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

SEILER SALAS LAGARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Barrancabermeja
2022

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

SEILER SALAS LAGARES

Nombre
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Barrancabermeja
2022

1 RESUMEN

El presente documento contiene cada uno de los escenarios previstos etapa por etapa del seminario de Ciberseguridad Red team y Blue team los cuales permiten conocer el modo de operación de cada uno de estos equipos para que según ello se puedan analizar y presentar sugerencias y soluciones a un problema planteado. El primer escenario propuesto indica realizar el montaje del banco de trabajo donde se instalen las máquinas virtuales de Windows y Linux para la ejecución de las pruebas tendientes de cada etapa, de igual forma el tratamiento de los aspectos legales que componen la ley colombiana como la 1273 y la 1581; también incluye la definición de las fases que compone la prueba de penetración. El escenario 2 propone la realización del análisis legal del contrato de reclutamiento para los equipos de red y blue team esto con el fin de hallar falencias en la elaboración del documento las cuales pudiesen desencadenar en líos con la justicia aparte de estar inmersa las implicaciones éticas que esto trae como consecuencia de un mal proceder. El escenario 3 solicita analizar una posible fuga de información que se puede estar presentando a través de una maquina con Windows 7 en esta fase se evalúa la posible vulnerabilidad de la aplicación rejetto y si esta existe realizar la vulneración. En el escenario 4 se requiere la contención del ataque que se estaba ejecutando en el escenario anterior, analizar la red con una herramienta GPL ya que la entidad no dispone de recursos, en esta fase se busca poder encontrar el medio por el cual se está realizando el ataque y detenerlo, además de proponer medidas de hardenización o endurecimiento del sistema operativo para prevenir futuros ataques. Por último, el escenario 5 propone la recopilación de todas las fases y la realización de un informe técnico para la organización The WhiteHose Security.

CONTENIDO

pág.

1 RESUMEN....2

2 GLOSARIO....3

3 INTRODUCCIÓN....5

4 OBJETIVOs....6

5 DESARROLLO DEL TRABAJO....7

5.1 Desarrollo escenario 1....9

5.1.1 Configuración del banco de trabajo....9

5.1.2 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.....12

5.1.3 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.....14

5.1.4 Definir y explicar las siguientes herramientas:....15

5.2 Desarrollo del escenario 2....16

5.2.1 Como consecuencia del análisis realizado de la información suministrada inicialmente se describirán los aspectos legales en los que pueden incurrir como delito derivado de la suscripción del contrato y posteriormente los éticos.....16

5.2.2 Análisis de los anexos, en relación a la vulneración de la ley 1273 argumentando cualquier proceso ilegal.....20

5.2.3 Análisis de la propuesta laboral, teniendo presente en cuenta la revisión desde el punto de vista legal y ético....21

5.3 Desarrollo del escenario 3....22

5.3.1 Describa de manera específica las herramientas software que....22

5.4 Desarrollo del escenario 4....33

5.4.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.....38

5.4.2 ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?....39

5.4.3 ¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?....40

5.4.4 ¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?....41

5.4.5 Explique y redacte las funciones y características principales de lo que es un SIEM.....42

5.4.6 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. 43

6 Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam. ***45***

7 Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización. ***46***

8 Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad. ***48***

9 BIBLIOGRAFÍA ***49***

2 GLOSARIO

Máquina Virtual: Software que simula un sistema de cómputo, en este puede operar cualquier sistema operativo como si fuese una maquina real.

Red Team: Equipo encargado de simular ataques informáticos a una organización con el fin de encontrar vulnerabilidades en sus sistemas.

Blue Team: Equipo encargado de contener los posibles ataques que pueda presentar su organización con el fin de proteger los activos de este.

Ciberseguridad: El área de la informática encargada de la protección de la infraestructura computacional.

Vulnerabilidad: Debilidad existente en cualquier sistema que puede ser utilizada por cualquier persona malintencionada con el fin de afectar los servicios.

GPL: Licencia pública general, licencia de software libre y código abierto.

Metasploit:[1] Es una herramienta para crear y accionar exploits contra un equipo remoto, realizando así verificación y auditoría de la seguridad del sistema atacado con el fin de descubrir vulnerabilidades comúnmente utilizado por administradores de sistemas informáticos con el fin de protegerlos o de piratas informáticos para atacarlos. Es muy práctico debido a que cualquiera sea su intención esta herramienta permite la creación de todo tipo y variaciones de exploits.

Nmap:[2] Mapeador de redes, es una herramienta de código abierto diseñada para la exploración de redes y auditorias de seguridad. Es utilizada para el análisis expreso de grandes redes, aunque se puede usar específicamente hacía algún equipo utilizando la IP de esta manera funciona muy bien. En su análisis muestra gran cantidad de información como los equipos que están disponibles, con nombre y versión de la aplicación, puertos usados, cerrados abiertos, etc.

[1] Qué es Metasploit. https://openwebinars.net/blog/que-es-metasploit/
[2] Nmap Network Scanning. https://nmap.org/man/es/index.html#man-description

ExploitDB: como su nombre lo indica es una base de datos o directorio web de exploits, en este se publican todo tipo de vulnerabilidades con instrucciones claras de cómo usarlas y aprovecharlas.

CVE: Vulnerabilidades y exposiciones comunes es un listado el cual se expone públicamente las vulnerabilidades y exposiciones de seguridad las cuales se categorizan en software y firmware y con un identificador o código para que sea más fácil su búsqueda, estas falencias son aportadas por muchos administradores y especialistas los cuales a su vez generan una serie de opciones para las posibles soluciones. En ocasiones el mismo proveedor las reconoce, documenta y soluciona. Es una organización sin ánimo de lucro liderada por MITRE.

3 INTRODUCCIÓN.

El informe técnico sobre el seminario de especialización generado en este documento mostrará el concepto, el objeto las funciones y los procedimientos del funcionamiento de los equipos de blue team y red team basados en un ejercicio práctico el cual evidenciará como operan estos dos equipos, uno de forma ofensiva y el otro defensiva, además de mostrar distintas alternativas y soluciones al problema, se busca que la organización conozca de forma clara y precisa como se ejecutan estos ataques, cuáles son las vulnerabilidades, como resolverlas como protegerse y reconozcan la importancia de mantener un buen equipo que trabaje mancomunadamente en pro de la organización con el fin de reducir los riesgos de posibles ataques o futuras amenazas. Esto sin dejar a un lado las organizaciones internacionales que apoyan a las distintas personas entidades u organizaciones del orden público o privado a que mejoren sus procesos internamente esto con el objetivo de aumentar el nivel de su seguridad, la experiencia de esta es muy importante ya que cuentan con personal capacitado que continuamente actualizan sus procesos y sus desarrollos compartiéndola con toda la comunidad.

4 OBJETIVOS

OBJETIVO GENERAL

Desarrollar el informe final gerencial con los escenarios propuestos a lo largo del seminario de seguridad informática con el fin de brindar algunas alternativas a un problema específico.

OBJETIVOS ESPECÍFICOS

Elaborar un informé técnico teniendo en cuenta los eventos más importantes desarrollados en cada uno de los escenarios

Realizar las recomendaciones pertinentes para la solución del problema de seguridad teniendo en cuenta los procedimientos documentados por los equipos de blue team y las organizaciones internacionales como la CIS.

5 DESARROLLO DEL TRABAJO

INFORME TÉCNICO

El documento es construido teniendo en cuenta cada uno de los escenarios propuestos en el seminario es por esto que se describirá cada uno de estos a continuación con el objeto de crear un contexto de la situación y se pueda desarrollar este de una forma comprensible.

Escenario 1.

Situación problema: Montaje banco de trabajo

The Whitehouse Security requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de The WhiteHouse Security. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.
De manera simultánea The WhiteHouse security requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

Escenario 2.

Situación problema: Análisis legal

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

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

Escenario 3.

Situación problema: Análisis Red team.

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. 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 llamada rejetto v. 2.3 bajo un Windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Dentro de la investigación también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema. El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

Escenario 4

Situación problema: Análisis Blue team

WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en

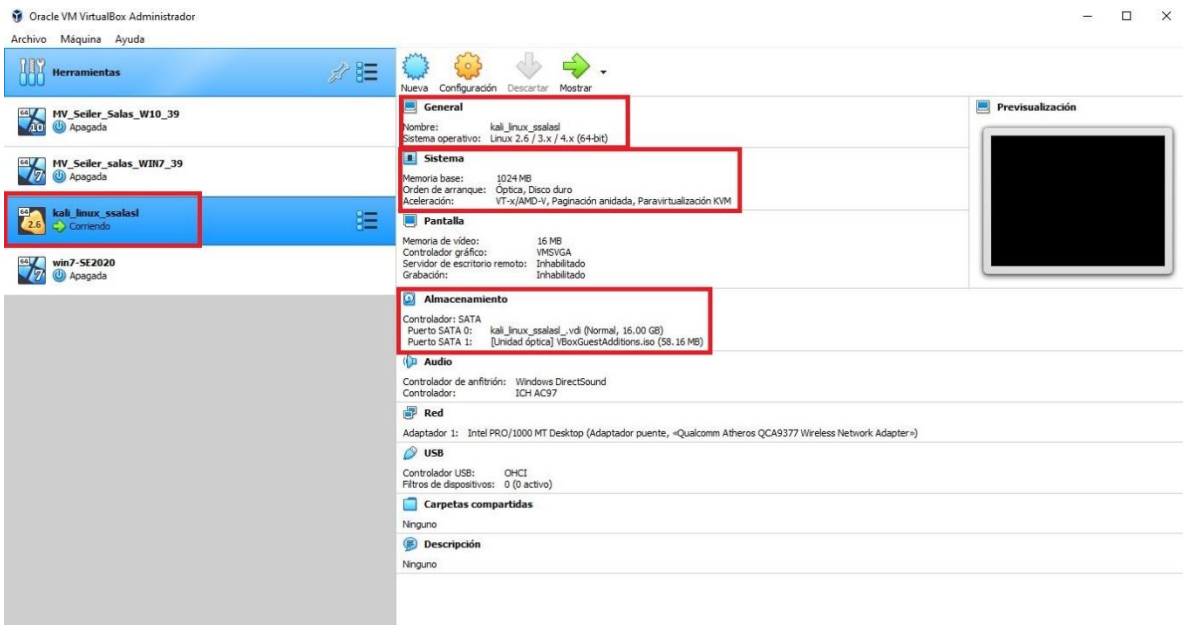
tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", con la información recolectada se espera que dentro de su grado de experticia usted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

5.1 DESARROLLO ESCENARIO 1

5.1.1 Configuración del banco de trabajo

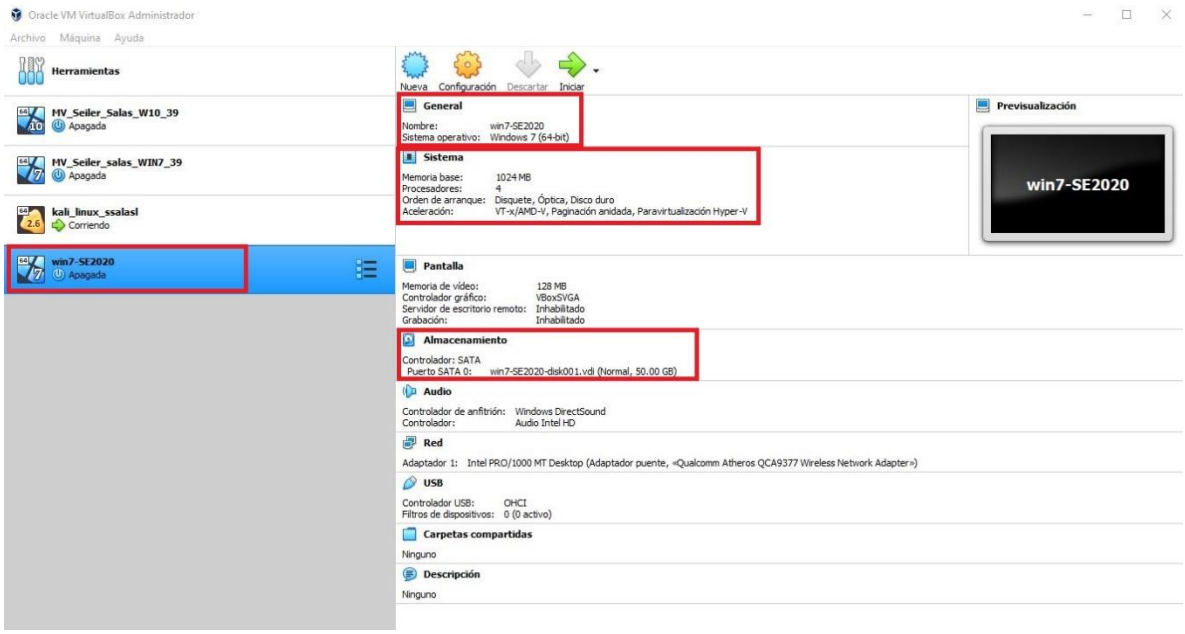
Para el desarrollo de este escenario es necesario la configuración de las dos máquinas virtuales tanto de Linux como de Windows en las cuales se desarrollarán las prácticas y se debe comprobar que haya conexión entre ambas.

Imagen 1. Características técnicas Maquina Kali



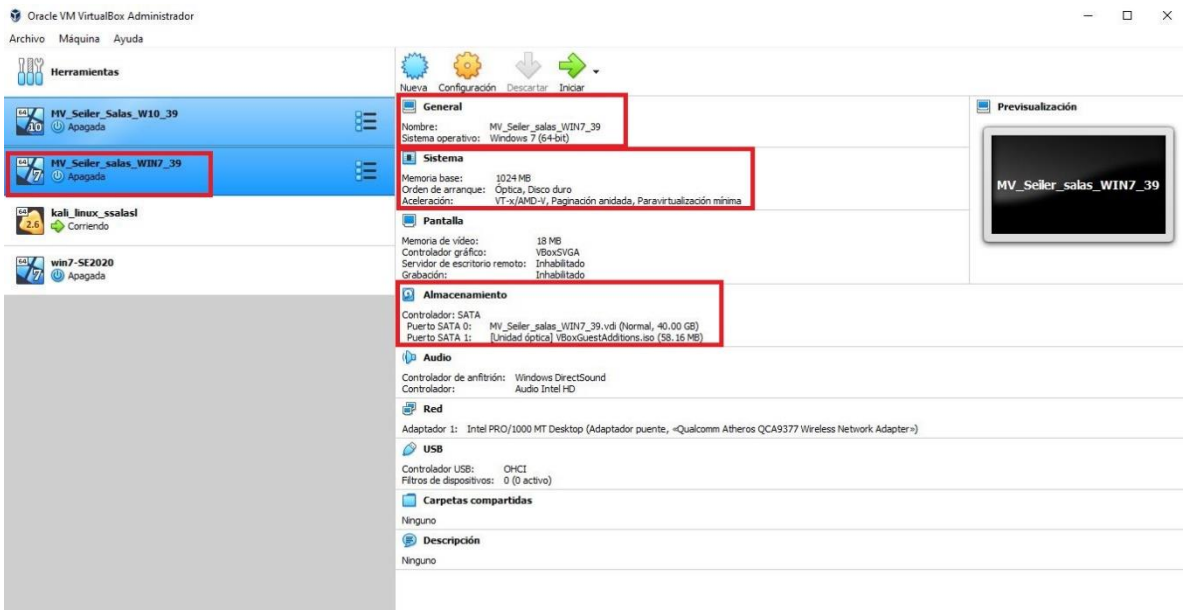
Fuente: Autor

Imagen 2. Características técnicas Maquina Windows 32B



Fuente: Autor

Imagen 3. Características técnicas Maquina Windows 64B



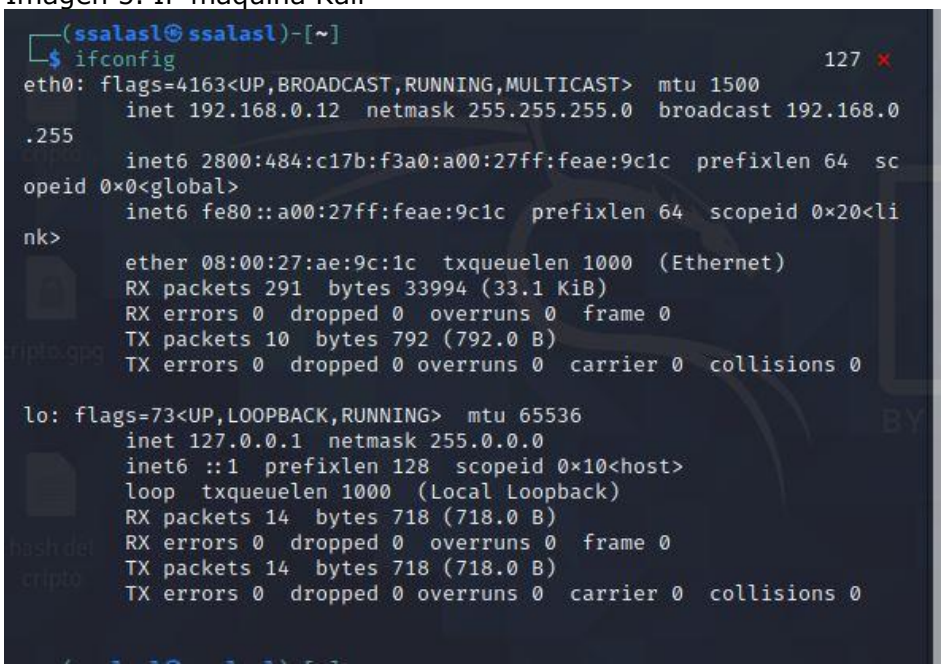
Fuente: Autor

Ping entre máquinas.

Imagen 4. IP máquina Windows

Fuente: Autor

Imagen 5. IP máquina Kali

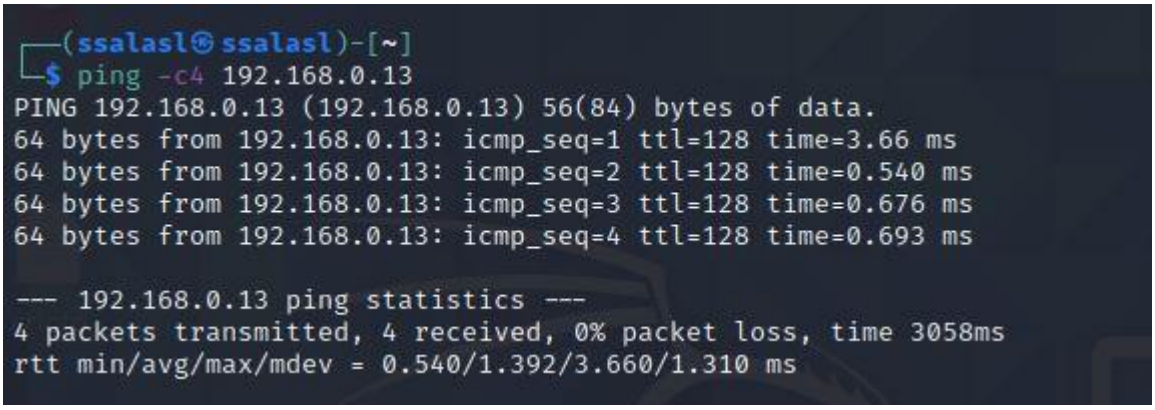


Fuente: Autor

Imagen 6. Ping Windows a Kali

Fuente: Autor

Imagen 7. Ping Kali a Windows



Fuente: Autor

5.1.2 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.

Existe la ley 1273 del 05 de enero del 2009 el cual busca la protección de la información y de los datos y también la preservación integral de los sistemas que utilicen las tecnologías de la información.
Este comprende 2 capítulos el primero trata temas sobre ataques contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos y datos. El cual comprende 8 Artículos descritos a continuación los cuales tienen en su mayoría el mismo tipo de sanción

económica y en tiempo dependiendo de la gravedad, esta va desde de 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos. Y el segundo capítulo de los atentados informáticos y otras infracciones.

LEY ESTATUTARIA 1581 DE 2012

La ley de tratamiento de datos.

Esta en su primer artículo define el objeto de la ley en la cual se define que por derecho constitucional que tienen todos a conocer, actualizar y rectificar los datos recopilados sobre cada uno de ellos en las distintas bases de datos o ficheros, y demás derechos y garantías que se refiera en el artículo 15 de la constitución.
Las disposiciones y principios estipulados en esta ley serán aplicables a cualquiera de los datos personales incluidos en cualquier base de datos susceptibles al tratamiento de estos sea entidad privada o pública.
No será aplicable a:
Bases de datos o archivos de uso exclusivo domestico o personal.
Bases de datos con finalidad de defensa nacional o seguridad, así como las que usan para el control de lavados de activos o financiamiento del terrorismo.
Bases de datos con finalidad de obtener información de inteligencia y contrainteligencia
Bases de datos y archivos con información de contenidos editoriales y periodísticas.

En conclusión, está ley define todos los parámetros bajo los cuales se puede dar tratamiento a la información del ciudadano en búsqueda también de proteger sus derechos al no revelar información sensible sin su previa autorización que pueda afectar a este.

5.1.3 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.

Para realizar un pentesting hay que tener clara cada una de las fases que se describen a continuación:

1. Reconocimiento
2. Análisis de vulnerabilidades
3. Explotación
4. Informes

1. Reconocimiento: Es la fase inicial donde se recopila la información de la organización con miras a que acciones tomar y el tipo de pentesting realizar, todo esto con el aval del cliente que generalmente es el que determina el tipo de información puede suministrar.

2. Análisis de vulnerabilidades: Se utilizan distintas herramientas para verificar el estado del sistema mediante el cual puedan descubrir puertos abiertos, fallos de fabricación de algún software o configuraciones por defecto o deficiente, se pueden utilizar herramientas como OWASP, Nmap, Nessus o CVEs.

3. Explotación: Se ejecutan acciones de ataques para comprometer el sistema teniendo en cuenta los hallazgos encontrados en el análisis de vulnerabilidades, se pueden realizar inyección de código, inserción de ficheros, evasión de autenticación, denegación de servicios etc.

4. Informes: en este se describe el impacto que causan las fallas de seguridad en el sistema atacado, presentándolo a manera de resumen informativo donde se incluyan todas las falencias encontradas y las posibles consecuencias, así como las recomendaciones para minimizarlas o eliminarlas.

Una de las muchas herramientas que se puede utilizar como ejemplo para test de penetración es **OWASP ZAP**, esta permite interceptar tráfico de un sitio web para analizarlo y modificarlo si es necesario, esto se realiza a través de escaneos automáticos o en búsqueda de una vulnerabilidad especifica.

5.1.4 Definir y explicar las siguientes herramientas:

- **Metasploit**:[3] Es una herramienta para crear y accionar exploits contra un equipo remoto, realizando así verificación y auditoría de la seguridad del sistema atacado con el fin de descubrir vulnerabilidades comúnmente utilizado por administradores de sistemas informáticos con el fin de protegerlos o de piratas informáticos para atacarlos. Es muy práctico debido a que cualquiera sea su intención esta herramienta permite la creación de todo tipo y variaciones de exploits.

- **Nmap:**[4] Mapeador de redes, es una herramienta de código abierto diseñada para la exploración de redes y auditorias de seguridad. Es utilizada para el análisis expreso de grandes redes, aunque se puede usar específicamente hacía algún equipo utilizando la IP de esta manera funciona muy bien. En su análisis muestra gran cantidad de información como los equipos que están disponibles, con nombre y versión de la aplicación, puertos usados, cerrados abiertos, etc.

- **OpenVas** : Es un escáner de vulnerabilidades muy completo compuesto por distintos tipos de pruebas incluyendo autenticadas y no autenticadas, estas se pueden usar de forma individual o en conjunto, su interface permite el uso por línea de comandos o una web utilizando dos servicios uno Manager y el otro Scanner uno filtra y clasifica los resultados del análisis y control de base de datos y el otro realiza las pruebas de vulnerabilidad de red mediante rutinas que puedan identificar problemas de seguridad sean ya conocidos o potenciales amenazas.

[3] Qué es Metasploit. https://openwebinars.net/blog/que-es-metasploit/
[4] Nmap Network Scanning. https://nmap.org/man/es/index.html#man-description

Servicios en línea:

- **ExploitDB**: como su nombre lo indica es una base de datos o directorio web de exploits, en este se publican todo tipo de vulnerabilidades con instrucciones claras de cómo usarlas y aprovecharlas.
- **CVE:** Vulnerabilidades y exposiciones comunes es un listado el cual se expone públicamente las vulnerabilidades y exposiciones de seguridad las cuales se categorizan en software y firmware y con un identificador o código para que sea más fácil su búsqueda, estas falencias son aportadas por muchos administradores y especialistas los cuales a su vez generan una serie de opciones para las posibles soluciones. En ocasiones el mismo proveedor las reconoce, documenta y soluciona. Es una organización sin ánimo de lucro liderada por MITRE.

5.2 DESARROLLO DEL ESCENARIO 2

Análisis de los anexos Escenario 2 y Acuerdo desde el punto de vista legal y no ético.

5.2.1 Como consecuencia del análisis realizado de la información suministrada inicialmente se describirán los aspectos legales en los que pueden incurrir como delito derivado de la suscripción del contrato y posteriormente los éticos.

- La primera irregularidad se puede determinar en la **segunda clausula**

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

Sobre esto se puede evidenciar que existe una falta puesto que indican tratamiento de datos obtenidos de forma irregular como chuzadas,

interceptaciones y accesos abusivos y esto contraviene el artículo[5] 1519 del código civil Objeto ilícito por el cual describe que hay un objeto ilícito en todo lo que contraviene al derecho público de la nación. Ya que las partes no pueden hacer acuerdos sobre un objeto ilícito.

- **En la cuarta clausula** donde se obliga a la parte receptora a asumir algunas consideraciones bastante dudosas la ley del código civil colombiano en el artículo[6] 1502 Requisitos para obligarse.

Para que una persona se obligue a otra por un acto o declaración de voluntad, es necesario:

1o.) que sea legalmente capaz.

2o.) que consienta en dicho acto o declaración y su consentimiento no adolezca de vicio.

3o.) que recaiga sobre un objeto lícito.
4o.) que tenga una causa lícita.

En consecuencia, estaría en clara violación a este artículo ya que se manifiesta sobre acciones ilícitas a las cuales incurriría la parte receptora en cumplimiento del contrato.

- Dentro de esta misma clausula los numerales 3 y 4

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

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

Son violaciones claras al código de procedimiento penal en su **artículo 67** denominado **Deber de denunciar**. El cual indica que: Toda persona

[5] https://leyes.co/codigo_civil/1519.htm
[6] https://leyes.co/codigo_civil/1502.htm

debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento y que deban investigarse de oficio.[7]

Estos numerales también comprometen éticamente las directrices del consejo profesional nacional de ingeniería (COPNIA) en su capítulo II de los deberes y obligaciones de los profesionales en su apartado F, donde estipula que debe denunciar los delitos, contravenciones y faltas contra este Código de ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder[8].

- Continuando con la misma clausula en su numeral 7 indica que debe

"***responder por el mal uso que le den sus representantes a la información confidencial"***

En términos de responsabilidad contractual y conforme al régimen de obligaciones del código civil, en este caso estaríamos ante una obligación que es imposible de cumplir por parte del contratista, ya que se trata de una responsabilidad que está en cabeza de otra persona. El contratista no puede entrar a responder por la conducta dolosa o culposa del contratante. Esta es regulada en el artículo 63 del código civil. El articulo debe eliminarse.

- Numeral 8

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

En este artículo se le atribuye al contratista una responsabilidad que está en manos del contratante, quien que es el dueño de la información. De igual manera este articulo debe considerar que al momento de establecerse una responsabilidad contractual la misma debe analizarse teniendo en cuenta el concepto de dolo y culpa en el comportamiento

[7] https://leyes.co/codigo_de_procedimiento_penal/67.htm
[8] https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

exigido al individuo, y en todo caso la responsabilidad en la generación de un daño y los perjuicios causados debe probarse.

- Numeral 9

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

Este numeral viola el artículo 1502 sobre los requisitos para obligarse, jurídica y éticamente está en deber de denunciar y divulgar cualquier ilícito

- En la **cláusula Quinta** habla sobre las obligaciones de la parte reveladora e indica que debe ***"mantener la reserva de la información confidencial hasta tanto"*** está incompleto y no determina el periodo causal por el cual se deba mantener la discreción como lo define al **artículo 1551** del código civil el cual menciona la definición de plazo: [9]***El plazo es la época que se fija para el cumplimiento de la obligación; puede ser expreso o tácito. Es tácito, el indispensable para cumplirlo.***

Dentro del contrato no está descrita o estipulada la cláusula **séptima**, se salta de la **sexta** a la **octava.**

- **Clausula octava: Solución de controversias**

"En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security."

[9] https://leyes.co/codigo_civil/1551.htm

Va en contra del ordenamiento jurídico ya que en la responsabilidad se debe valorar la conducta del individuo y probarse los daños causados por lo que no es posible establecer que va a quedar exenta de una responsabilidad legal y penal en todo caso debe ser sujeto a las instancias judiciales o acudir a la vía de la conciliación o mecanismos alternos de resolución de conflictos.

También se debe precisar responsabilidad sobre la información en que etapa, si durante el cumplimiento del objeto contractual o posterior a este

No se puede obligar a que sea un abogado privado hay entidades que prestan el servicio de manera gratuita y se considera desfavorable al obligarlo a requerir estos servicios.

Al suscribir este contrato el profesional que hace de la parte receptora estaría incurriendo en una falta gravísima a la ética y los valores que rige el código de ética que precisamente busca propender que se actúe con honestidad y compromiso en aras de brindar a los ciudadanos garantía de ejercer la profesión con ética.
Indistintamente el profesional se encuentra en la capacidad de tomar la decisión acertada independiente de ser esta buena o mala, todo depende de la formación en principios y valores que haya recibido esta persona, pero con el análisis realizado y evidenciando tantas falencias estaría expuesto a recibir duras sanciones en caso de verse involucrado en cualquier hecho doloso.

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

Luego del análisis realizado se puede determinar clara violación a 3 de los artículos de la ley 1273 enumerado a continuación:

ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.
ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFOMÁTICOS.
ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES.

El artículo **269A y 269C** se ven vulnerados en la cláusula 2 numeral 2 del acuerdo ya que en estos menciona que se debe mantener confidencialidad

por la parte receptora de los datos obtenidos de cualquier índole mediante **acceso abusivo a sistemas informáticos e interceptación de información "chuzadas".** Si bien la mayor parte de esta información es suministrada por la parte reveladora, específicamente en este numeral indica que el receptor podrá tener acceso por cualquier medio en virtud de reuniones sostenidas.

El artículo **269F** se ve vulnerado en la cláusula 4 numeral 3 donde señala no denunciar apropiación de información de terceros en este caso estaría obteniendo datos de otras personas para beneficio propio realizando la violación de datos personales con objeto de cumplir sus funciones o el contrato con la empresa reveladora.

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

Tal y como está actualmente el acuerdo no es viable aceptar la propuesta, aunque económica y laboralmente es tentadora debido a que va en contravención de lo legal y lo ético, tiene demasiados vacíos e inconsistencias que podrían desencadenar a mediano o largo plazo estar involucrado en un proceso jurídico que pueda llevar a cumplir algún tipo de condena ya que incluso sugieren responsabilidades por acciones de las cuales no se tiene control. Ahora desde el ámbito ético faltaría a la razón principal del código que es actuar con compromiso y honestidad para dignificar la profesión y brindar garantías a los ciudadanos desde nuestra profesión.
Dentro de los deberes como profesionales está en custodiar debidamente la información que se nos haya suministrado impidiendo ocultamiento o uso indebido y esto se manifiesta de forma tácita en varios de los numerales contenidos en el acuerdo en uno exclusivamente se prohíbe publicar o divulgar información ilegal. Otra de las causas es que llegaría a ser cómplice del actuar de la empresa ya que se pide abstener de denunciar actos ilegales o sospechosas siendo este uno de los deberes estipulados en el código de ética, con esto se incurriría en una de las prohibiciones generales de los profesionales que es permitir o facilitar el ejercicio ilegal. Estas contravenciones están incluidas dentro de las faltas gravísimas al ejercicio de la profesión por lo cual se estaría propenso a suspensión o cancelación de la matrícula profesional de acuerdo a la falta. Teniendo en cuenta todas estas falencias encontradas es preferible

trabajar dignamente por un sueldo menor y sin estabilidad contractual que verse inmerso en situaciones judiciales que pueden afectar el buen nombre y trabajo realizado a lo largo de la profesión.

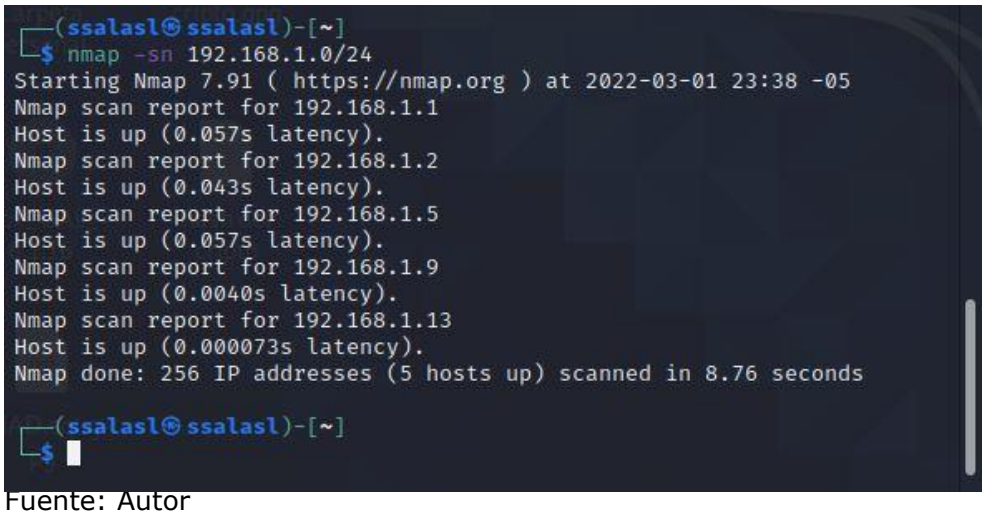
5.3 DESARROLLO DEL ESCENARIO 3

En este escenario se analiza la maquina por la cual se cree existe la fuga de información una con sistema operativo Windows 7 de 64bits y una aplicación que se está usando actualmente llamada rejetto.

5.3.1 Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Red team. 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.

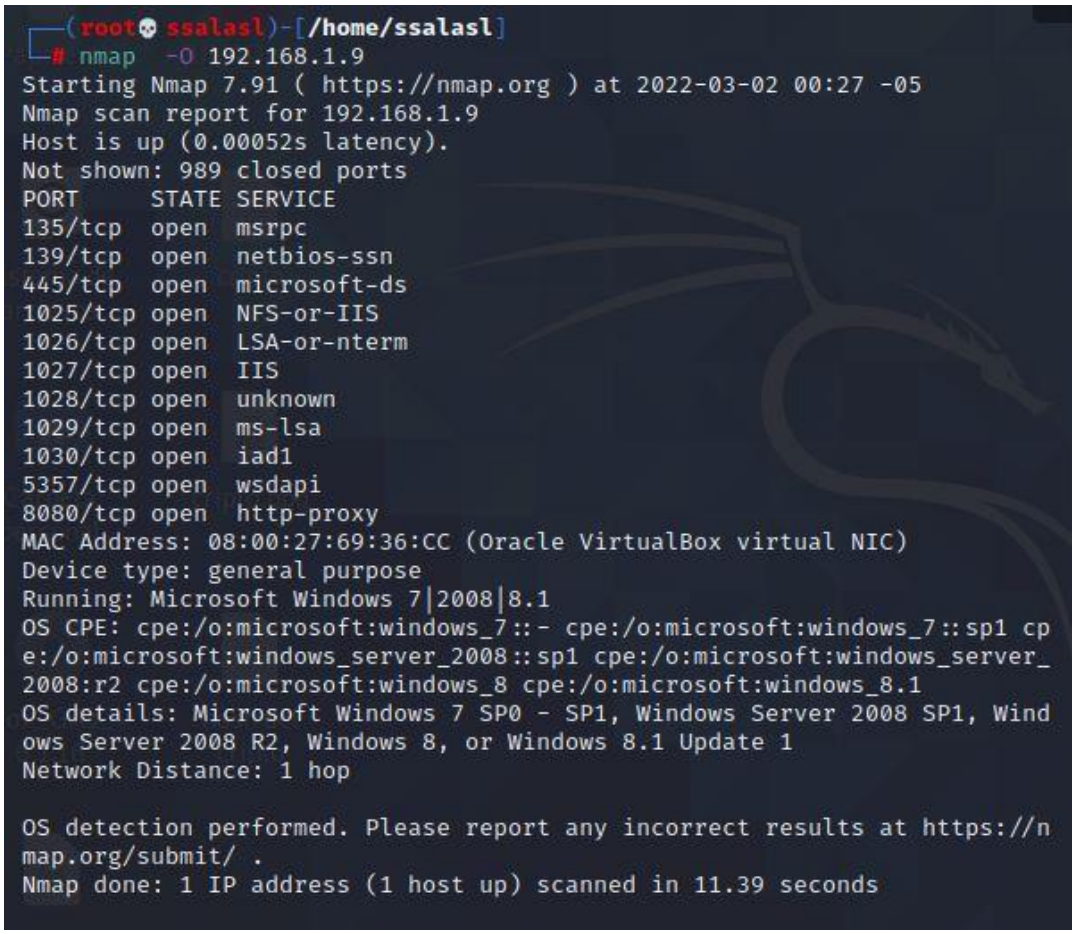
Las pruebas realizadas básicamente fueron realizadas bajo la distribución de Kali Linux, principalmente el Nmap y Exploit Framework. Para cada una de las etapas del pentesting fueron importantes y necesarias, inicialmente en la primera parte de recolección de información activa fue usado Nmap para ver las máquinas disponibles y dentro de estas el posible objetivo. La siguiente imagen muestra la ejecución de la herramienta mediante el comando **nmap -sn 192.168.1.0/24** con esto lo que se busca es que se realice un rastreo de los hosts disponibles dentro de todo el rango de red sin que se muestren los puertos.

Imagen 8. Escaneo de host disponibles



Fuente: Autor

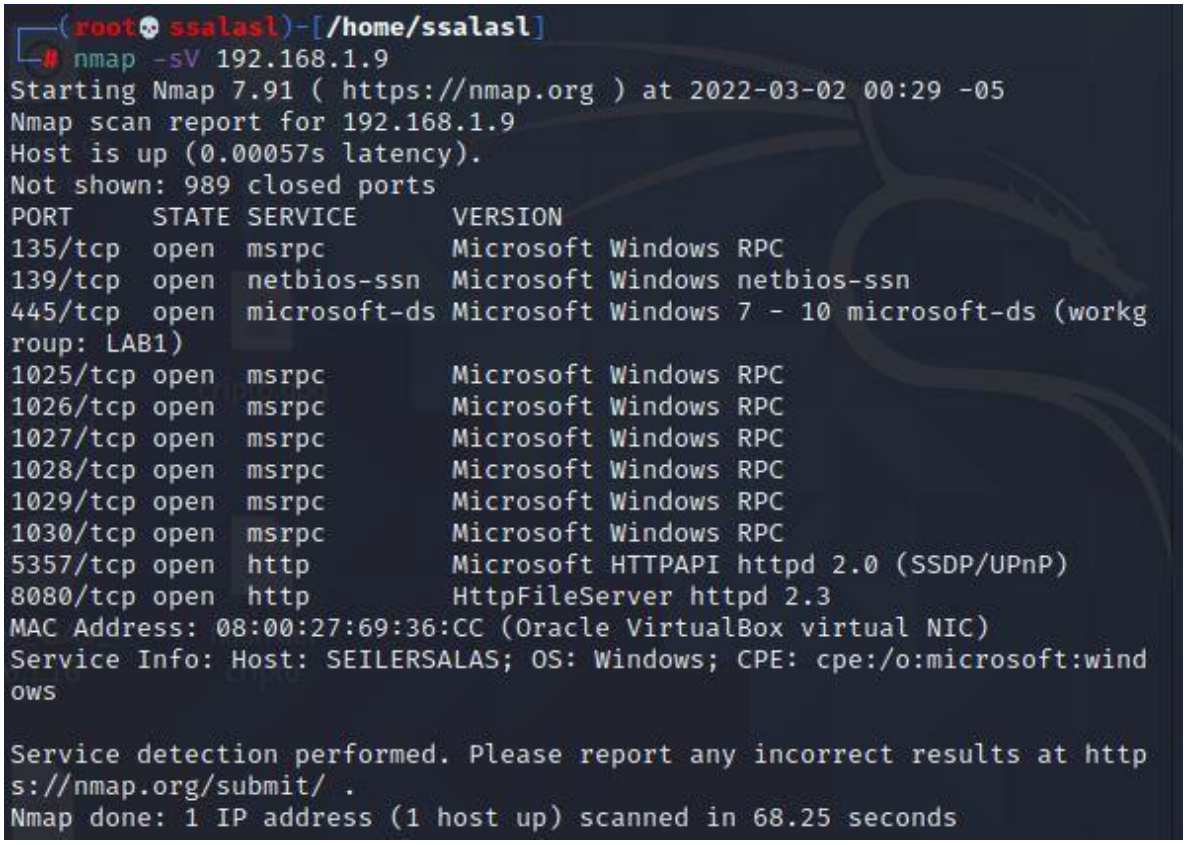
Imagen 9. Identificación del S.O del host objetivo



Fuente: Autor

En la imagen 8 se pudo ver los hosts disponibles y el objetivo que es la maquina con IP 192.168.1.9 por lo cual con el comando **nmap -o 192.168.1.9** como lo nuestra la imagen 2 podemos ver el sistema operativo de esta que es Windows 7, adicional a esto muestra algunos servicios y puertos disponibles.

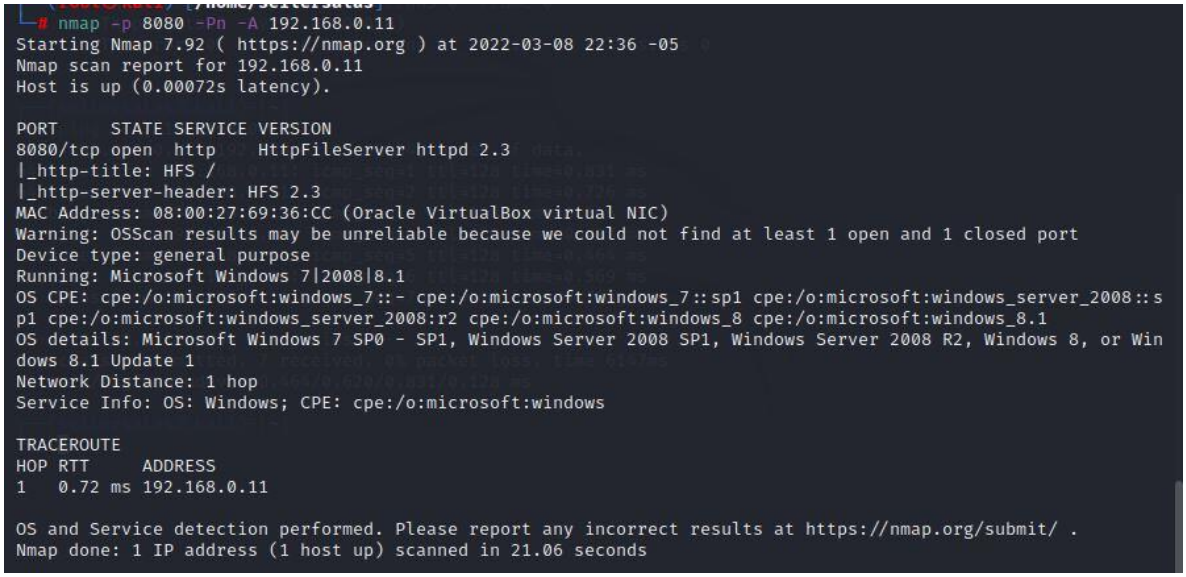
Imagen 10. Búsqueda de puertos y versión



Fuente: Autor

Mediante el comando **nmap -sV 192.168.1.9** se puede ver además de los puertos disponibles el estado, el tipo de servicio y la versión de estos como lo muestra la imagen 10.

Imagen 11. Verificación de puerto sospechoso

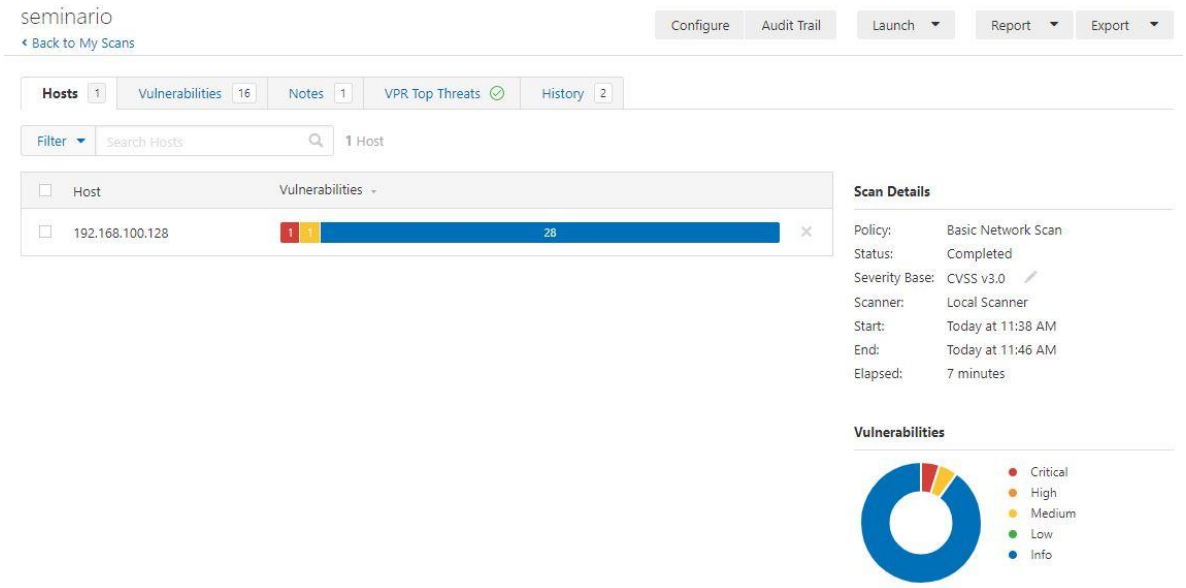


Fuente: Autor

En la imagen 10 se pudieron verificar los puertos disponibles, de estos llama la atención el 8080 en el cual se está ejecutando un servicio para transferencia de archivos y mediante el comando **nmap -p 8080 -Pn -A 192.168.0.11** se puede constatar que el puerto está abierto, disponible y ejecutando la aplicación.

- La siguiente fase de análisis de vulnerabilidades y enumeración se usó la herramienta Nessus de tenable mediante la cual se realizó una búsqueda en el host determinado para encontrar vulnerabilidades que pueda presentar el sistema operativo somo sus aplicaciones

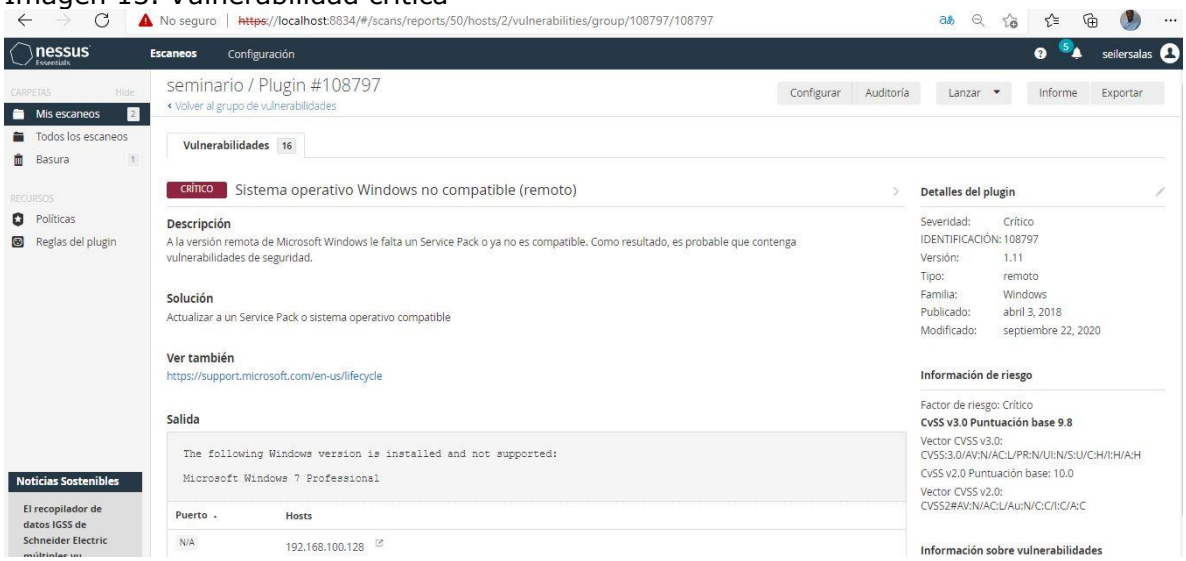
Imagen 12. Análisis con Nessus



Fuente: Autor

Dentro del análisis se pudieron hallar 16 tipos de vulnerabilidades de las cuales 2 requerían atención 1 de esta crítica.

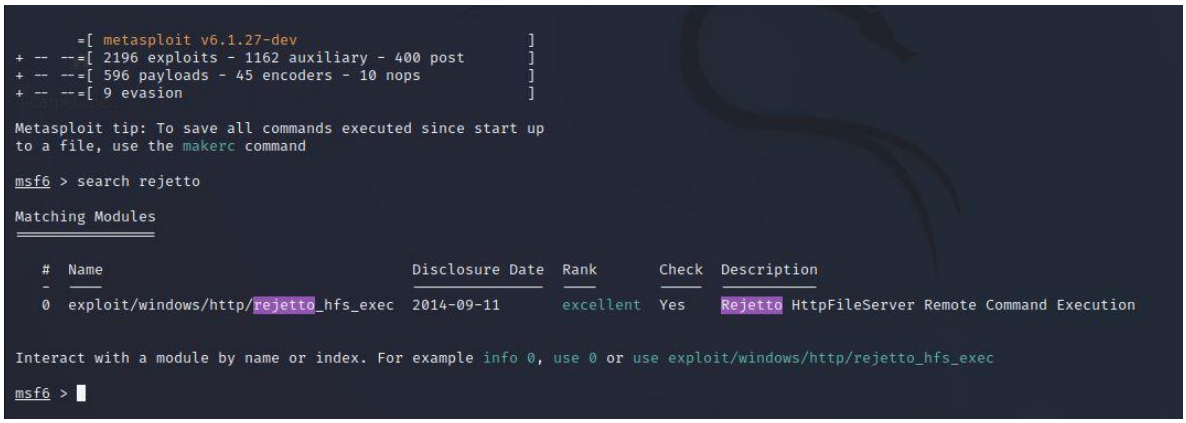
Imagen 13. Vulnerabilidad crítica



Fuente: Autor

Luego de una consulta en internet sobre las posibles vulnerabilidades se encontró que HttpFileServer se podría realizar un ataque con un exploit de la herramienta metasploit framework de Kali Linux. Por lo que a continuación se describirá el proceso.

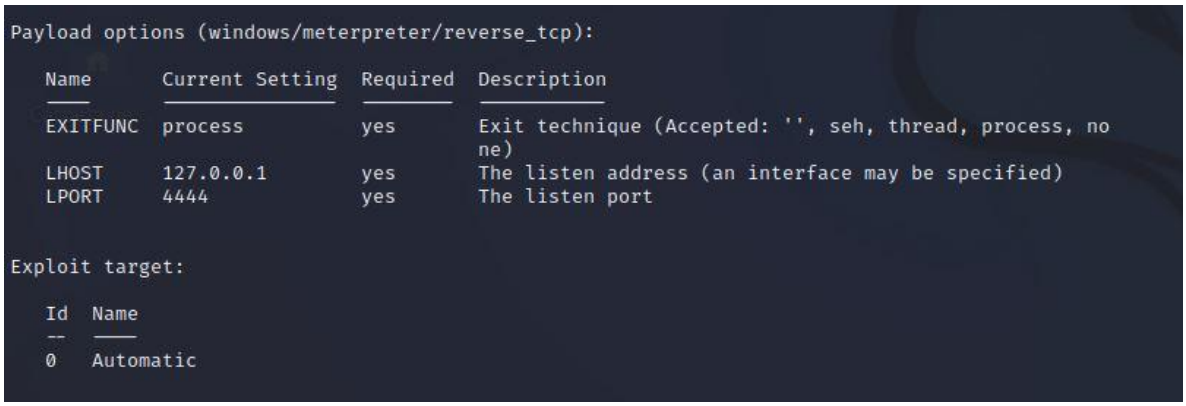
Imagen 14. Ejecución de metasploit



Fuente: Autor

Esta herramienta permite realizar búsquedas sobre vulnerabilidades de todos los sistemas operativos, en este caso con solo colocar Rejetto trae la explotación lista para ejecutar.

Imagen 15. Objetivos disponibles



Fuente: Autor

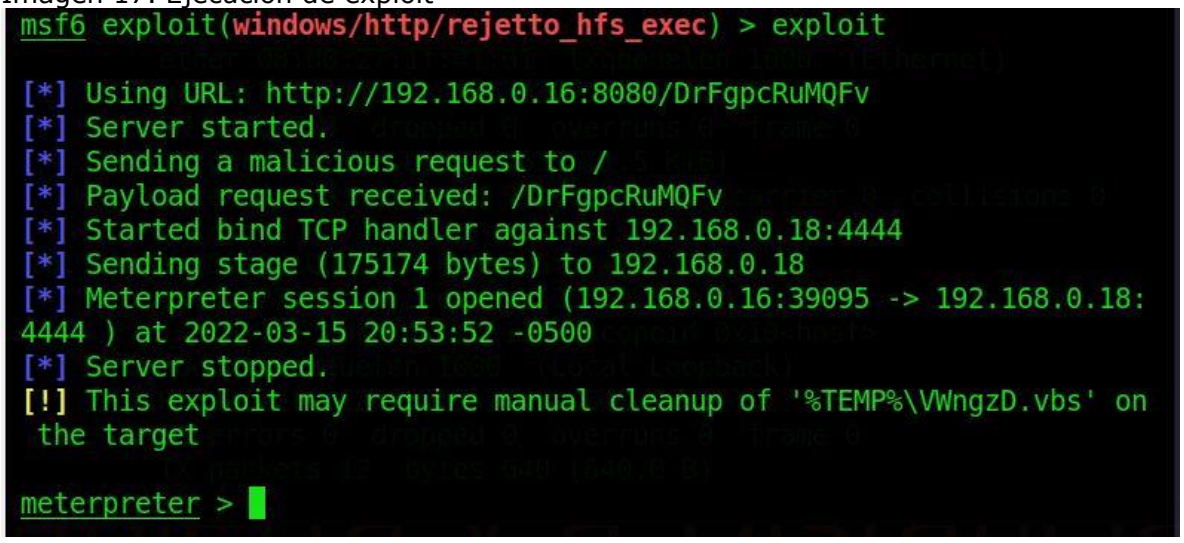
Luego de esto configuramos el equipo victima IP 192.168.0.18 y equipo atacante 192.168.0.16.

Imagen 16. Configuración de las máquinas para el ataque

Fuente: Autor

Posterior a esto se ejecuta el exploit y se envía el script malicioso para acceder a la máquina.

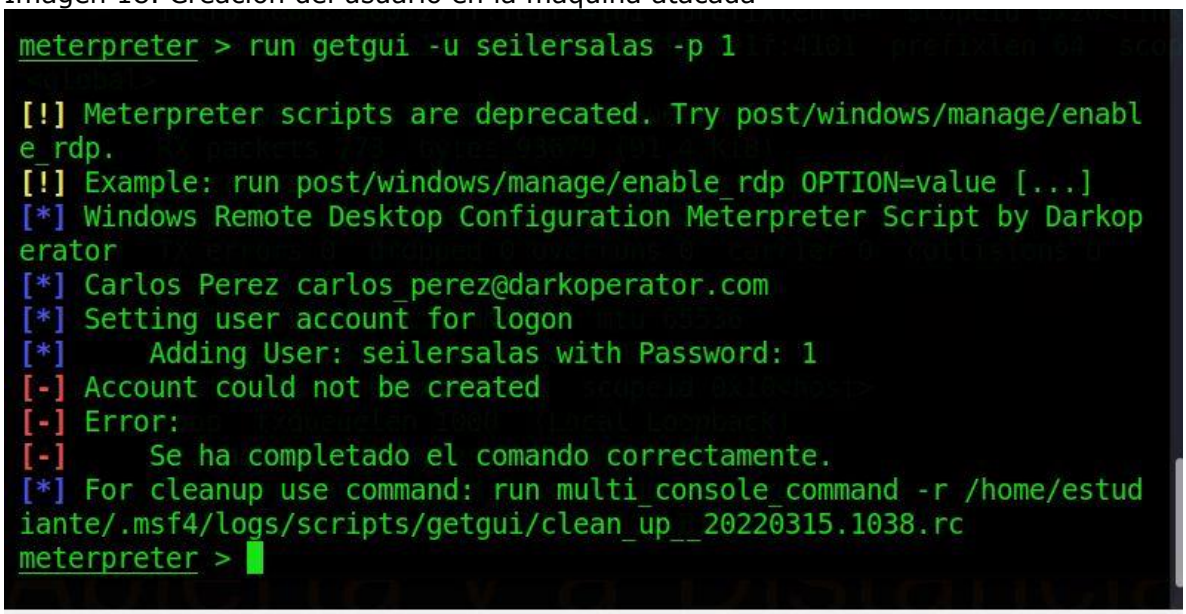
Imagen 17. Ejecución de exploit



Fuente: Autor

Se ingresa como incognito y se crea el usuario mediante el comando run getgui -u y se asigna el nombre de usuario y la contraseña.

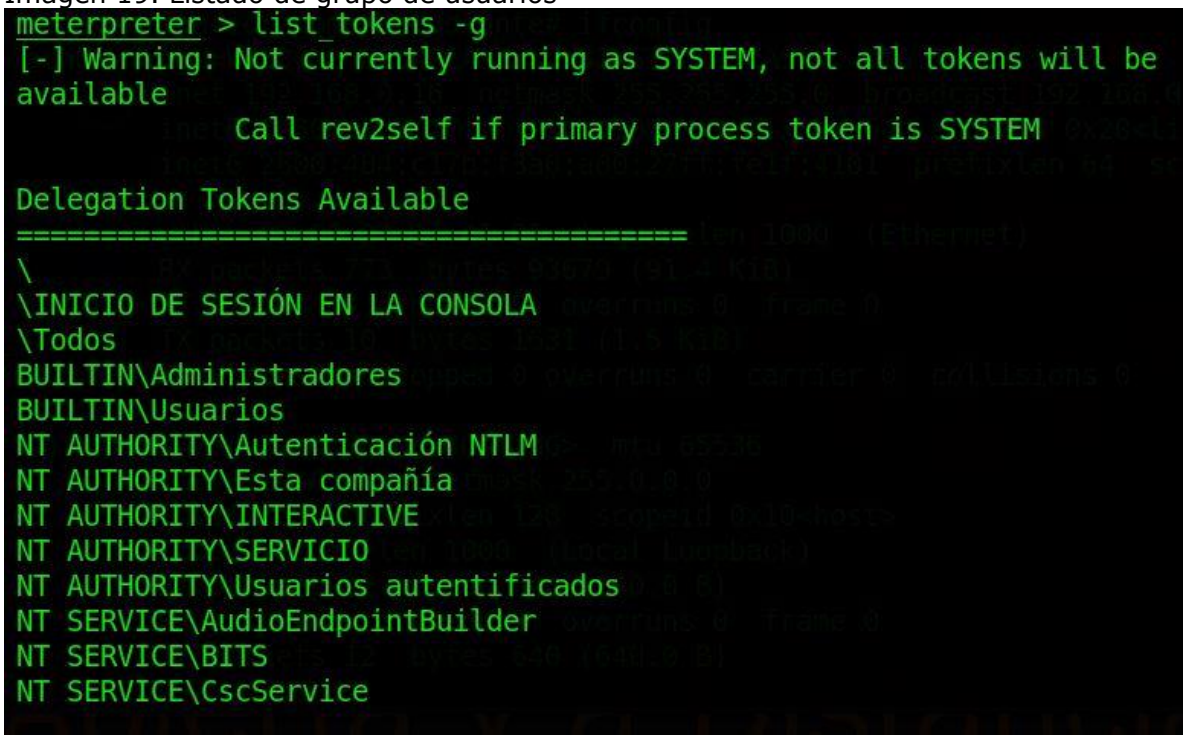
Imagen 18. Creación del usuario en la maquina atacada



Fuente: Autor

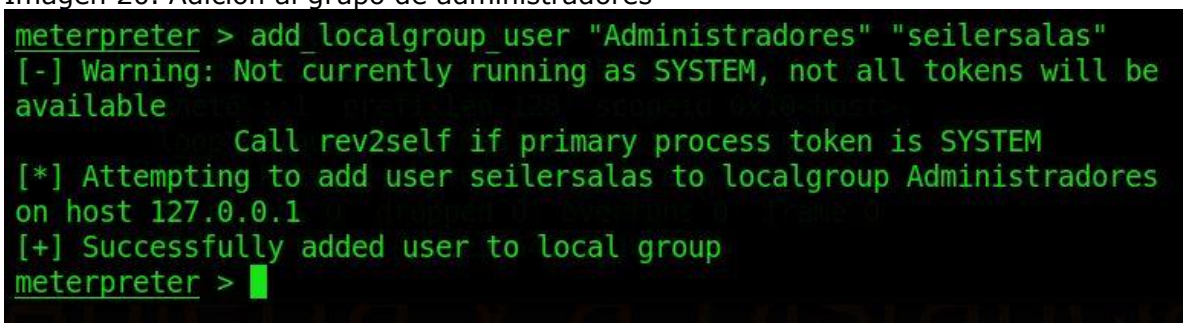
Una vez creado el usuario se procede a revisar los distintos grupos de usuarios existentes en la máquina para asignarle uno de mayor privilegio, esto se realiza mediante el comando **list_tokens -g**

Imagen 19. Listado de grupo de usuarios



Fuente: Autor

Imagen 20. Adición al grupo de administradores

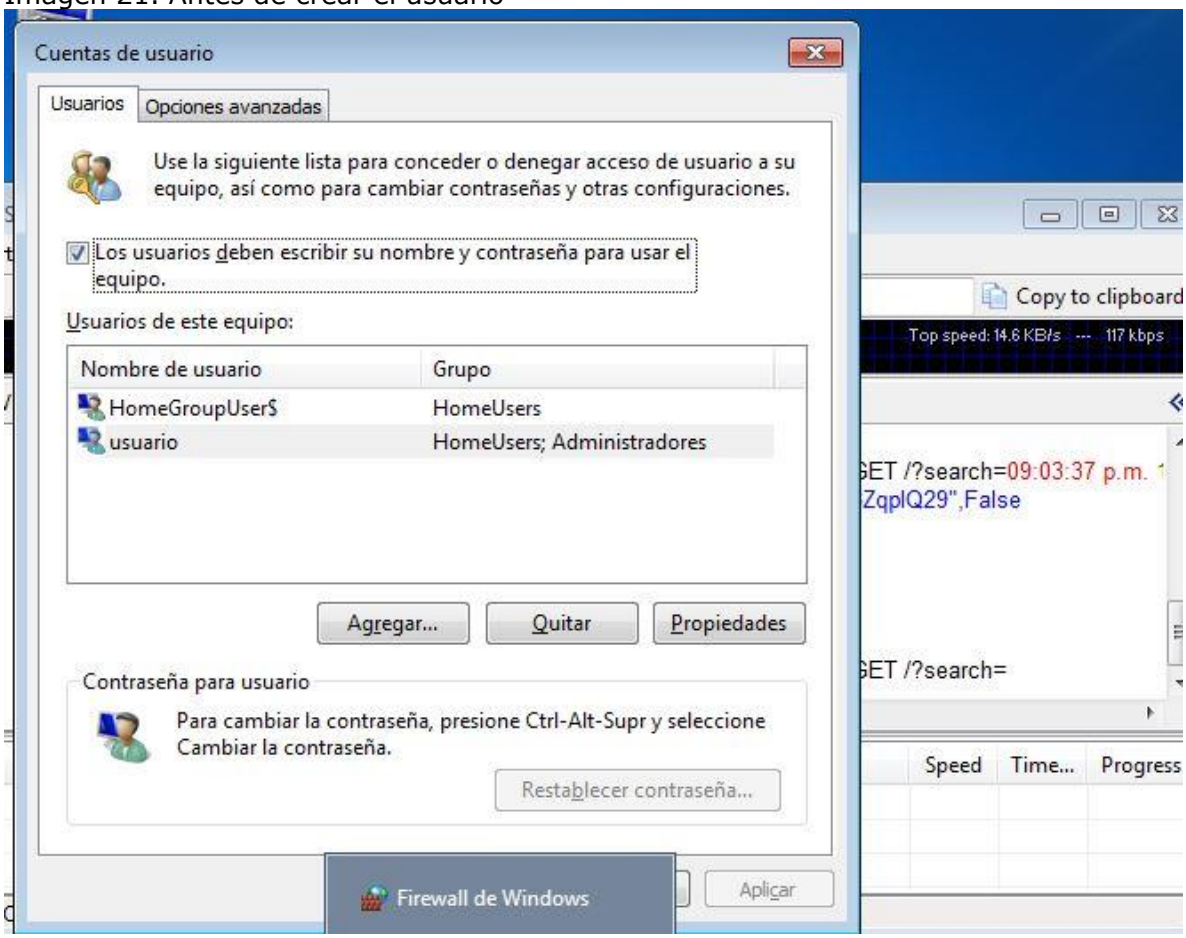


Fuente: Autor

En la imagen anterior se agrega el usuario al grupo de administradores mediante comando add_localgroup_user.

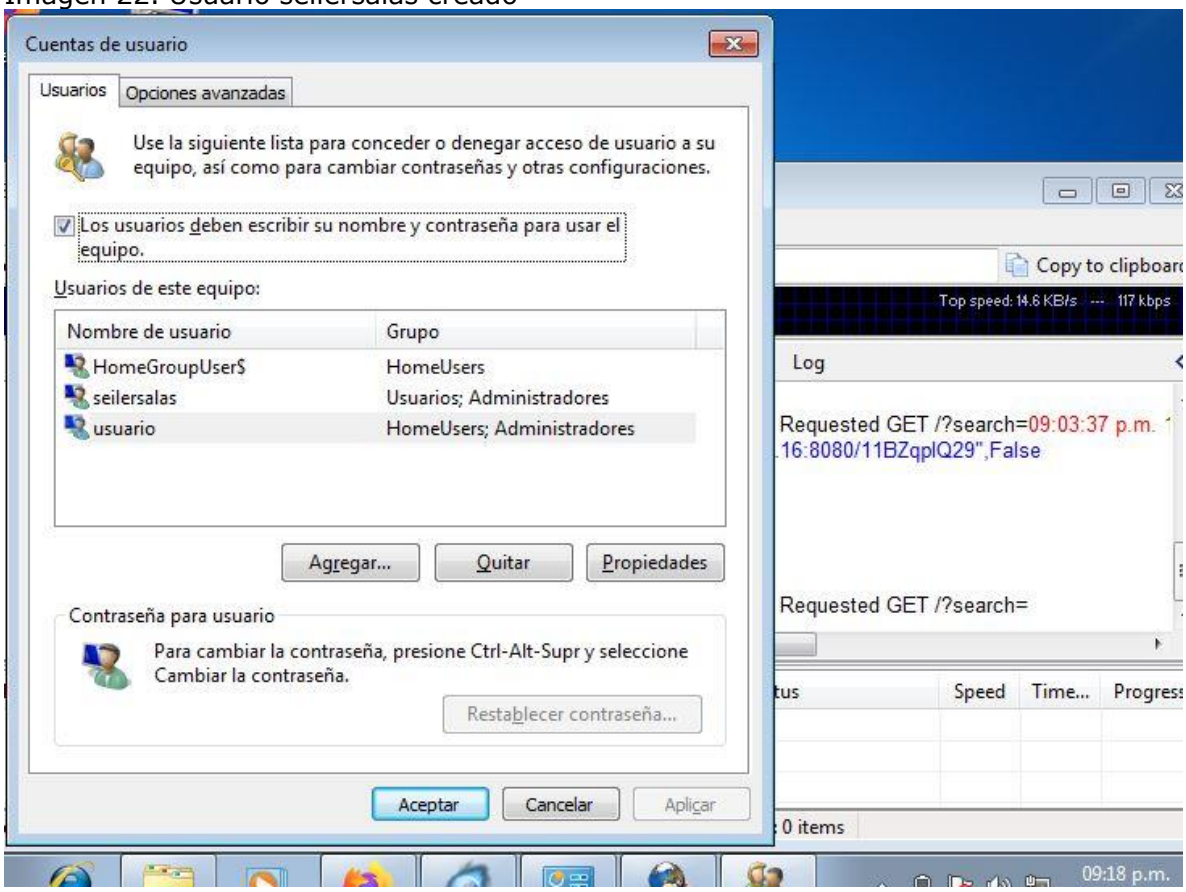
A continuación, se mostrará el antes y el después de la creación del usuario en la maquina víctima.

Imagen 21. Antes de crear el usuario



Fuente: Autor

Imagen 22. Usuario seilersalas creado



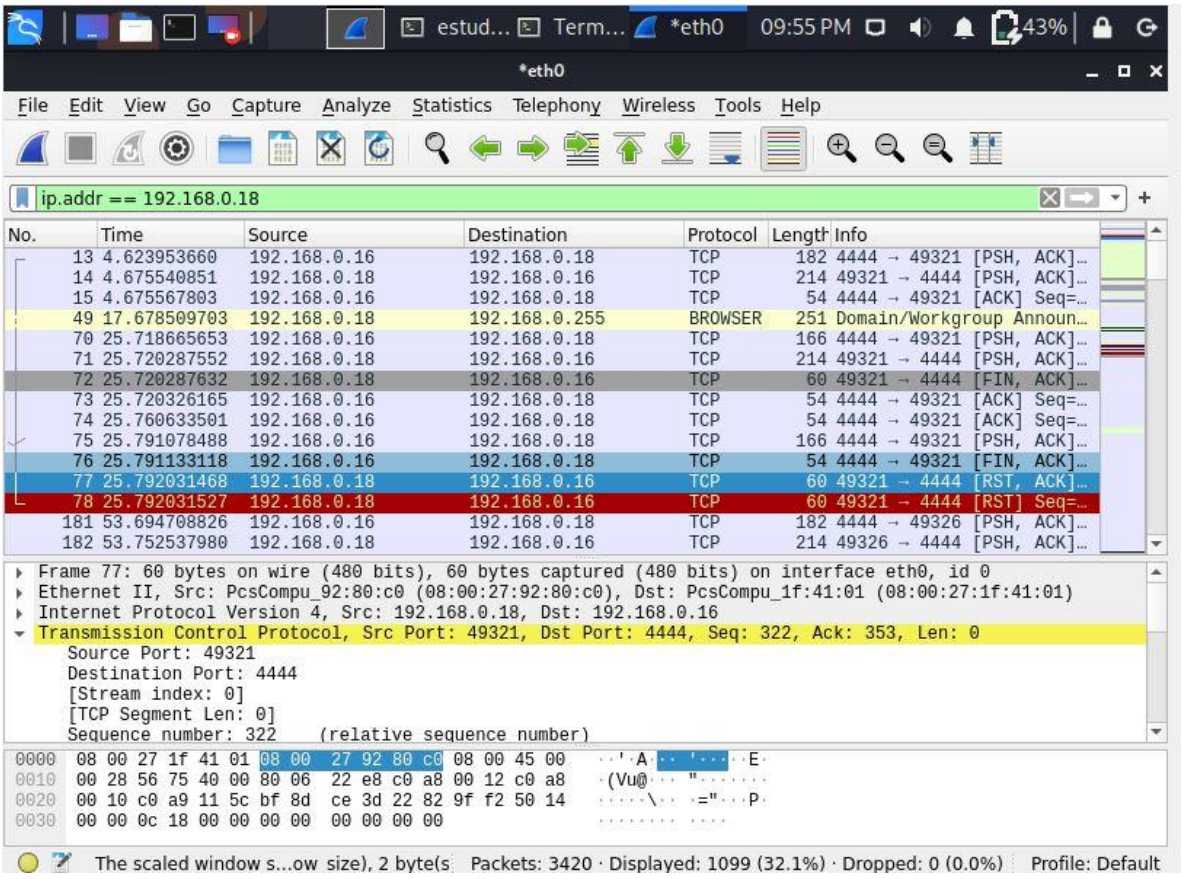
Fuente: Autor

Se evidencia que la aplicación rejetto fue vulnerada a través de la cual se pudo generar una sesión Meterpreter y crear el usuario seilersalas con privilegios de administrador.

5.4 DESARROLLO DEL ESCENARIO 4

Como lo era solicitado en el anexo 5 del escenario 4 sea ha realizado un análisis con una herramienta GPL para analizar el ataque que está sucediendo en tiempo real en uno de los equipos para así realizar propuestas que conlleven una solución y contener la amenaza.

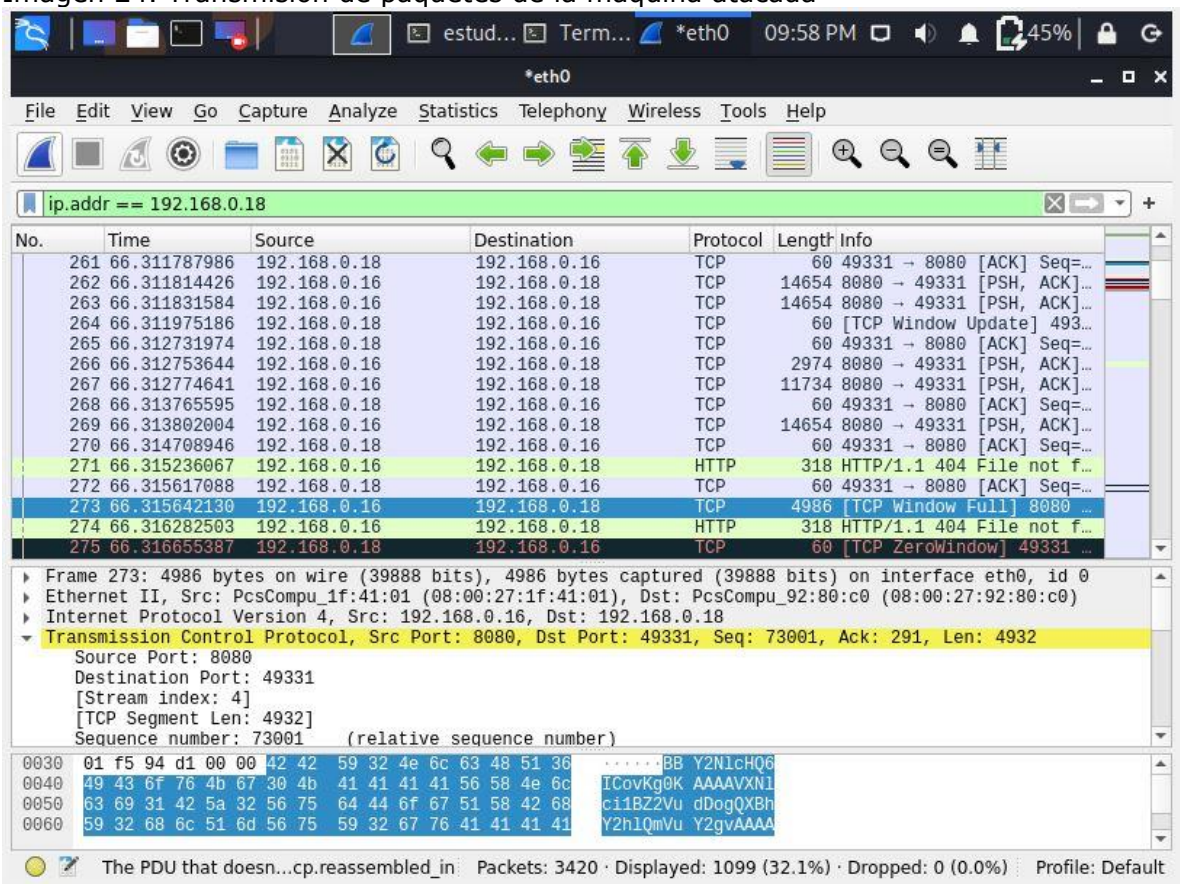
Imagen 23. Análisis de la máquina atacada con Wireshark



Fuente: Autor

En la imagen anterior se filtró el tráfico desde la maquina atacada y se puede ver que desde esta se había trasmisión a través de los puertos de transporte 49321 y 4444 desde el cual la maquina ataca respondía a la petición del atacante.

Imagen 24. Transmisión de paquetes de la maquina atacada

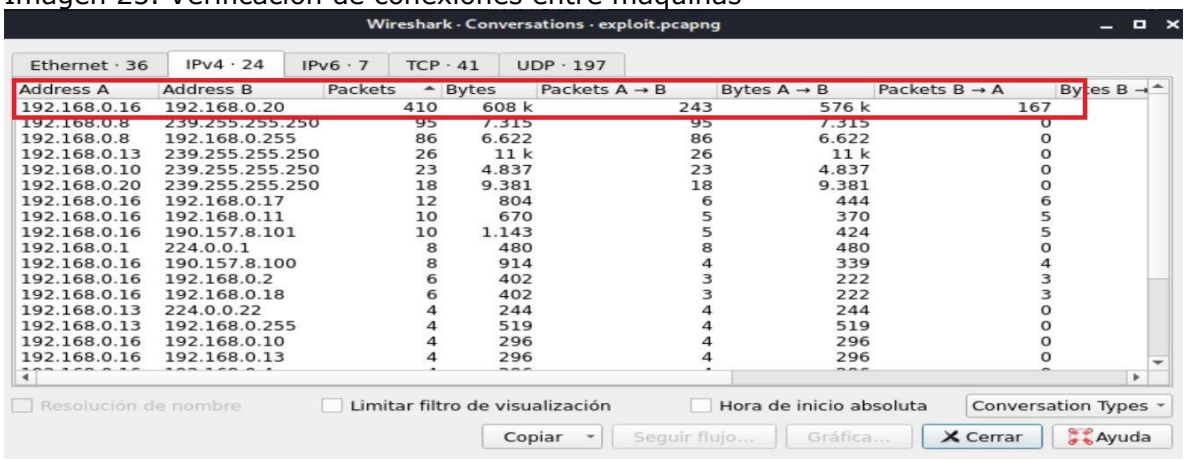


Fuente: Autor

En este frame podemos detectar que se trasmiten paquetes a través del puerto 8080 el cual se pudo identificar es usado por la aplicación hfs rejetto encontrada en la maquina atacada y la cual presenta una vulnerabilidad que está siendo aprovechada por el atacante.

A continuación, podemos analizar con que host la maquina atacada tuvo más transferencias para identificar el posible atacante, para este caso la IP de la víctima cambió a la 0.20 debido a una nueva configuración en esta.

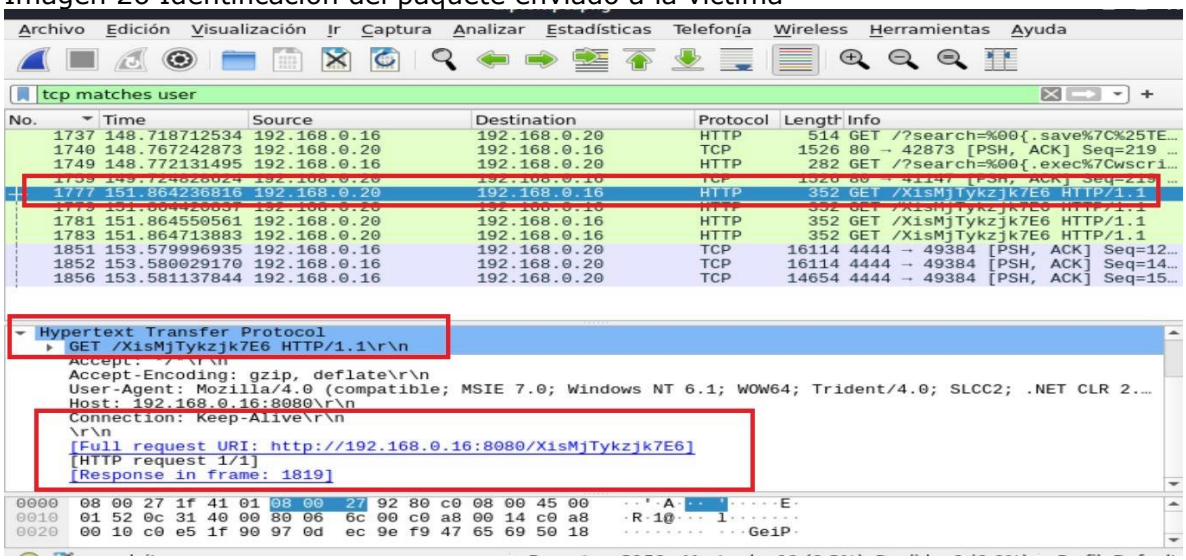
Imagen 25. Verificación de conexiones entre maquinas



Fuente: Autor

Se puede apreciar que la maquina con la cual tuvo más transferencias la víctima es la 192.168.0.16 posible atacante.

Imagen 26 Identificación del paquete enviado a la victima

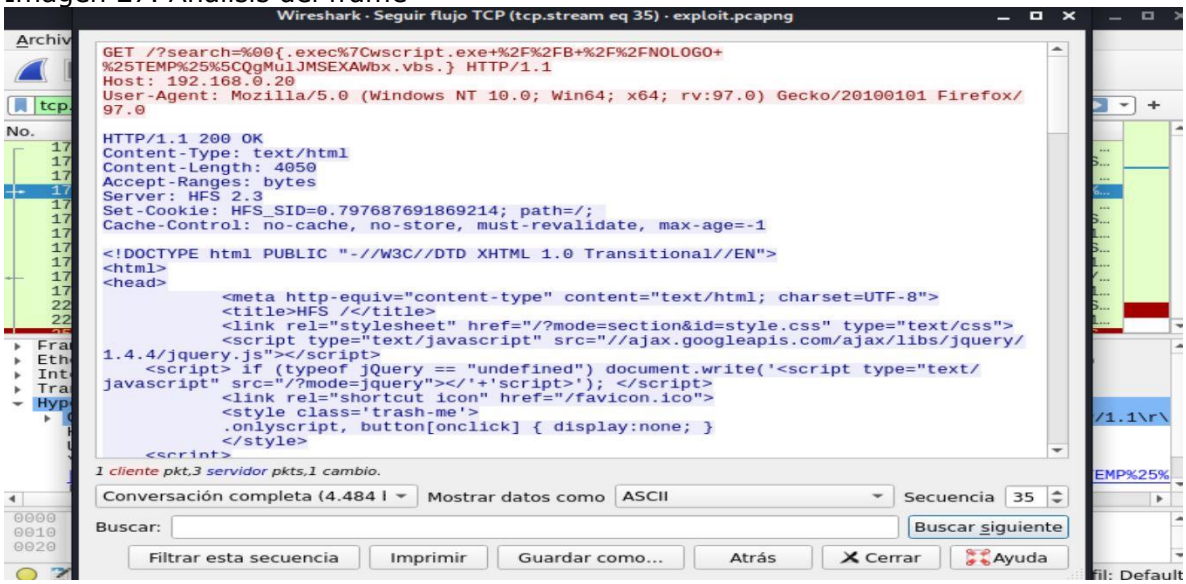


Fuente: Autor

En este frame se puede apreciar la transferencia del código malicioso desde la maquina atacante.

Se inspeccionará el archivo para analizar su contenido.

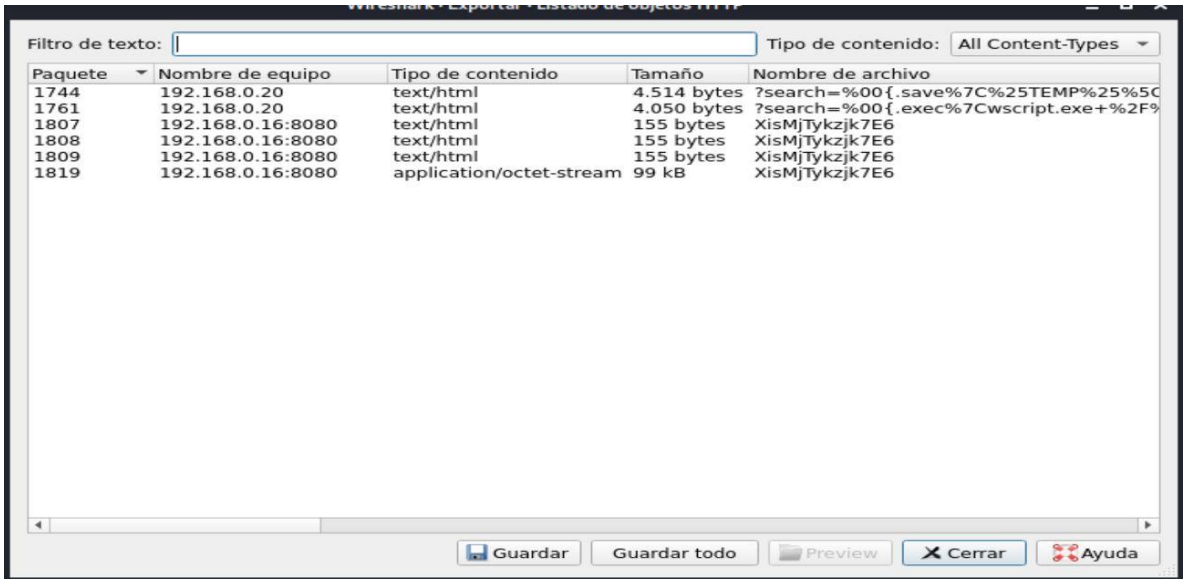
Imagen 27. Análisis del frame



Fuente: Autor

Efectivamente el frame muestra que se realizó la transferencia del Script con el código malicioso a la maquina víctima.

Imagen 28. Archivos transmitidos durante el ataque



Fuente: Autor

Al proceder a realizar la extracción de los archivos que se transmitieron durante el ataque se aprecia el script con el ejecutable.

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

Los cuestionamientos que realizaría serian:

- Si el equipo ha mostrado algún comportamiento anómalo.
- Ha presentado bloqueos, reinicios o apagados improvistos.
- Alguna alerta por parte de los sistemas de seguridad como el antivirus o el firewall.
- Si algún usuario distinto al que normalmente usa el equipo ha tenido acceso a este.

Lo que haría

- Realizar el análisis del equipo con alguna herramienta como Wireshark o Snort que permitan identificar o determinar qué tipo de ataque se está realizando y de acuerdo a esto proceder de forma adecuada.
- Una vez identificado el tipo de ataque aislar si es posible el equipo de la red para preservar la integridad de los demás dispositivos que componen esta.
- Realizar una copia de seguridad del disco duro para no comprometer los datos y registros que se produjeron o se están produciendo en el momento del ataque.
- Revisar los logs de los sistemas, aplicaciones, servidores etc.
- Analizar cualquier fuente que registre eventos mediante el cual se pueda hallar indicios de alguna falla presentada.

- Sino es posible aislar el equipo de la red, identificar si existe alguna conexión externa y bloquearla inmediatamente sea restringiendo el puerto, bloqueando la IP o eliminando el usuario.

- Una vez realizado el análisis con base a la información recolectada evaluar el impacto del ataque teniendo en cuenta la severidad de este y los activos afectados, estos serían de bajo, medio y alto impacto.

5.4.2 ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

- **Actualización e instalación de los últimos parches del sistema operativo**: con esto se busca que los fallos identificados se puedan subsanar mediante la aplicación de estos.

- **Revisión de los elementos de seguridad como antivirus y firewall:** verificar que se encuentren activos y actualizados ya que si bien el ataque se ejecutó estos dos elementos no estaban funcionando y pudiesen haber contenido la amenaza.

- **Bloqueo de puertos innecesarios:** estos contienen servicios de gestión que son generalmente los de mayor vulnerabilidad como lo son los HTTP, FTP, Telnet entre otros, con esto se limitaría el acceso de intrusos al sistema. Se evaluaría la viabilidad de inhabilitarlos o reconfigurarlos para aumentar su seguridad.

- **Implementación de IPv6:** Si bien este no garantiza que se le pueda realizar un análisis a la red por parte del atacante si ayudaría a que este no sea tan sencillo de hacer ya que su composición hace que pase de 32bits de la IPv4 128 en la IPv6 evitando que no sea tan factible un ataque por fuerza bruta. En el caso que no sea necesario se recomienda deshabilitarla ya que está opción viene por defecto activada.

- **Limitar el acceso al equipo:** controlando la conexión mediante IPs previamente autorizadas, de igual forma restringir el acceso remoto validando los permisos a una cantidad limitada de usuarios.

- **Verificar el software instalado en los equipos:** que sean solo los necesarios, en lo posible licenciados así sea gratuita para evitar la utilización de cracks. De igual manera actualizar las versiones para evitar fallos ya que los atacantes aprovechan las obsolescencias de estos.

- **Auditoria de usuarios:** Validar los permisos de los usuarios en el sistema, limitarlos tanto en roles como en cantidad, dejar solo los necesarios y permitir un solo administrador.

- **Gestión de contraseña:** Crear reglas para la gestión de las contraseñas que estén formadas por una estructura que permita brindar una mayor seguridad en la asignación de esta compuestas por una cantidad específica de caracteres normales y especiales con una caducidad no mayor a 60 días y no permitir creación de contraseñas en blanco o con caracteres en secuencia. Bloquear las cuentas por un número determinado de intentos no válidos.

5.4.3 ¿Describa con sus palabras las diferencias entre un equipo Blue team y un equipo de respuesta a incidentes informáticos?

La diferencia entre blue team y el equipo de respuesta a incidentes es que el primero busca prevención de ataques mediante la información recopilada y procesada actuando con base a los estándares de procesos políticas y procedimientos que tienen, mientras que el equipo de respuesta a incidentes es solo eso un equipo de reacción y no prevención lo que hacen es tratar de restablecer en el menor tiempo posible los servicios del ente atacado con esto se busca causar la menor afectación posible, siempre se busca una recuperación rápida y eficiente coordinada con el equipo de TI para que operación del servicio se pueda llevar con normalidad.
Otra diferencia se puede encontrar en que el equipo de respuesta actúa cuando se materializa un riesgo mientras que el blue team trabaja como

un analizador revisando las posibles vulnerabilidades que pueda hallar en la organización.

De igual forma el equipo de respuesta trabaja en coordinación con otros CSIRT recibiendo incidentes de todo tipo de distintas organizaciones, algunas son públicas otras privadas en ocasiones como apoyo y en otras para compartir experiencias y conocimiento, mientras que blue team trabaja de forma interna y específica sobre el sistema de información de determinada entidad.

Blue team documenta las vulnerabilidades para que sean resueltas de acuerdo con las recomendaciones realizadas y sean tenidas en cuenta mediante los procesos, políticas y procedimientos para proponer mejoras, mientras que el equipo de respuesta lo hace para crear una base de conocimiento mediante la cual se pueda guiar cuando un proceso similar ocurra.

5.4.4 ¿Si dentro de un equipo Blue team le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

Lo utilizaría como aliado ya que es una gran organización con suficiente experiencia y personal calificado que ayuda a gobiernos, personas o entidades y sería de mucha utilidad en el momento de que se requiera un apoyo o asesoría. Aprovecharía que su objetivo es similar al de blue team para constantemente ir actualizando los procesos y políticas al interior del equipo debido a que usan un modelo para identificar y perfeccionar mayores medidas de seguridad el cual es compartido a toda la comunidad para su revisión y evaluación.

Un fin muy importante sería la aplicación de las recomendaciones que realizan por medio de sus benchmarks o referencias de configuración en una gran variedad de productos, Windows, Linux, Apple, apache etc., en los cuales realizan distintos tipos de recomendaciones para tener en cuenta al momento de hallar alguna vulnerabilidad y esta sea mitigada a través de estas salvaguardas.

Implementaría los controles CIS de acuerdo a la necesidad y dependiendo de la organización, los cuales son un conjunto de buenas prácticas en

seguridad y acciones defensivas en la prevención de ataques permitiendo el enfoque en el conjunto más efectivo de medidas y técnicas disponibles para el mejoramiento de la defensa en la organización.

5.4.5 Explique y redacte las funciones y características principales de lo que es un SIEM.

Es un sistema que ofrece supervisión y análisis de los eventos en tiempo real, así como el seguimiento y los registros de los datos de seguridad con fines de cumplimiento o auditoria.
Ayuda a las organizaciones a reconocer amenazas y vulnerabilidades de seguridad antes que estas puedan ejecutarse.

[10]Un sistema SIEM realiza un análisis y evaluación de todos los activos de una organización en tiempo real, como inventario de activos y gestión de software y licencia, escaneo de red, monitorización pasiva. Buscando de esta manera intrusiones, vulnerabilidades, actividades sospechosas, y con esto poder tomar medidas necesarias a tiempo evitando que se materialice el ataque.

Una de las funciones de SIEM son las de almacenar e interpretar registros en tiempo real permitiendo actuar con una mayor reacción y brevedad a la hora de alguna falencia en los sistemas de seguridad.
Recopila toda la información centralizándola en una base de datos para su análisis y determinar comportamientos anormales.

Se caracteriza por:

- Centralizar el monitoreo de las amenazas potenciales.
- Diferenciar de amenazas reales a las falsas.
- Enfocado hacia la acción inmediata.
- Brindar la mayor cantidad de información sobre el incidente para que sea más fácil su resolución.
- Documenta todo el procedimiento, desde la detección, el proceso hasta la solución.
- Evita o minimiza las consecuencias de un ataque.
- Gestión de datos de riesgos.
- Visibilidad de la red
- Inteligencia de amenazas.

[10]https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

- Analítica.
- Alertas en tiempo real.
- Tableros e informes.

5.4.6 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.

[11]**IBM QRadar SIEM** es una gran herramienta de detección que permite a los equipos de seguridad comprender las amenazas y priorizar las respuestas. Qradar toma los datos de activos, usuarios, redes, nubes y terminales, luego los correlaciona con la inteligencia de amenazas y la información de vulnerabilidades. Después de esto, aplica análisis avanzados para detectar y rastrear amenazas a medida que penetran y se propagan a través de los sistemas.

La solución crea información inteligente sobre los problemas de seguridad detectados. Esto muestra la causa raíz de los problemas de seguridad junto con el alcance, lo que permite a los equipos de seguridad responder, eliminar las amenazas y detener la propagación y el impacto rápidamente. En general, IBM QRadar es una solución analítica completa con una diversidad de características, incluida una opción de modelado de riesgos que permite a los equipos de seguridad simular posibles ataques.

[12]**Sumo Logic**

Lógica de sumo es una plataforma de análisis de seguridad inteligente y flexible basada en la nube que funciona por sí sola o junto con otras soluciones SIEM en entornos de múltiples nubes e híbridos.

La plataforma utiliza el aprendizaje automático para mejorar la detección e investigación de amenazas y puede detectar y responder a una amplia gama de problemas de seguridad en tiempo real. Basado en un modelo de datos unificado, Sumo Logic permite a los equipos de seguridad consolidar el análisis de seguridad, la gestión de registros y el cumplimiento y otras soluciones en uno. La solución mejora los procesos de respuesta a incidencias además de automatizar diversas tareas de

[11] IBM. What is SIEM? https://www.ibm.com/topics/siem
[12] ibid

seguridad. También es fácil de implementar, usar y escalar sin costosas actualizaciones de hardware y software.

[13]Rapid7 InsightIDR

Rapid7 InsightIDR es una potente solución de seguridad para la detección y respuesta a incidentes, visibilidad de endpoints, autenticación de monitoreo, entre muchas otras capacidades.

La herramienta SIEM basada en la nube tiene funciones de búsqueda, recopilación de datos y análisis y puede detectar una amplia gama de amenazas, incluidas credenciales robadas, phishing y malware. Esto le da la capacidad de detectar y alertar rápidamente sobre actividades sospechosas, acceso no autorizado de usuarios internos y externos
InsightIDR emplea tecnología de engaño avanzada, análisis de comportamiento de atacantes y usuarios, monitoreo de integridad de archivos, administración de registros central y otras características de descubrimiento. Esto la convierte en una herramienta adecuada para escanear varios puntos finales y proporcionar detección en tiempo real de amenazas de seguridad en organizaciones pequeñas, medianas y grandes. Los datos de búsqueda de registros, endpoints y comportamiento del usuario proporcionan información que ayuda a los equipos a tomar decisiones de seguridad rápidas e inteligentes.

[14]Varonis

Varonis proporciona análisis y alertas útiles sobre la infraestructura, los usuarios y el acceso y uso de datos. La herramienta proporciona informes y alertas procesables y tiene una personalización flexible para incluso responder a algunas actividades sospechosas. Proporciona paneles de control completos que brindan a los equipos de seguridad una visibilidad adicional de sus sistemas y datos.

Además, Varonis puede obtener información sobre los sistemas de correo electrónico, los datos no estructurados y otros activos críticos con la opción de responder automáticamente para resolver problemas. Por ejemplo, bloquear a un usuario que intenta acceder a archivos sin permisos o usar una dirección IP desconocida para iniciar sesión en la red de la organización.

---

[13] ibid
[14] ibid

La solución de respuesta a incidentes de Varonis se integra con otras herramientas para proporcionar información y alertas procesables mejoradas. También se integra con LogRhythm para proporcionar capacidades mejoradas de detección y respuesta de amenazas. Esto permite a los equipos optimizar sus operaciones e investigar de manera fácil y rápida las amenazas, los dispositivos y los usuarios.

6 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM.

La implementación de un equipo blue team y red team al interior de una organización permite que esta tenga la facilidad de probar activamente sus defensas y la capacidad de respuesta de manera continua y en un entorno de riesgo controlado. Al involucrar estos dos equipos se abre la posibilidad desarrollar continuamente estrategias de seguridad en la organización evidenciando falencias que solo ocurran dentro de esta utilizando técnicas de ataques actuales.

Algunos aspectos importantes a tener en cuenta para el desarrollo de mejores estrategias serían:

- Identificar previamente productos a adquirir por parte de la organización con el fin de verificar y evaluar posibles vulnerabilidades que estos puedan presentar, así como en los que actualmente estén usando.

- Fortalecer la seguridad de la red para detectar ataques específicos y mejorar la capacidad de respuesta

- Fomentar la sana competencia sana entre los equipos red, blue y demás integrantes de TI con el fin de aumentar las capacidades de cada uno de estos generando motivación y fomento de la cooperación.

- Sensibilización al usuario final de las implicaciones que tiene una desatención en el tema de seguridad y los riesgos a los que estaría expuesto él o ella tanto como la organización.

- Desarrollo de las capacidades de seguridad de la organización en cuanto a madurez y habilidades dentro de un área de capacitación segura y bajo riesgo.

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

Sin duda alguna contar con un equipo de blue team y red team dentro de una organización es un elemento fundamental para fortalecer los temas de seguridad de una organización, pero no solo eso basta ya que la seguridad no es solo en el tema de los sistemas de información sino también en el ámbito de los usuarios ya que estos son uno de los principales actores dentro de este planteamiento, se debe implementar un proceso que abarque los elementos ya mencionados y que tenga en cuenta otros como lo es el perimetral, que brinde seguridad en este aspecto como en los otros también. Es por esto que sugeriría utilizar los controles de implementación CIS los cuales son un conjunto de buenas prácticas en seguridad y acciones defensivas en la prevención de ataques permitiendo el enfoque en el conjunto más efectivo de medidas y técnicas disponibles para el mejoramiento de la defensa en la organización.
Estos se ajustan fácilmente a otras normas como la ISO 27000, NIST Cybersecurity Framework, PCI DSS entre otros.

Básicos

Control 1: Inventario y control de dispositivos hardware.
Control 2: Inventario de software autorizado y no autorizado.
Control 3: Gestión continua de vulnerabilidades.
Control 4: Uso controlado de privilegios administrativos.
Control 5: Configuración segura para hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores.
Control 6: Mantenimiento, monitorización y análisis de logs de auditoría.

Fundamentales

Control 7: Protección de correo electrónico y navegador web.
Control 8: Defensa contra malware.
Control 9: Limitación y control de puertos de red, protocolos y servicios.

Control 10: Capacidad de recuperación de datos.
Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores.
Control 12: Defensa perimetral.
Control 13: Protección de datos.
Control 14: Control de acceso basado en la necesidad de conocer.
Control 15: Control de acceso inalámbrico.
Control 16: Monitorización y control de cuentas.

Organizacionales

Control 17: Implementar un programa de formación y concienciación en seguridad.
Control 18: Seguridad del software de aplicación.
Control 19: Respuesta ante incidentes.
Control 20: Pruebas de penetración y ejercicios de red team.

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

La ciberseguridad es un asunto bastante amplio y en el seminario se pudo comprender una pequeña parte de esta y es como continuamente las organizaciones se deben ir reformando en el tiempo y con tendencia no solo a la reacción sino a la prevención de ataques y fallas que se puedan presentar, en un inicio se le daba mayor importancia a la reacción y no a la prevención siendo que ambos son valiosos y con el crecimiento y masificación de la información en internet los ataques se han ido incrementando ya que algunas ocasiones no se requiere de gran experticia en el tema para poder ejecutar uno, de ahí nació la necesidad de reforzar más el asunto de la prevención con esto se crea contención y se evitan ataques. Es de esta forma como trabajan las organizaciones que cuentan en sus estructuras con equipos blue team y red team, importante también que tienen apoyo de organizaciones especiales dedicadas a preservar la seguridad en internet buscando con esto se puedan desarrollar actividades con mayor tranquilidad y seguridad.

También se puede concluir que como resultado del ejercicio que la seguridad no solo es necesaria a nivel de sistema operativo sino de las aplicaciones que se utilicen en esta, de nada sirve tener las últimas versiones en cada uno de estos si se desatienden las aplicaciones usadas en estos, es importante que continuamente se revise el versionamiento y la integridad de cada una de las aplicaciones que se utilicen en los equipos.

En el plano nacional se cuentan con algunas leyes que sancionan el uso indebido de los sistemas informáticos, tratamiento de datos e información y delitos que se puedan cometer, estas se deben ajustar y en el caso de que sea necesario ampliarlas ya que los métodos continuamente siguen cambiando y en algunas ocasiones la ley puede llegar a presentar vacíos o ambigüedades.

LINK DE LA PRESENTACION

https://youtu.be/2PQyJ5ESW08

9 BIBLIOGRAFÍA

Amos Kingatúa (31/03/2021). Las 9 mejores herramientas de respuesta a incidentes de seguridad para pequeñas y empresas https://geekflare.com/es/security-incident-response-tools/

Ambit. (29/04/2021). ¿Qué significa SIEM y cómo funciona? https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

Blog de isecauditors. (28/11/2019). Controles del CIS: novedades de la versión 7.1 https://blog.isecauditors.com/2019/11/novedades-version-7-1-controles-cis.html

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

COLOMBIA.CONGRESO DE LA REPÚBLICA. (enero 05 2009). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

DVIDSHUB. (18/05/2015). ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? Recuperado de: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). (p. 14 - 27).

https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Héctor Rizaldos. (22/10/2018). Qué es Metasploit framework. https://openwebinars.net/blog/que-es-metasploit/

IBM. What is SIEM? https://www.ibm.com/topics/siem

Insecure.ORG. Nmap Network Scanning. https://nmap.org/man/es/index.html#man-description

Manuel Hernandez. (26/01/2022). Pentesting con OWASP: fases y metodología. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35). https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

Smartekh. (17/08/21). CYBER WARS. ¿Qué es Red Team vs Blue Team? https://blog.smartekh.com/cyber-wars-que-es-red-team-vs-blue-team

UNIR. (07/01/2020). Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

Zoho Corp. ¿Qué son y cómo implementar los Controles de Seguridad Crítica CIS? https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html#