos, que para el ejercicio se tiene abierto el puerto 80/TCP con la aplicación Rejetto de versión 2.3 HFS

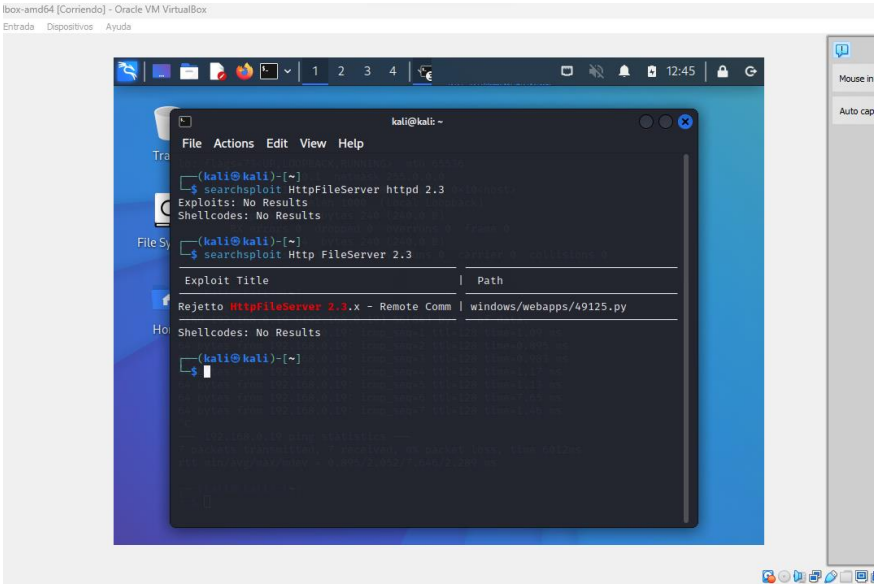
5.1.2.1.3 HERRAMIENTA SEARCHEXPLOIT

La herramienta SearchExploit, es una aplicación que sirve para realizar una búsqueda de Exploits conocidos de un título o aplicación en particular[6]. En nuestro ejemplo el resultado de la búsqueda obtiene un Exploit como se ve en la figura 5

[6] Ethical Hacking. CÓMO USAR SEARCHSPLOIT PARA ENCONTRAR EXPLOITS(2018).Disponible en: https://blog.ehcgroup.io/2018/11/27/01/00/39/4198/como-usar-searchsploit-para-encontrar-exploits/hacking/ehacking/

con el nombre del Exploit, ubicación y en el nombre del exploid un código que nos permitirá obtener el Código de Vulnerabilidad CVE.

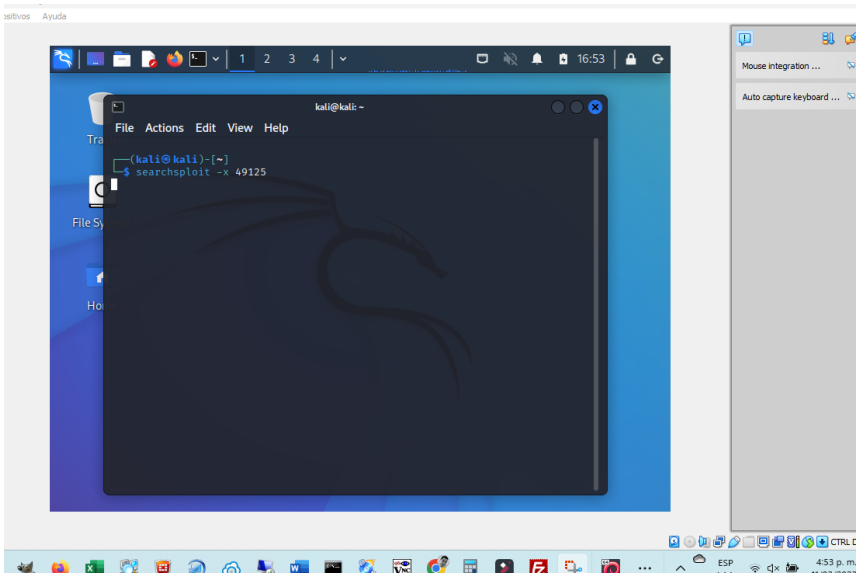
Figura 27. Resultado SearchExploit de Http Fileserver 2.3



Fuente: El Autor

A continuación digitamos el comando searchsploit -x 49125 para abrir la ubicación del Exploid y así poder obtener el código CVE

Figura 28. Resultado comando searchsploit -x 49125 para obtener el CVE



Fuente: El Autor

5.1.3 FASE DEL ATAQUE

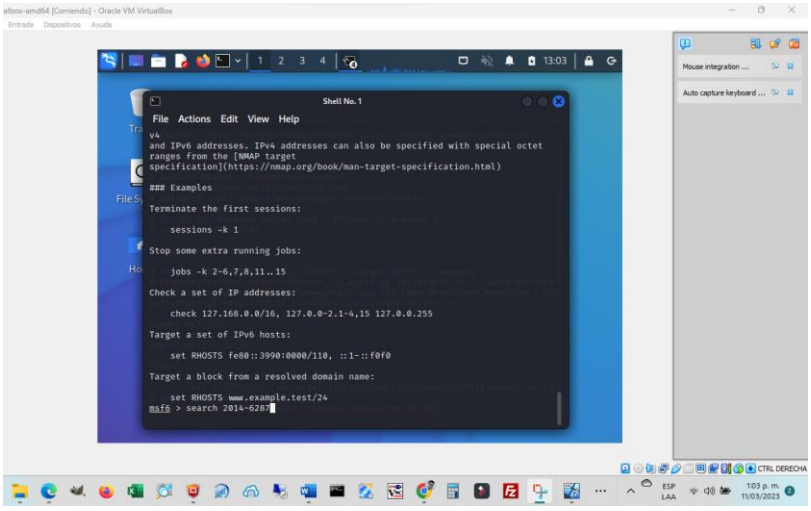
5.1.3.1 HERRAMIENTAS UTILIZADAS

5.1.3.1.1 HERRAMIENTA METASPLOIT

Para realizar el ataque dentro de nuestro escenario planteado, se utilizará la herramienta Metasploit, la cual “es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos”[7].

Con esta herramienta se realizará el ataque, para lo cual se debe ingresar desde la máquina con Kali Linux a la aplicación Metasploit, y ejecutar el comando **search 2014-6287** en busca del exploit encontrado en la fase de descubrimiento, como se puede observar en la figura 7.

Figura 29. Resultado Búsqueda en Metasploit la vulnerabilidad encontrada



Fuente: El Autor

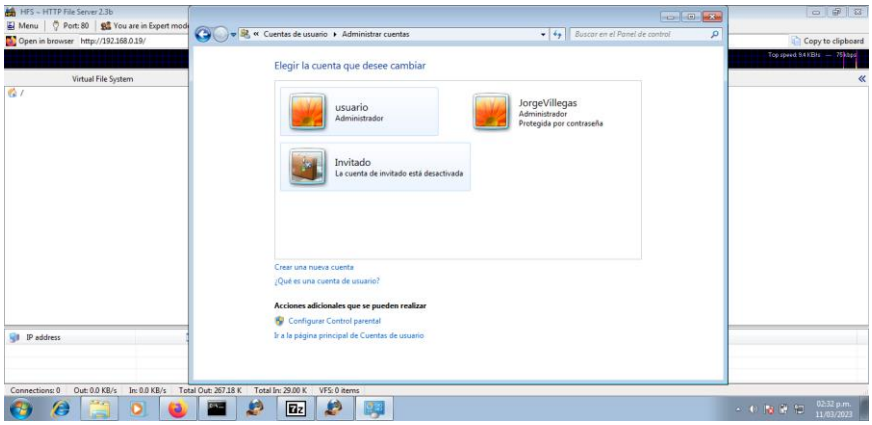
5.1.4 FASE DEL POST ATAQUE – ESCALAR PRIVILEGIOS

Se continúa usando la herramienta Metasploit, usando el exploit se crea un usuario con los permisos de administrador, para ello usamos el comando getsystem y luego

[7] Wikipedia. Metasploit(2023).Disponible en: https://es.wikipedia.org/wiki/Metasploit

Shell, de tal forma que se crea una sesión en el equipo victima para crear el usuario administrador

Figura 30. Resultado Escalamiento de Privilegios Usuario Creado en Windows



Fuente: El Autor

5.2 DATOS E INFORMACIÓN DEL ANEXO 4 – ESCENARIO 3 QUE SE TUVO EN CUENTA PARA IDENTIFICAR EL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 7 X64.

A continuación se lista los datos e información específica que dio las pautas para realizar la planeación y ejecución de la prueba de seguridad, la cual dio como resultado la identificación del fallo de seguridad sobre la máquina Windows 7:

- Aplicación Rejetto v 2.3: La aplicación da el primer indicio, por tanto es crucial para realizar la investigación sobre la aplicación, funcionamiento y versiones de la misma, con el objetivo de entender su funcionamiento técnico.
- Sistema Operativo Windows 7 x64: El sistema Operativo Windows 7 x64 se encuentra desatendido por su fabricante, por tanto también es un dato importante para la identificación de las vulnerabilidades
- Se sospecha de una sesión Shell reversa y una sesión abierta de Meterpreter y escalamiento de privilegios, lo que nos da indicio que se está ejecutando probablemente un Exploit dentro de la máquina, por tanto uno de los objetivos será encontrar dicho Exploit

Una vez con la información inicial se procede a realizar los pasos del Pentesting para encontrar el fallo de seguridad en la máquina con Windows 7, encontrando que

la aplicación Rejjeto v2.3 que se está usando está usando, es una versión desactualizada, lo cual es aprovechada por un Exploit conocido de dicha aplicación.

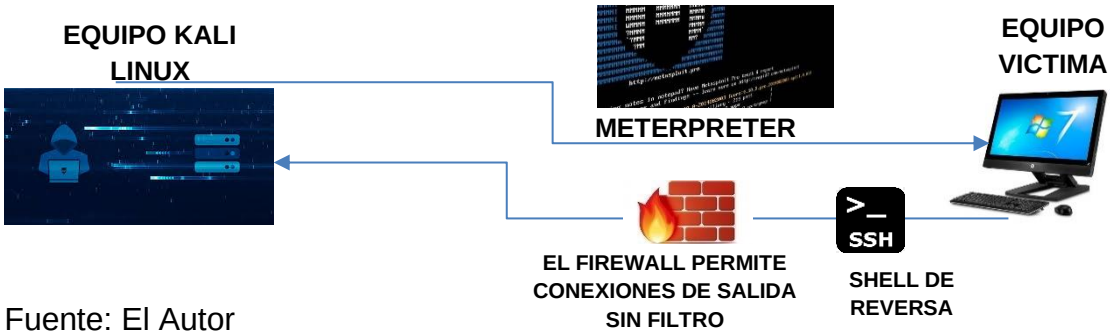
5.3 HERRAMIENTAS PARA IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA “MÁQUINA WINDOWS 7”? ¿CUÁL ES PUERTO ABIERTO?

- Se utilizó la herramienta Nmap para buscar los puertos abiertos, nombre de servicios y versiones, encontrando la aplicación Rejetto v 2.3 por el puerto 80 /TCP
- Luego se usó la herramienta SearchExploit para identificar los fallos de seguridad y ver los Exploit de dicha aplicación.
- Una vez encontrada la vulnerabilidad y un exploit para dicha vulnerabilidad se uso la herramienta Metasploit para atacar la máquina y hacerse con el control del equipo.
- El puerto que usa la aplicación Rejetto v 2.3 es el puerto 80 corriendo sobre TCP(Tranfer Control Protocol)

5.4 CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64)

El ataque afecta a la máquina de Windows 7 de forma crítica, dado que el ataque toma control total de la máquina pudiendo incluso llegar al punto de escalar privilegios y crear un usuario administrador de la máquina, por tanto la afectación sobre la máquina puede ser catastrófica, y lo hace gracias a que en la máquina con Windows 7 que se ejecuta la aplicación Rejetto en una versión desactualizada y vulnerable (v 2.3), El atacante usa un Exploit conocido para enviar código malicioso a través de la herramienta MetaSploit y ejecutar una Shell TCP de reversa y una sesión abierta de Meterpreter, pudiendo hacerlo gracias a la carga de un Payload. A continuación describimos dicho ataque en la siguiente gráfica:

Figura 31. Ataque



Fuente: El Autor

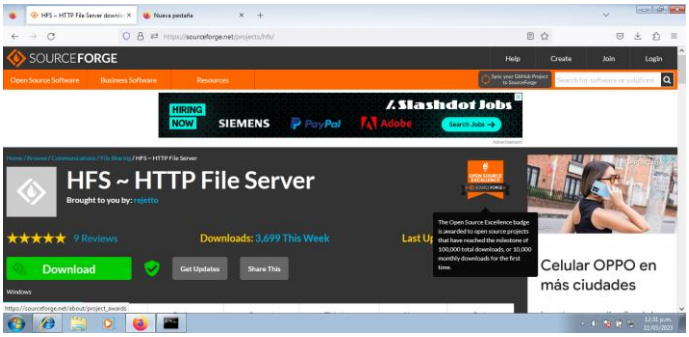
5.5 DOCUMENTACION DE LOS PASOS QUE SE EJECUTARON PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS 7

A continuación se realiza la descripción y documentación completa de todo el proceso del Pentesting realizado:

5.5.1 INSTALACION DE REJETTO V. 2.3

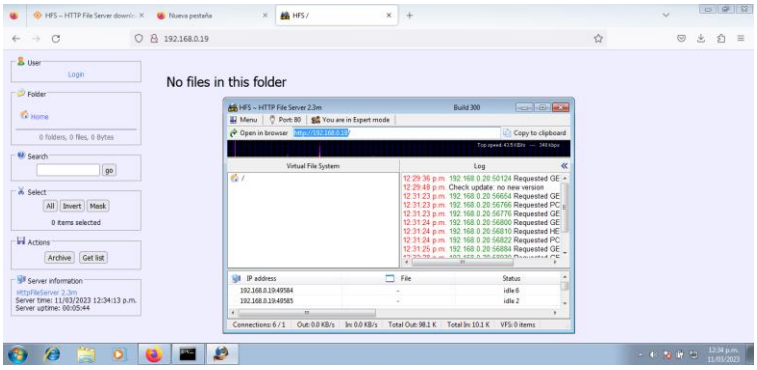
Para recrear el escenario y poder identificar las vulnerabilidades se procede a descargar e instalar la aplicación en cuestión Rejetto v 2.3b, aplicación que es un software (programa) que permite enviar y recibir archivos a través del protocolo http(web), en donde se puede limitar a compartir archivos solo con unos pocos amigos o se puede abrir el servidor a todo el mundo.[8]

Figura 32. Descarga de HFS Rejetto 2.3b de https://www.rejetto.com/hfs/?f=dl



Fuente: El Autor

Figura 33. Instalación de HFS Rejetto 2.3b



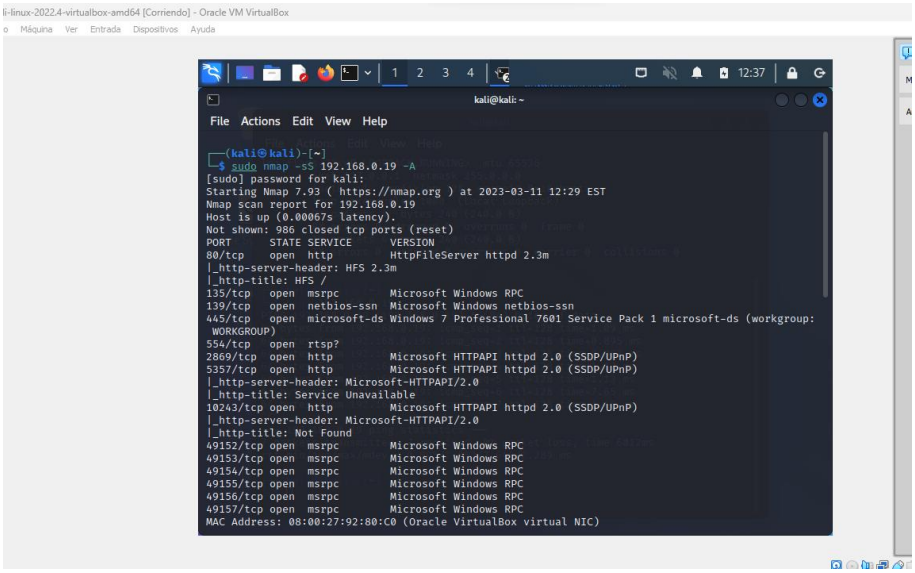
Fuente: El Autor

[8] REJETTO. (2018). Wiki Disponible en: https://www.rejetto.com/wiki/index.php?title=HFS:_Introducci%C3%B3n

5.5.2 ANALISIS Y ESCANEO DE PUERTOS CON NMAP

Una vez se cuenta con el escenario completo, se procede a realizar el análisis de puertos. Usamos para nuestro ejercicio el comando nmap -sS 192.168.0.19 para descubrir puertos abiertos en la máquina víctima con Windows 7 X64, con dirección ip 192.168.0.19

Figura 34. Escaneo de puertos con Nmap



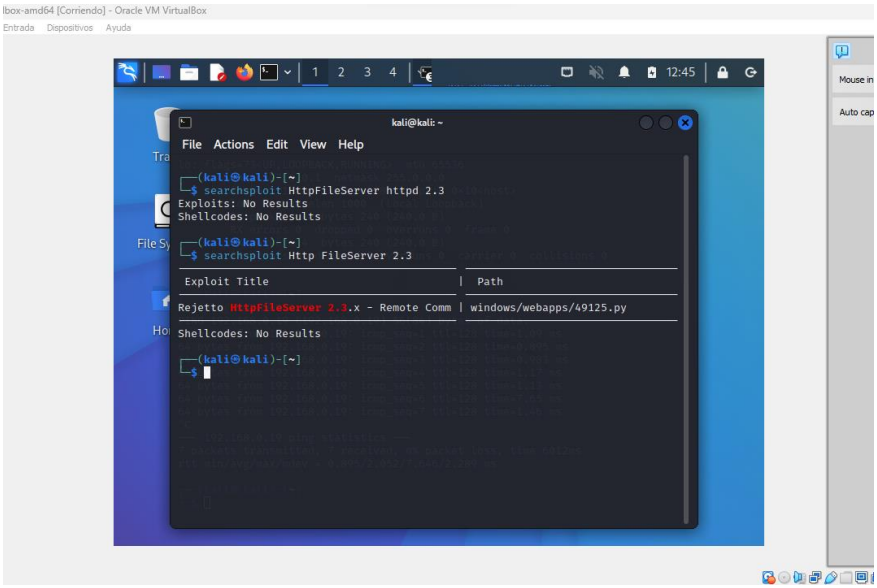
Fuente: El Autor

Una vez se ha completado la ejecución de la herramienta podemos visualizar en el resultado de la figura 6, los puertos y servicios abiertos, que para nuestra actividad se encuentra abierto el puerto 80/TCP con la aplicación Rejetto de versión 2.3.

5.5.3 ANALISIS DE VULNERABILIDADES EN BUSCA DE EXPLOITS

Continuando con la fase de descubrimiento una vez conocemos el número del puerto abierto, el nombre del servicio en ejecución, y la versión, se procede a realizar una búsqueda con la herramienta SearchExploit. En nuestro ejemplo el resultado de la búsqueda obtiene un Exploit como se ve en la figura 7 con el nombre del Exploit, ubicación y en el nombre del Exploid un código que nos permitirá obtener el Código de Vulnerabilidad CVE.

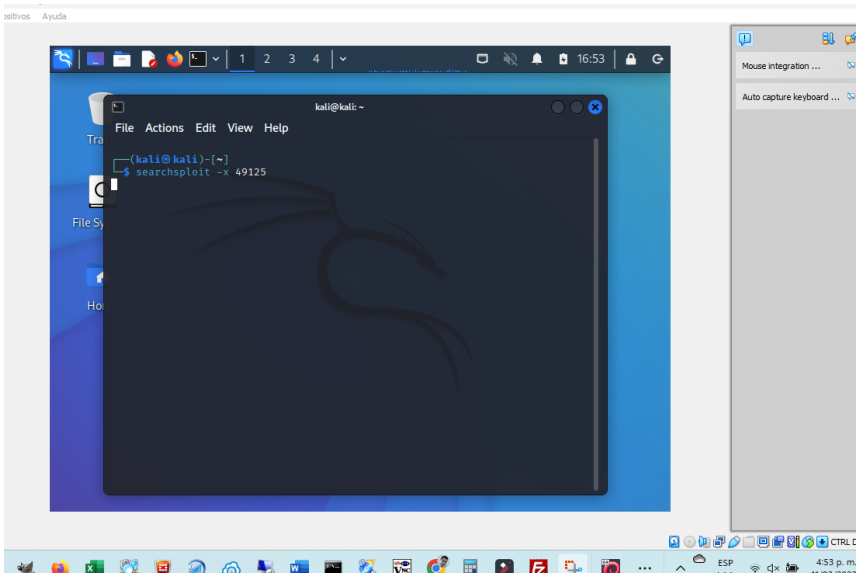
Figura 35. Resultado SearchExploit de la búsqueda de http Fileserver 2.3



Fuente: El Autor

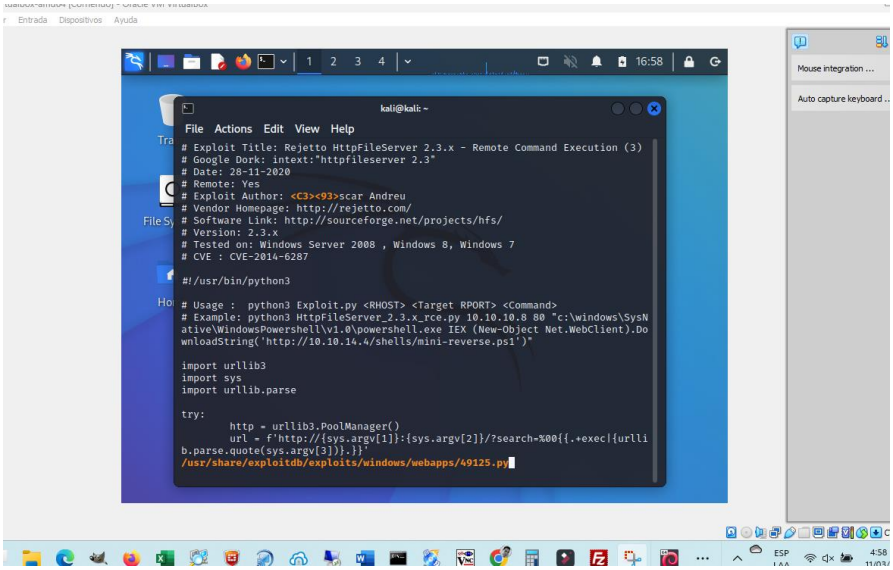
A continuación digitamos el comando searchsploit -x 49125 para abrir la ubicación del Exploid y así poder obtener el código CVE

Figura 36. Uso del Comando searchsploit -x 49125 para obtener el CVE



Fuente: El Autor

Figura 37. El código CVE 2014-6287

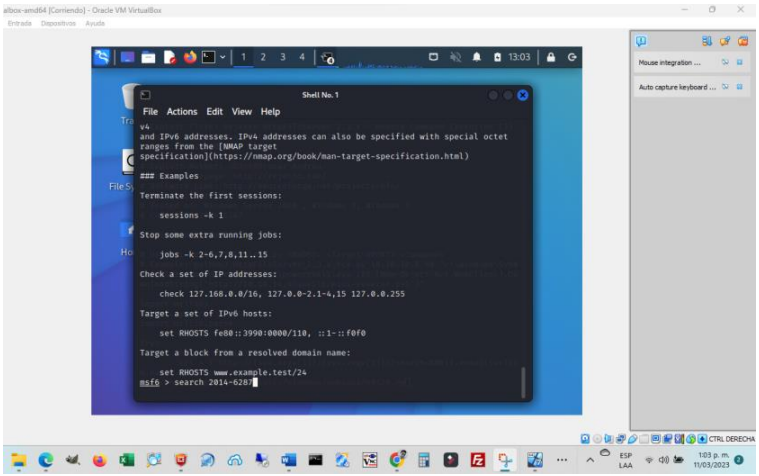


Fuente: El Autor

5.5.4 REALIZANDO EL ATAQUE CON METASPLOIT

Para realizar el ataque dentro de nuestro escenario planteado, se usa Metasploit. Con esta herramienta se realizará el ataque, para lo cual se debe ingresar desde la máquina con Kali Linux a la aplicación Metasploit, y ejecutar el comando **search 2014-6287** en busca del exploit encontrado en la fase de descubrimiento, como se puede observar en la figura 22.

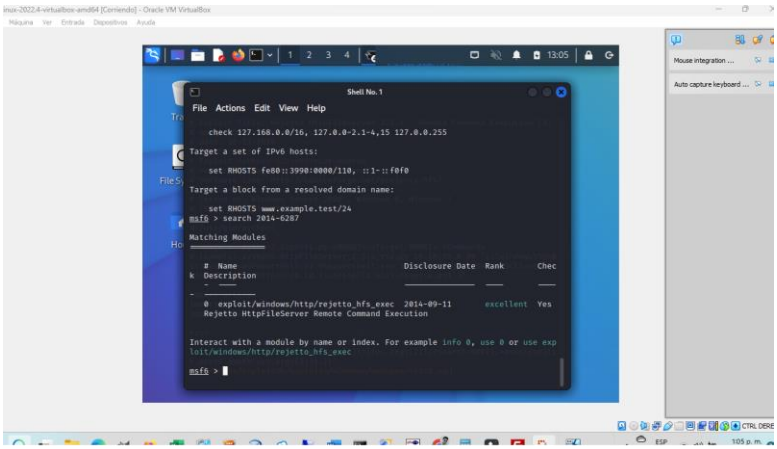
Figura 38. Buscando en Metasploit la vulnerabilidad encontrada



Fuente: El Autor

Una vez Metasploit localice el Exploit nos dará la opción de usar el Exploit con el comando ***use 0***

Figura 39. Usando el Exploit Rejetto v 2.3

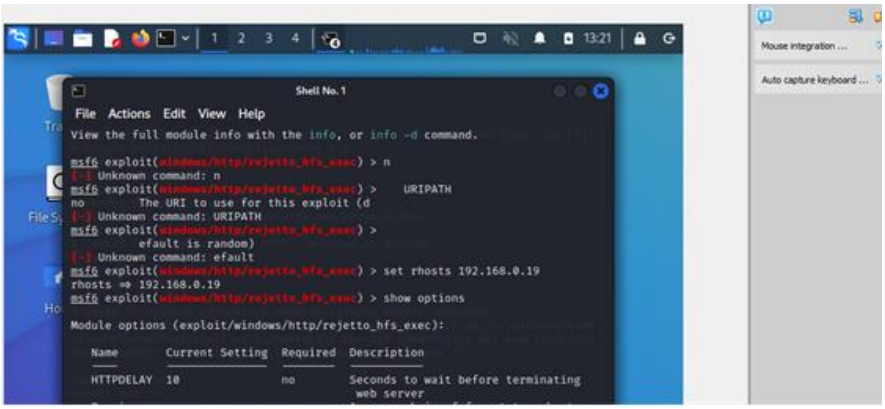


Fuente: El Autor

Visualizamos las opciones que tiene disponible el exploit con el comnano ***Show Options***

Encontrando que únicamente es necesario ajustar la ip o dirección del destino a atacar, en este caso usamos el comando set rhosts 198.168.0.19

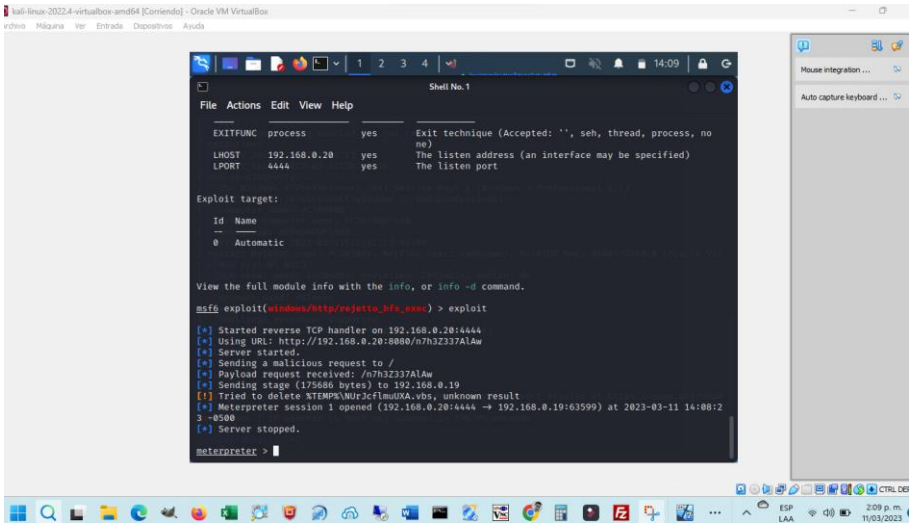
Figura 40. Configurando máquina destino para el ataque



Fuente: El Autor

Se realiza la verificación nuevamente de la configuración del exploit y se genera el ataque de estar todo correcto con el comando ***exploit***

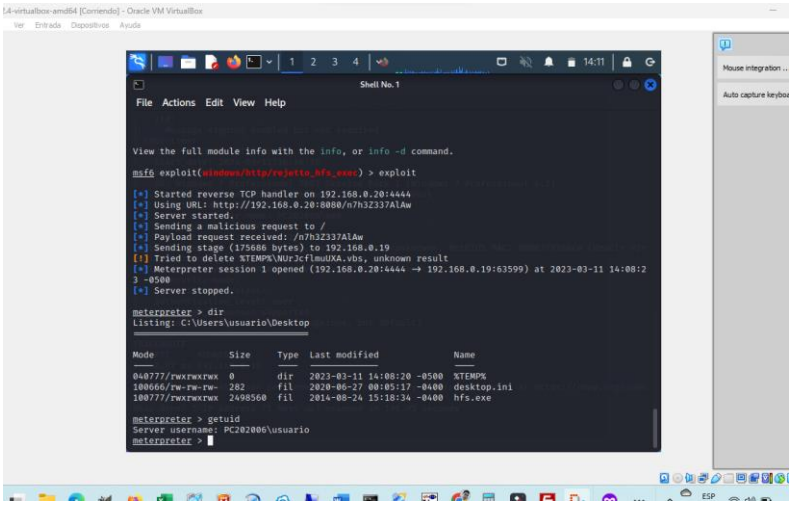
Figura 41. Ejecución del Ataque exitoso



Fuente: El Autor

Una vez dentro del sistema ejecutamos el comando ***getuid*** para ver con que usuario nos logueamos en el equipo Windows, como se puede ver en la figura 26

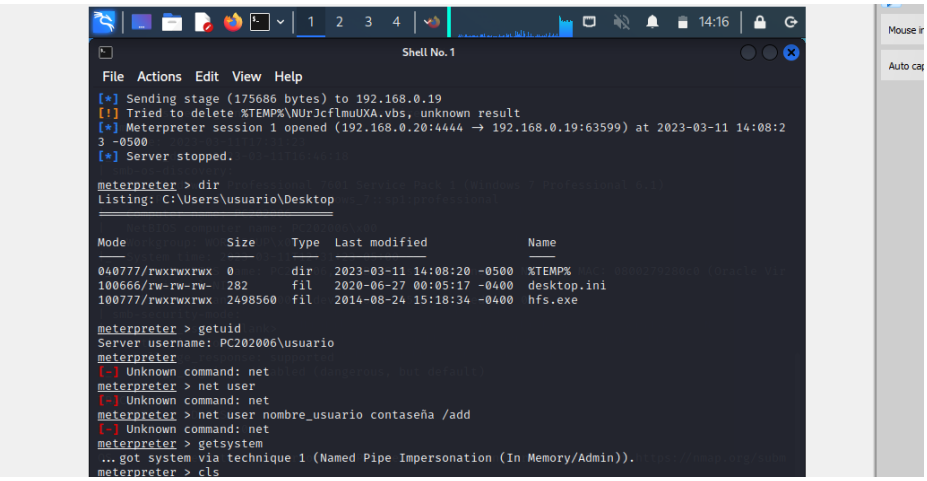
Figura 20. Ver el usuario con el que se logueo luego del ataque



Fuente: El Autor

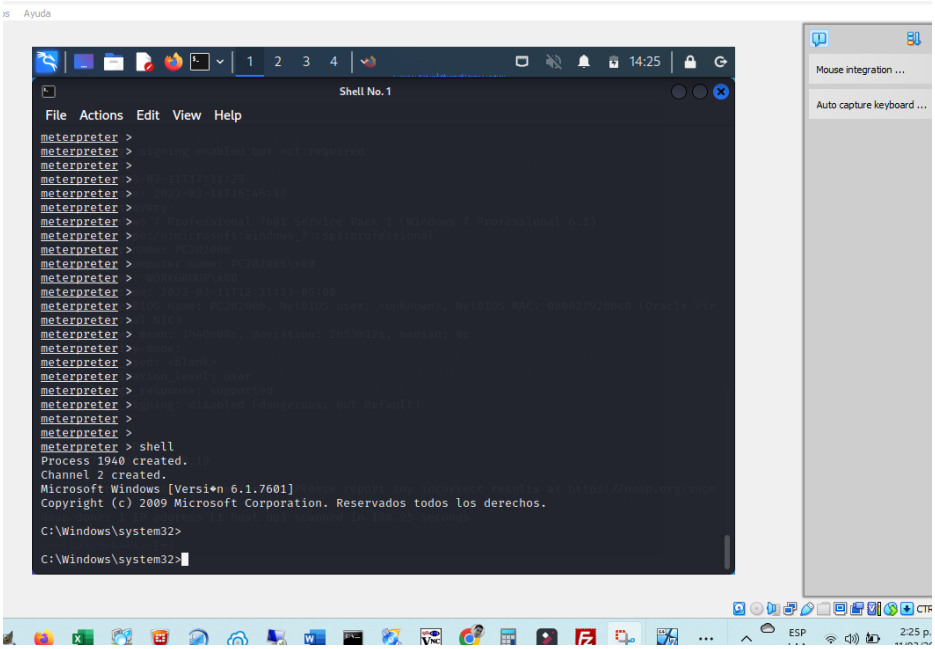
Para completar el ataque se crea un usuario con los permisos de administrador, para ello usamos el comando getsystem y luego Shell, de tal forma que se crea un sesión en el equipo victima para crear el usuario administrador

Figura 42. Getsystem



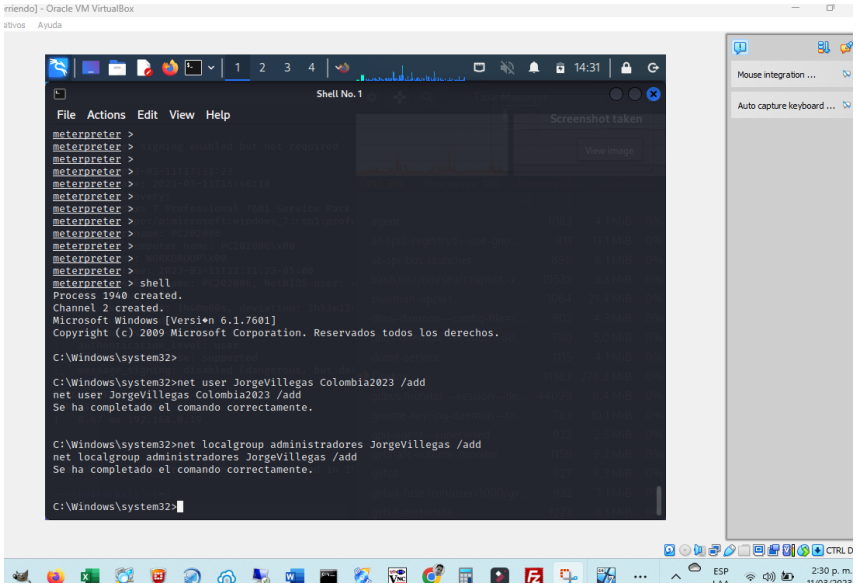
Fuente: El Autor

Figura 43. Comando Shell que crea una sesión en el equipo victima



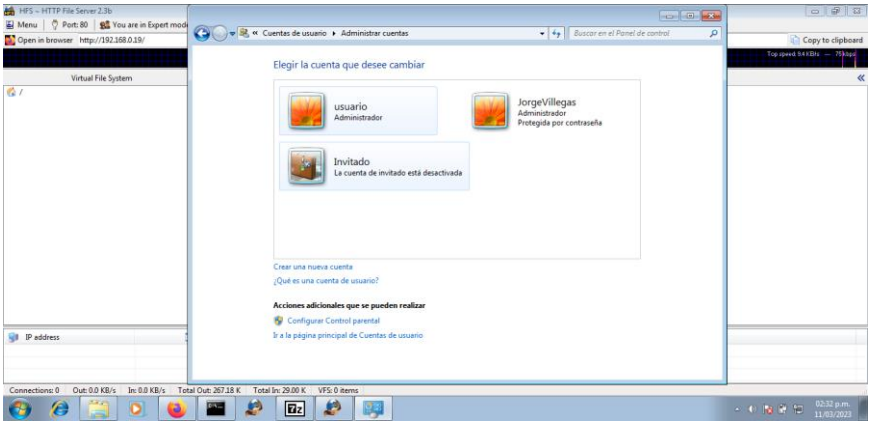
Fuente: El Autor

Figura 44. Creando usuario Jorge Villegas como administrador en máquina atacada



Fuente: El Autor

Figura 45. Usuario Creado en Windows



Fuente: El Autor

6. CONTENCIÓN DE ATAQUES INFORMÁTICOS

6.1 RESPUESTAS CUESTIONARIO

6.1.1 ¿QUÉ SERÍA LO PRIMERO QUE INDAGARÍA Y HARÍA SI LLEGARA A ENCONTRARSE UN ATAQUE EN TIEMPO REAL? ESPECIFIQUE SU RESPUESTA CON ARGUMENTOS TÉCNICOS.

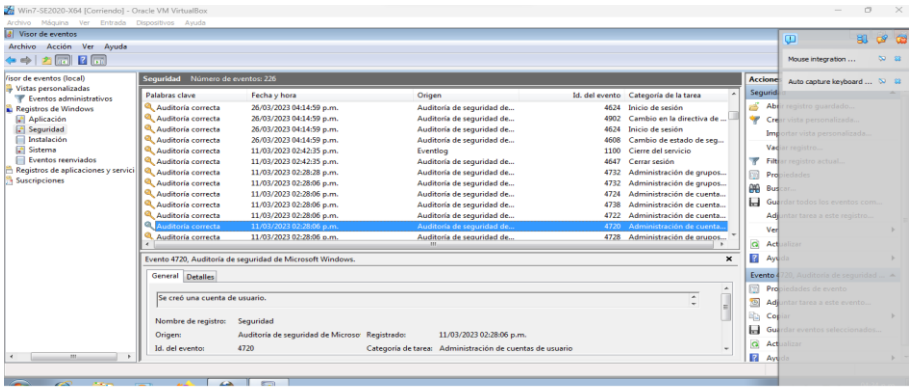
6.1.1.1 ANALISIS BLUE TEAM

De acuerdo con el escenario planteado en el anexo 5, lo primero a indagar sería que no se hayan comprometido los siguientes escenarios validando el estado de cada uno:

6.1.1.1.1 ACCESO NO AUTORIZADO

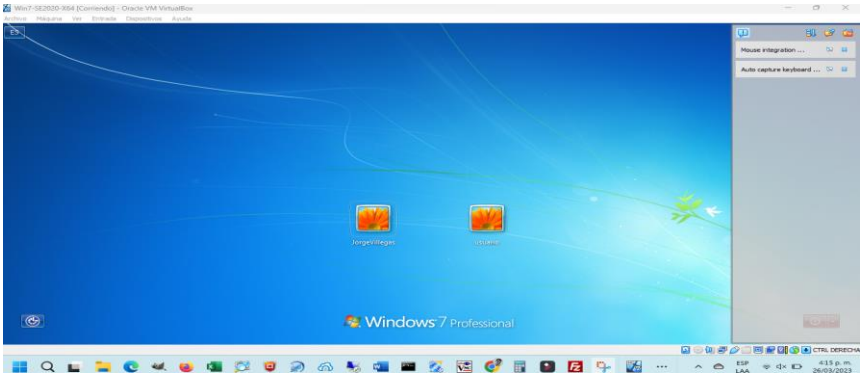
Lo primero que validaría sería el **acceso no autorizado**, de tal forma que se revisaría que en la máquina que no existan nuevos usuarios creados y que además no existan conexiones remotas sospechosas, para ello en primero lugar revisamos el log de eventos de Seguridad del Sistema Operativo Windows 7 X64, para verificar que no existan usuarios creados recientemente, encontrando para nuestro caso un usuario creado en el sistema sin autorización.

Figura 46: Se encuentra un Usuario creado recientemente en el sistema Windows 7



Fuente: El Autor

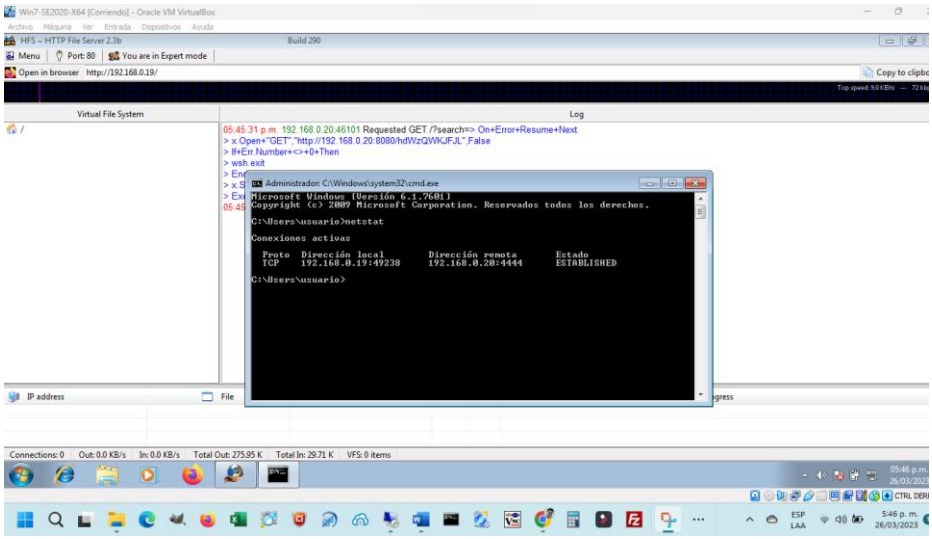
Figura 47: Usuario no Autorizado Creado: JorgeVillegas



Fuente: El Autor

Luego en segundo lugar revisamos con ayuda del comando NETSTAT las conexiones activas en el sistema, encontrando una conexión no autorizada desde una máquina con dirección ip 192.168.0.20 (Máquina Kali Linux):

Figura 48: Detectar conexiones remotas abiertas en la máquina con Windows



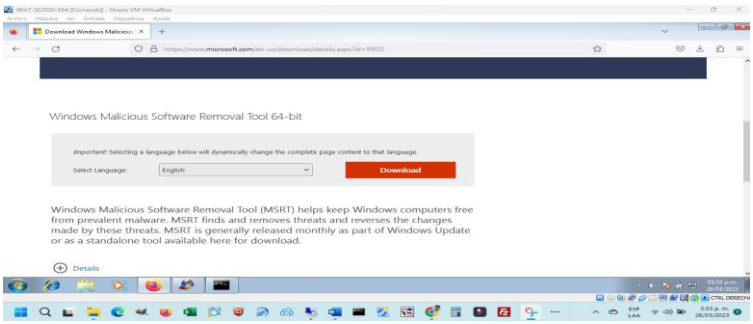
Fuente: El Autor

6.1.1.1.2 CODIGO MALICIOSO

Una vez identificado que el sistema fue vulnerado, se procedería a tomas las medidas necesarias contener el ataque, que para el caso del escenario se recomienda buscar y eliminar el código malicioso que se cargó a la máquina, para ello se pueden usar herramientas gratuitas de Windows como son la Herramienta

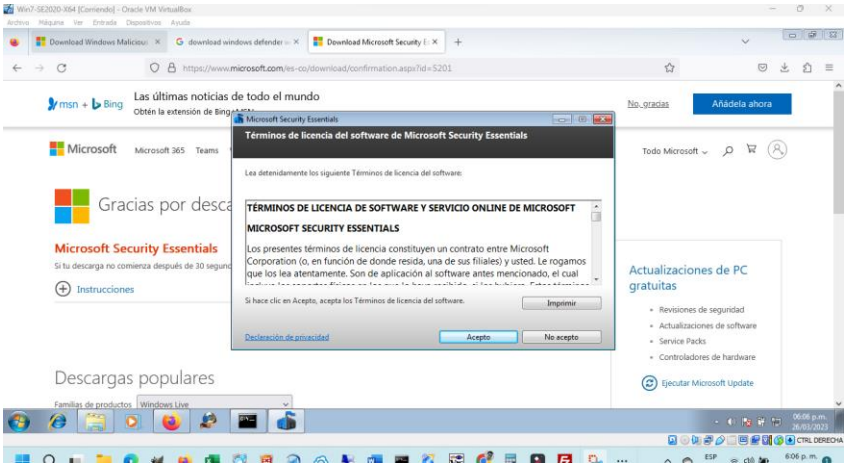
de Eliminación de Código Malintencionada de Microsoft o el Antivirus para Windows 7 X64, Microsoft Secure Essentials.

Figura 49 Windows Malicius Software Removal Tool



Fuente: El Autor

Figura 50: Microsoft Secure Essentials.

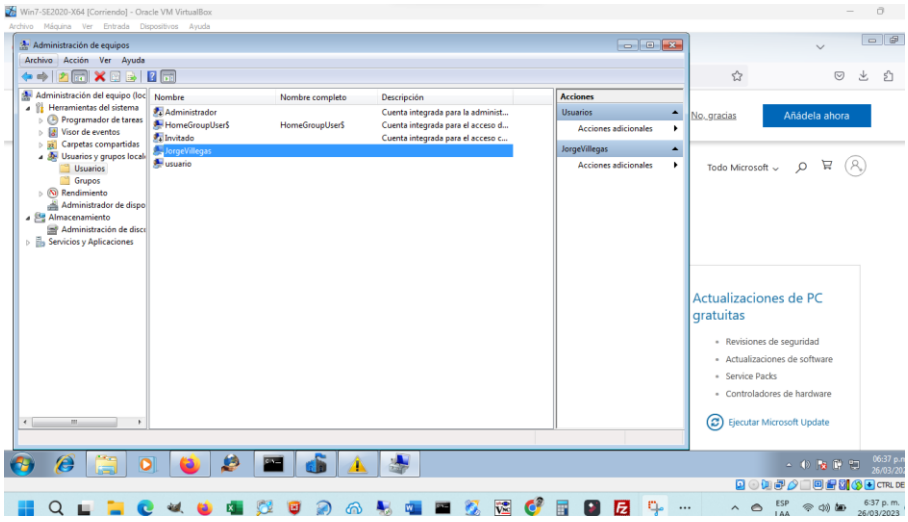


Fuente: El Autor

6.1.1.1.3 COMPROMISO DEL ADMINISTRADOR DEL SISTEMA

Es importante en el análisis identificar si hubo escalamientos de privilegios, para lo cual en el ejemplo validamos que el usuario creado es ahora parte de un grupo de usuarios con privilegio administrador, para lo cual bastará con validar desde la consola de administración de usuarios los permisos del nuevo usuario, como se observa en la Figura 5, para nuestro caso si hubo compromiso del Administrador.

Figura 51: Detectar escalamiento de Privilegios

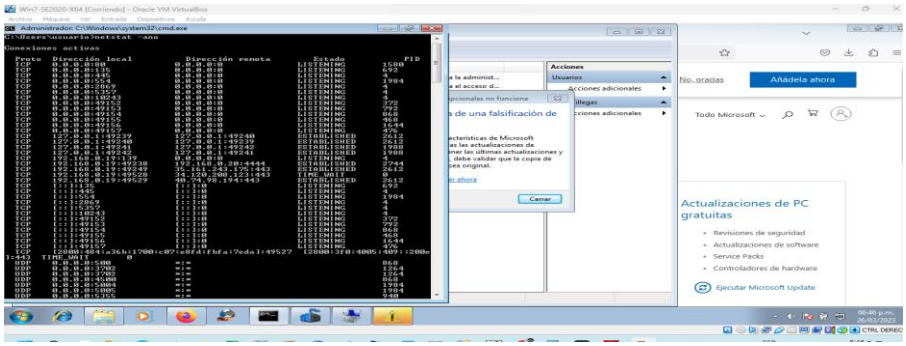


Fuente: El Autor

6.1.1.1.4 PUERTOS ABIERTOS DEL SISTEMA WINDOWS 7 X64

Continuando con la revisión del incidente del ataque se puede revisar los puertos abiertos del sistema a través de la ejecución del comando netstat -ano en Windows, tal como se muestra en la figura 7, donde podemos ver los puertos abiertos y la conexión desde la máquina 192.168.0.19

Figura 52: Revisar puertos abiertos en la máquina con Windows 7 X64



Fuente: El Autor

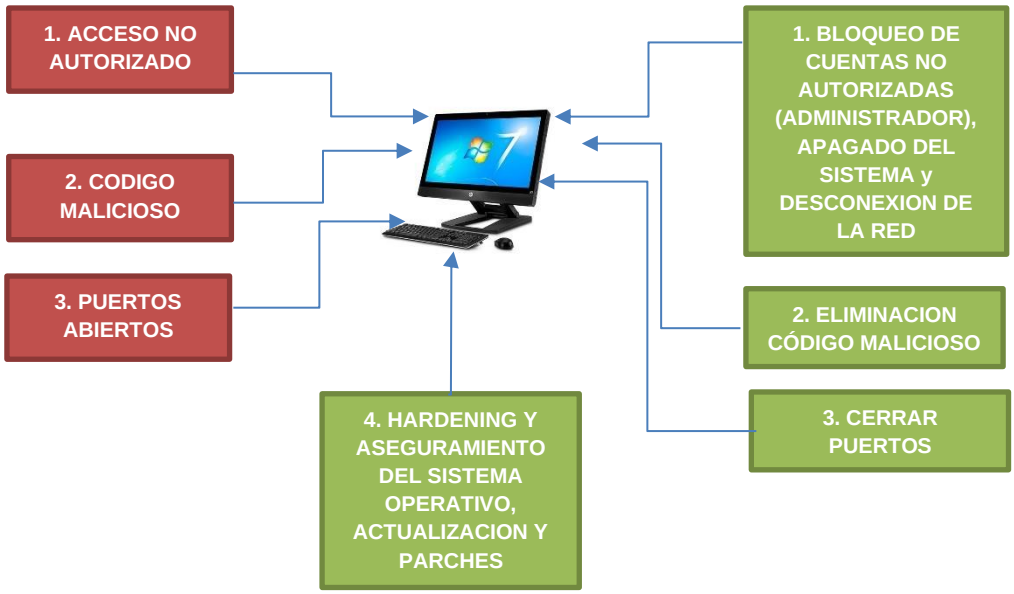
6.1.1.1.5 ESTRETEGIA DE CONTENCION

Como lo menciona la guía para contención de incidentes del MINTIC “Esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la

entidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones por ejemplo: apagar sistema, desconectar red, deshabilitar servicios"[9].

Finalmente se describe a través de una gráfica la estrategia planteada de contención al ataque en el escenario del Blue Team descrito en el escenario 4:

Figura 53: Estrategia de Contención y Hardening



Fuente: El Autor

6.1.2 ¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM QUÉ MEDIDAS DE HARDENIZACIÓN PROPONDRÍA PARA QUE EL ATAQUE NO SE REPITA?

6.1.2.1 ACTUALIZACIONES

Se recomienda de manera prioritaria las siguientes actualizaciones a las versiones más estables del sistema operativo y aplicativos que corrigen bajo el sistema Windows, que de acuerdo con el análisis de vulnerabilidades se encuentran que tanto Windows como la herramienta Rejetto v 2.3 no cuentan con las últimas versiones, lo que hace más vulnerable el sistema

[9] Mintic 2014, Gestión de Incidentes, (Pag 29), https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

6.1.2.2 ANTIVIRUS Y FIREWALL

De acuerdo con el análisis de vulnerabilidades se encuentra que el sistema no cuenta con un Antivirus instalado ni el firewall de Windows correctamente configurado, por ende se recomienda como parte del Hardening(Endurecimiento) del sistema instalar un software antivirus y configuración del firewall de Windows tanto para conexiones de entrada y de salida, dado que el ataque realizado en el escenario aprovecha y utiliza un Shell de reversa a través de conexiones salientes y no entrantes del sistema.

6.1.2.3 RECOMENDACIONES GENERALES ADICIONALES

Como parte de la protección del sistema se pueden de acuerdo con el escenario planteado aplicar las siguientes medidas de seguridad:

- Garantizar que el sistema y aplicaciones cuente con actualizaciones de software y parches de seguridad frecuentes.
- Instalación antispyware u otros softwares de seguridad perimetral
- Establecer una Política de Seguridad que brinde los lineamientos para la seguridad de la empresa y sus activos, como son creación y desactivación de usuarios, manejo de contraseñas robustas, bloqueo de cuentas de usuario por intentos fallidos, configuración de seguridad en cuanto a acceso remoto y recursos compartidos, validando la necesidad de usar la aplicación Rejetto v 2.3, la cual pese a ser actualizada puede seguir presentando problemas de seguridad, bloqueo de los puertos de unidades externas USB, entre otras que se establezcan por el equipo Blue Team para prevenir la materialización de incidentes de seguridad.
- Instalar y configurar sistemas de prevención y detección de intrusos (IPS – IDS)
- Establecer un plan de contingencia y recuperación del servicio a través de la creación y configuración de programas de respaldo (Backup)
- Asegurar el Sistema Windows 7 X64 cumpliendo y revisando los puntos de referencia de seguridad del CIS(Center for Internet Security) publicada en https://www.cisecurity.org/cis-benchmarks

6.1.4 DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

Un Equipo de Respuesta frente a Incidencias informáticos conocido como (CSIRT) es un grupo de profesionales especializados que recibe las denuncias e informes relacionados cualquier tipo de incidentes de seguridad, para luego analizarlos de acuerdo a las situaciones particulares presentadas y así tratar de responder de forma proactiva lo más rápido posible para gestionar, minimizar el impacto y recuperarse lo antes posible ante los incidentes presentados; por tanto un CSIRT o Equipo de Respuesta frente a Incidencias informáticos es un grupo de ámbito mayor establecido a nivel de Entidades, Gobiernos y empresas con funciones específicas para atender una comunidad digital dividida de forma geográfica o política, pudiendo ser parte de gobiernos, empresas, organizaciones con y sin ánimo de lucro.

Un equipo Blue Team es un equipo de profesionales expertos en seguridad informática que se establecen al interior de una organización o empresa, con el objetivo de realizar análisis de vulnerabilidades de los diferentes sistemas informáticos, como son equipos de cómputo, redes y equipos de comunicación, software y aplicaciones a través de diferentes técnicas especializadas con el ánimo de descubrir de manera preventiva las brechas de seguridad y vulnerabilidades dentro de la empresa u organización, siendo su tarea principal asegurar que dichos sistemas, redes, aplicaciones estén lo mejor protegidas contra posibles ataques.

De acuerdo a lo anterior los equipos Blue Team pueden encajar perfectamente en los equipos CSIRT, dado que tienen mucho que aportar, por los conocimientos especializados que se requieren en dichos equipos CSIRT, sin embargo son dos conceptos diferentes por la forma de establecerse y configurarse en las entidades y organizaciones.

6.1.5 ¿SI DENTRO DE UN EQUIPO BLUETEAM LE INDICAN QUE DEBE TRABAJAR CON CIS “CENTER FOR INTERNET SECURITY” USTED LO UTILIZARÍA PARA QUÉ FIN?

6.1.5.1 CIS “CENTER FOR INTERNET SECURITY”

Se usaría el módulo CIS Benchmarks de CIS “Las cuales son guías de configuración de seguridad basadas en el consenso y las mejores prácticas desarrolladas y aceptadas por el gobierno, las empresas, la industria y el mundo académico”[10].
De acuerdo con el escenario planteado en el escenario 4, se puede usar como recomendamos anteriormente para asegurar el Sistema Windows 7 X64 bits, siguiendo los puntos de referencia de CIS Benchmarks, que brindan las mejores prácticas para la configuración segura de un sistema, en este caso Windows 7 X64.

6.1.6 FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM

Un sistema de Gestión de Eventos e Información de Seguridad (en inglés: Security Information and Event Management, SIEM) es un software especializado y de alto nivel que combina y centraliza funciones de dos sistemas[11], siendo el primero un sistema de Gestión de Información de Seguridad (Security Information Management, SIM), encargado del almacenamiento a largo plazo, el análisis y la comunicación de los datos de seguridad, y el segundo un sistema de Gestión de Eventos de Seguridad (Security Event Management, SEM), encargado del monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de la consola de la información de seguridad, de tal forma que centralizan el almacenamiento y la interpretación de los datos más importantes y relevantes de la seguridad, permitiendo el análisis de la situación desde diversas localizaciones y desde un punto de vista unificado, lo que facilita la detección de tendencias y patrones no habituales en las transacciones y flujos de comunicación, esto se consigue desplegando múltiples agentes de recopilación, que recopilan datos y eventos relacionados con la seguridad[12].

---

[10] CIS(Center for Internet Security), Benchmarks™ FAQ traducido de https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq

[11] IMPLEMENTACION DE UN GESTOR DE SEGURIDAD DE LA INFORMACION Y GESTION DE EVENTOS (SIEM). Juan David Pedroza Arango. Universidad de San Buenaventura. Medellín 2016, http://bibliotecadigital.usb.edu.co/bitstream/10819/3944/1/Implementacion_Gestor_Seguridad_Pedroza_2016.pdf

[12] Gestión de eventos e información de seguridad (SIEM). Margaret Rouse. Agosto 2017, http://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

Las principales funciones y características que se pueden encontrar en un SIEM según Patricio Moreano son [13]:

6.1.6.1 FUNCIONES:

- Monitoreo de la Red en tiempo real
- Almacenar los datos de los usuarios, transacciones, etc en un repositorio de eventos
- Creación y edición de reglas operacionales para los módulos de análisis de riesgo, correlación de eventos.
- Alertas y detección de ataques gracias al Modelamiento de ataques, representación de resultados en modelos de ataques simulados, y contramedidas de selección (de ataques).
- Gerar informes detallados y el análisis sobre el estado de la Infraestructura de TI.
- Administración de los incidentes de seguridad y la administración y manejos de recursos de TI.

6.1.6.2 CARACTERISTICAS:

- Detectar los ataques, al correlacionar la actividad de los procesos y las conexiones de redes de las máquinas que están protegidas por el SIEM.
- Bloquear las amenazas a las redes, y evitar filtraciones de datos y fallo de procesos y sistemas.
- El SIEM Permite buscar las amenazas en registros archivados en el repositorio.
- El SIEM Combina tecnologías de la gestión de la seguridad de la información con la administración de eventos de seguridad.
- Permite identifica entre amenazas reales y falsos positivos.

6.1.6 3 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS HARDWARE O SOFTWARE".

6.1.6.1 OSSEC y OSSEC+ INTRUSION DETECTION SYSTEM (HIDS)

[13] Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63).
http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

La herramienta OSSEC de código abierto y la OSSEC+ que proporciona capacidades adicionales a la versión básica de OSSEC, como el sistema de aprendizaje automático, la Pila ELK, Intercambio de amenazas comunitarias en tiempo real, Miles de reglas nuevas y mucho más de forma gratuita. [14]

6.1.6.2 PACKETFENCE

PacketFence es una solución de control de acceso a la red (NAC) totalmente compatible, confiable, gratuita y de código abierto. Con un impresionante conjunto de características que incluye un portal cautivo para el registro y la reparación, gestión centralizada de VPN, inalámbrica y por cable, capacidades BYOD líderes en la industria, compatibilidad con 802.1X y RBAC, detección de anomalías de red integrada con aislamiento de capa 2 de dispositivos problemáticos; PacketFence se puede utilizar para proteger eficazmente redes heterogéneas pequeñas a muy grandes.

Lanzado bajo la GPL, PacketFence está construido utilizando componentes de código abierto confiables que le permiten ofrecer una cantidad impresionante de funciones.[15]

6.1.6.3 CONFIGSERVER SECURITY AND FIREWALL (CSF)

CSF es Un cortafuegos de inspección de paquetes con estado (SPI), aplicación de seguridad y detección de inicio de sesión/intrusos para servidores Linux, permite identificar fallas de autenticación de inicio de sesión para software de servidores Linux como Courier imap, Dovecot, uw-imap, Kerio, SSH, cPanel, WHM, Webmail (solo servidores cPanel), ftpd puro, vsftpd, Proftpd, Páginas web protegidas con contraseña (htpasswd), Fallos de Mod_security (v1 y v2), fallas de suhosin, AUTENTIFICACIÓN SMTP Exim, Errores de inicio de sesión personalizados con archivo de registro independiente y coincidencia de expresiones regulares, entre otras muchas opciones[16].

[14] OSSEC, Host Intrusion Detection for Everyone https://www.ossec.net/
[15] PacketFence, Tomado de https://www.packetfence.org/
[16] CONFIGSERVER SECURITY AND FIREWALL (CSF), https://configserver.com/configserver-security-and-firewall/

7. RECOMENDACIONES

7.1 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM

- La preparación y el conocimiento es fundamental para el desarrollo de estrategias Red Team & Blue Team, es así que resulta indispensable contar con integrantes muy bien preparados y expertos en seguridad informática, con conocimientos profundos cada uno en su campo de acción tanto para Red Team como Blue Team, siendo altamente recomendable que todo el personal cuente con certificaciones internacionales en equipos Red Team & Blue Team relacionados con la ciberseguridad.

- La experiencia es otro factor que sin duda permite crear a los equipos Red Team & Blue Team estrategias eficaces a la hora de analizar vulnerabilidades, establecer controles, detectar y contener ataques de seguridad y recuperarse ante eventualidades que se presenten en la organización.

- El apoyo de la alta gerencia a la creación y mantenimiento de equipos Red Team & Blue Team, hace que las organizaciones den un paso hacia adelante, siendo este de vital importancia para contar con el apoyo y recursos financieros de la Alta Gerencia, inversión que puede significar en un futuro el ahorro y salvaguarda económica de la organización.

- Para todo equipo Red Team & Blue Team es fundamental el conocimiento de los aspectos éticos y legales, dado que existe un límite que podría poner en una situación difícil a los equipos, por tanto toda estrategia que se implemente debe estar acompañada de un marco legal y normativo que permita la ejecución de estrategias seguras en el marco de las legislaciones vigentes.

7.1 RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN

- Toda Organización debe establecer y definir un Sistema de Gestión de Seguridad de la Información, con una Política de Seguridad clara y con un alcance bien definido que permita establecer mecanismos y controles para

mitigar los incidentes de información, a través de la identificación de los activos de información, riesgos y el tratamiento de estos.

- Se debe fortalecer la cultura organizacional de los trabajadores y empleados a través de sensibilizaciones y formación en seguridad digital, debido a que son el eslabón más débil en la cadena de la seguridad.

- Se debe tener lineamientos bien definidos para realizar actualizaciones tecnológicas tanto en software como hardware, que permitan mitigar los riesgos asociados a los activos de información.

- Brindar el apoyo desde la alta gerencia con los recursos necesarios para establecer las políticas y los equipos de seguridad como Red Team & Blue Team.

8. CONCLUSIONES

8.1 CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.

- El presente trabajo permitió ampliar los conocimientos relacionados con los equipos de seguridad, normatividad legal vigente en Colombia y la conformación de un Banco de Trabajo, que permita dar inicio con buenas bases a la realización de pruebas de seguridad en las empresa y entidades de forma organizada, siguiendo las reglamentaciones y estándares en ciberseguridad usados a nivel mundial.

- Se sienta la base como ejercicio práctico para desarrollar múltiples pruebas de seguridad a todo nivel, con las herramientas de código abierto más usadas.

- El presente trabajo permitió aclarar temas muy importantes sobre los delitos y las leyes en Colombia que legislan los delitos informáticos, además de conocer los principio y códigos de ética de los ingenieros que trabajan en las diversas organizaciones relacionadas con la seguridad informática, siendo así mismo un trabajo que permitió identificar el alcance que debe tener un integrante de una equipo Red Team & Blue Team, dado que el umbral para trasgredir y traspasar los pilares éticos y legales son muy delicados a la horas de realizar este tipo de trabajo, pudiendo cruzar fácilmente la barrera que divide el hacking Ético del Hacking tradicional.

- Gracias a los ejercicios y a las actividades se afianzaros los conocimientos relacionados con la legislación colombiana en materia de ética y leyes relacionadas con los delitos informáticos que son aplicables a los diferentes acuerdos de confidencialidad que se pueden establecer entre una empresa o entidad contratante y los expertos informáticos que llegan a trabajar como parte de los equipos Red Team & Blue Team

- Gracias a la práctica del presente trabajo se pudo recrear paso a paso un Pentesting de seguridad, en donde se afianzan los conocimientos y se crear estrategias de trabajo que permiten buscar las vulnerabilidades de una aplicación.

- El presente trabajo permitió identificar una vulnerabilidad con herramientas de software libre, herramientas de vital importancia y uso en las pruebas de seguridad, además de practicar y aprender el uso de dichas herramientas en su sintaxis y metodología.

- El conocimiento previo y el material suministrado del seminario, fue fundamental en la consecución del presente trabajo, gracias a que con ello se pudo realizar y concluir satisfactoriamente las actividades planteadas, siendo de muy valioso aporte el conocimiento adquirido durante el desarrollo del trabajo.

- Hoy en día la contención de ataques hace parte integral de los sistemas de seguridad en la empresa, por lo cual todo equipo de seguridad Blue Team, debe conocer y aplicar las mejores prácticas en contención de ataques y utilizar las herramientas disponibles, que dado el caso existen muchas herramientas de software libre que se pueden utilizar, permitiendo a todas las empresas contar con herramientas de bajo costo para la protección y detección de los ataques a los sistemas

- El conocimiento estudio y revisión previa del material suministrado del seminario, fue fundamental en la consecución del presente trabajo, gracias a que con ello se pudo realizar y concluir satisfactoriamente las preguntas planteadas, siendo de muy valioso aporte el conocimiento adquirido durante el desarrollo del trabajo.

- El presente trabajo permitió identificar un ataque y establecer las estrategias adecuadas para la contención efectiva de un ataque informático.

9. SUSTENTACION

Enlace del Video Sustentación:
https://drive.google.com/file/d/1F3B6ca2UFckYRA_kpXKD_NIaaxiNq-HK/view?usp=sharing

10. REFERENCIAS BIBLIOGRÁFICAS

SIC. (2009). Ley 1273 de 2009 (pp. 1) Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

FUNCION PUBLICA. Ley 1581 de 2012 (pp. 1) Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

SIC. (2009). Ley 1273 de 2009 (pp. 1-4) Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

COPNIA. Código de Etica para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. (pp. 1-20) Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

REVISTA SEMANA (2015). El informe que sacudió el caso de la fachada Andrómeda. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

Ethical Hacking. CÓMO USAR SEARCHSPLOIT PARA ENCONTRAR EXPLOITS(2018).Disponible en: https://blog.ehcgroup.io/2018/11/27/01/00/39/4198/como-usar-searchsploit-para-encontrar-exploits/hacking/ehacking/

Wikipedia. Metasploit(2023).Disponible en: https://es.wikipedia.org/wiki/Metasploit

Incibe. (2014). OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. INCIBE-CERT. https://www.incibe-cert.es/blog/owasp-4

REJETTO. (2018). Wiki Disponible en: https://www.rejetto.com/wiki/index.php?title=HFS:_Introducci%C3%B3n

Mintic 2014, Gestión de Incidentes, (Pag 29), https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

CIS(Center for Internet Security), Benchmarks™ FAQ traducido de https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq

IMPLEMENTACION DE UN GESTOR DE SEGURIDAD DE LA INFORMACION Y GESTION DE EVENTOS (SIEM). Juan David Pedroza Arango. Universidad de San Buenaventura. Medellín 2016, http://bibliotecadigital.usb.edu.co/bitstream/10819/3944/1/Implementacion_Gestor_Seguridad_Pedroza_2016.pdf

Gestión de eventos e información de seguridad (SIEM). Margaret Rouse. Agosto 2017, http://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

OSSEC, Host Intrusion Detection for Everyone https://www.ossec.net/

PacketFence, Tomado de https://www.packetfence.org/

CONFIGSERVER SECURITY AND FIREWALL (CSF), https://configserver.com/configserver-security-and-firewall/