HABILIDADES TECNICAS Y ESTRATEGIAS DE SEGURIDAD DE LA INFORMACION SOBRE LOS EQUIPOS RED TEAM & BLUE TEAM

MARIA ALEJANDRA CAGUA YANQUEN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2024

HABILIDADES TECNICAS Y ESTRATEGIAS DE SEGURIDAD DE LA INFORMACION SOBRE LOS EQUIPOS RED TEAM & BLUE TEAM

MARIA ALEJANDRA CAGUA YANQUEN

Nombre
EVER LUIS ARROYO BARON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2024

1. RESUMEN

En este informe se destaca la importancia crítica de fortalecer las estrategias en los equipos de Blue y Red Team. Para ello, se analizarán las principales características y responsabilidades de cada equipo, se presentarán escenarios relacionados al un ambiente real y con ellos se partirá las recomendaciones que implique para la protección de los sistemas informáticos.

Básicamente, este seminario nos brinda habilidades técnicas avanzadas, refuerza las capacidades para aplicar estrategias colaborativas entre los equipos Red Team y Blue Team, todo con el propósito de que la protección en los sistemas informáticos sea continua, también se hizo importancia del marco legal colombiano sobre la protección y seguridad de la información.

2. CONTENIDO

pág.

TABLA DE ILUSTRACIONES

3. GLOSARIO

Payload: Carga útil que se ejecuta en el sistema objetivo para obtener acceso o control.

Pentesting: Pruebas de penetración para identificar vulnerabilidades en un sistema.

Nmap: Herramienta para escanear puertos abiertos

Phishing: Suplantación de identidad para engañar a la víctima y obtener información confidencial.

CVE (Common Vulnerabilities and Exposures): es un sitio web para buscar ciertas vulnerabilidades de red y de software

Purple Team: Equipo que combina las habilidades de los equipos Red Team y Blue Team.

Exploit: código diseñado para aprovechar vulnerabilidades en un sistema

Hardening: son básicamente procesos de sistemas con el fin de reducir riesgo.

Malware: es un software malicioso para dañar sistemas y a un paso del hurto de información.

Ataque: Asedio virtual para conquistar información o causar daño.

Ciberseguridad: Tejido invisible que protege la información digital.

4. INTRODUCCIÓN

Con el presente informe técnico nos presentara sobre los conceptos básicos en el contexto de los equipos de Blue Team y Red Team, teniendo en cuenta los criterios legales y normatividad vigente en el marco legal colombiano. Se busca analizar la complejidad de las aplicaciones y las deficiencias en las prácticas de estos equiposen software virtyalizacion qye nos dan un enfoque real o un escenario quizás tangible, con el fin de proponer estrategias para fortalecer su eficacia en la protección de la información y poner en práctica muestras habilidades aprendidas de la ciberseguridad

5. OBJETIVOS

5.1 OBJETIVOS GENERAL

Fortalecer y empoderar las estrategias tanto de los equipos de Blue Teams y Red Team para mejorar la seguridad de la información, identificando las vulnerabilidades, amenazas, novedades y proponiendo mejoras continuas para los sistemas informáticos.

5.2 OBJETIVOS ESPECÍFICOS

- Analizar las leyes y decretos que existan en Colombia sobre los delitos informáticos y protección de datos.
- Investigar en que consiste el Código Ética del consejo profesional COPNIA
- Especificar las características de los servicios web de análisis de vulnerabilidades
- Demostrar las vulnerabilidades para aplicar metodologías y técnicas de intrusión,
- Diferenciar entre un Blue Team, un CSIRT y un Red Team
- Establecer simulaciones entre los equipos Red y Blue Team para evaluar fallas en tiempo real,

6. DESARROLLO DEL TRABAJO

6.1 ESCENARIO 1

1. Sobre el marco Legal Colombiano

   Existen varios artículos desde los delitos informáticos Ley 1273 de 2009, según la normativa en el código penal en la sesión tutelado de la protección de la información y de los datos se preservan integralmente los sistemas que usen las tecnologías de la información y las comunicaciones.

   Artículo 269A: acceso abusivo a un sistema informático. El que sin autorización o fuera de lo acordado, que acceda en parte del sistema protegido, se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

   Articulo 269B: [i]ob[1]staculización ilegitima de sistema informático, el que impida o obstaculice el funcionamiento a los datos, contenidos o en una red de telecomunicaciones.

   Articulo 269 C: Intercepción de los datos informáticos.

   Articulo 269D: Daño informático.

   Articulo 269 E: Uso de software malicioso, así produzca, trafique, adquiera, distribuya, extraiga del territorio nacional software malicioso con efectos dañinos.

   Artículo 269F: Violación de datos personales.

   Artículo 269G: Suplantación de sitios web para capturar datos personales.

   En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

   Estas leyes además de varias son originada de la normatividad desde el congreso de la república, y por otro lado, el derecho siempre llega a su cita, pero existen varios

[1] Mayo 2019. Normatividad sobre delitos informáticos. Policía Nacional de Colombia. Link https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

escenarios en los cuales el derecho ha estado siempre a un paso, además los asociados con desarrollos tecnológicos como la internet, la inteligencia artificial y el internet de las cosas.

E igual aparte de estas leyes, en el sector privado es importante y se vuelve necesario seguir forzando las barreras tecnológicas y los controles internos para evitar ser víctimas de estos delitos.

2. En el mundo de la ciberseguridad se hace pruebas de Pentesting:

Para hacer una prueba de pentesting, consiste en las siguientes fases que ayudaran a corregir los fallos y evitar los ciberataques en el futuro:

Planeación: se establece enlace de pruebas, se determina objetivos y metodología a utilizar

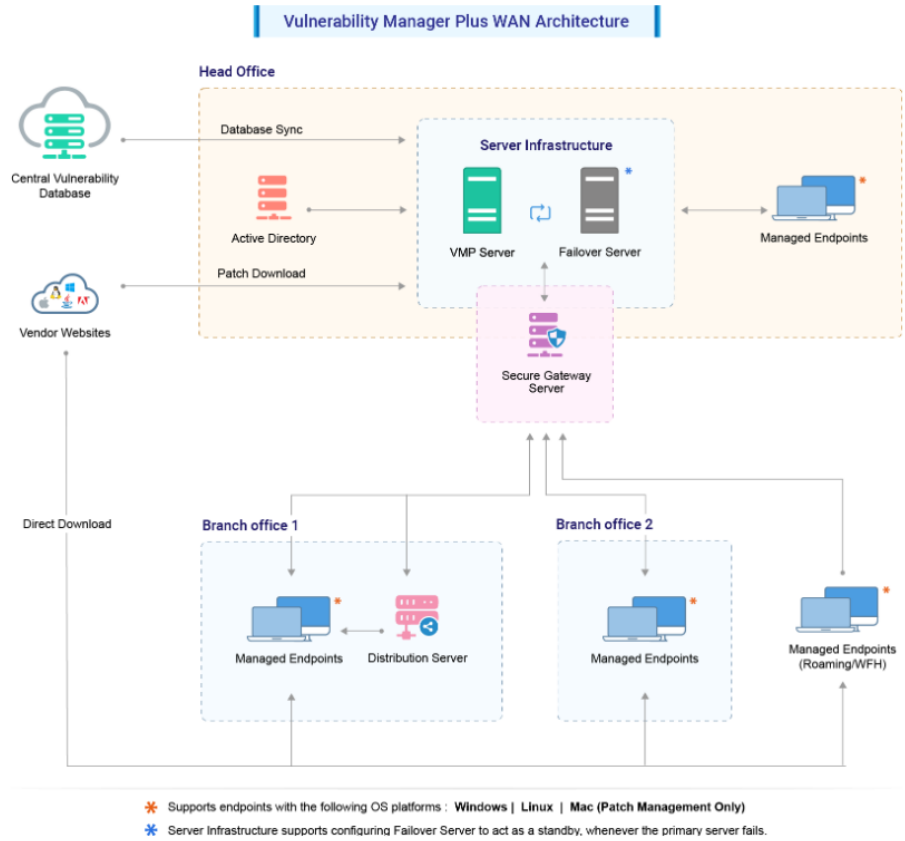
Ilustración 1. Tipos de pruebas

Fuente ManageEngine

Recopilación de información: se reúne toda la información, incluye a la identificación de sistemas en la red, servicios en ejecución y vulnerabilidades, también como más información[2].

Ilustración 2. Recopilación de la arquitectura de la red y servicios

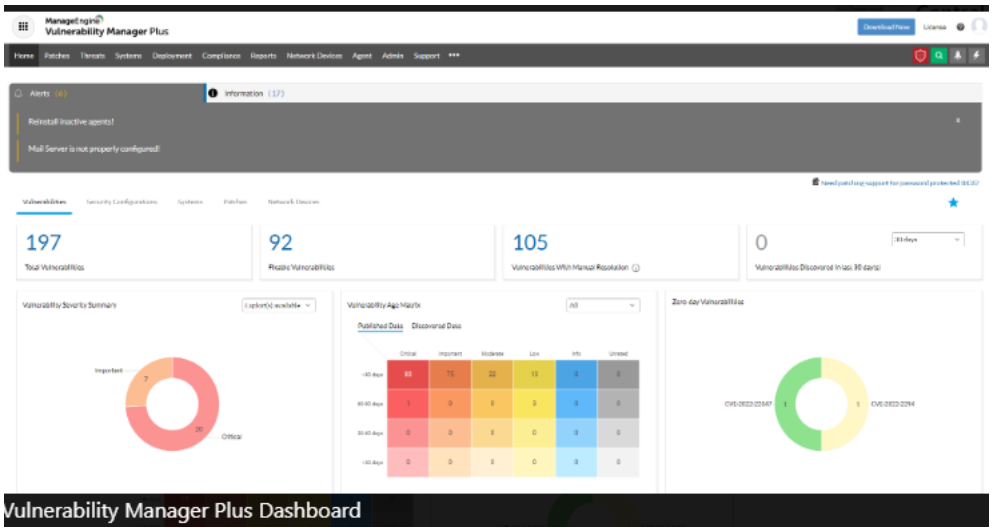
[2] Abril 2024. Ventajas WAN vulnerabilidades. Vulnerability Manager Plus https://www.manageengine.com/vulnerability-management/help/wan-architecture.html



Fuente ManageEnginePLus

Análisis de vulnerabilidades: pruebas iniciales para localizar las debilidades

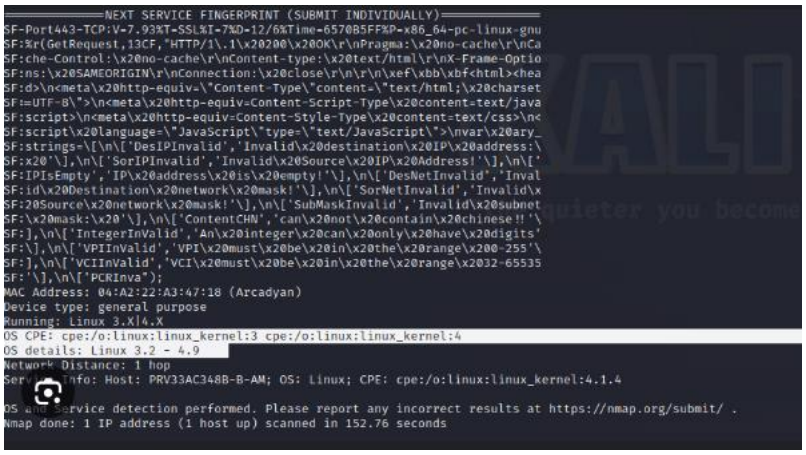
Ilustración 3. Análisis de vulnerabilidades en la red y los demás servicios



Fuente ManageEnginePLus

Explotación: explotar vulnerabilidades identificadas, esto incluye la ejecución de código malicioso, acceso a datos confidenciales.

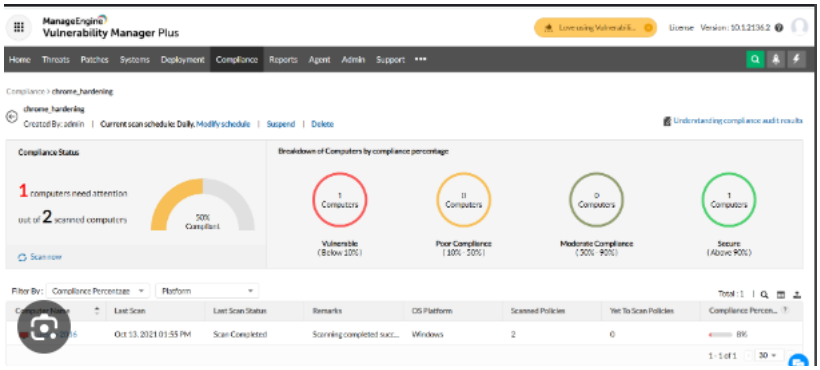
Ilustración 4. Ejemplo de Script o código en ejecución a segundo plano



Fuente Guia Hacking y pentesting

Análisis de resultados: básicamente con estos resultados se revisa debilidades y evaluación de riesgo potencial.

Ilustración 5. Resultados obtenidos según el escaneo que se ejecuta en la red



Fuente ManageEnginePLus

3. Acerca de las herramientas de ciberseguridad:

Herramientas:

- **Metasploit**: esta es una herramienta que tiene alrededor de 900 exploits para poner aprueba la ciberseguridad de cualquier sistema informático. Este software es de código abierto, es escrito por Perl y traducido a ruby, para mayor eficiencia y se ha evolucionado para convertirse en la herramienta de elección para la ejecución de exploits, principalmente trabaja dentro de un entorno del sistema operativo Kali Linux.

  No solo son herramientas de Hackeo, es un instrumento crucial para poner a prueba las vulnerabilidades en sistemas informáticos, es multiplataforma y gratuita.

- **Nmap**: es basicamente una herramienta de línea de comandos de Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.
  También ayuda a mapear rápidamente una red sin comandos ni configuraciones sofisticados. También admite comandos simples (por ejemplo, para verificar si un host está activo) y secuencias de comandos complejas a través del motor de secuencias de comandos Nmap.

- **OpenVas**: framework con base en servicios y herramientas que puede usarse de forma individual o como parte del conjunto de herramientas de seguridad incluidas en OSSIM, es básicamente de uso libre y se usa en Kali Linux, el gestor es el servicio que lleva a cabo tareas como el filtrado o clasificación de los resultados del análisis, control de las bases de datos que contienen la configuración o los resultados de la exploración y la administración de los usuarios, incluyendo grupos y roles[3].

  Servicios en línea

- **ExploitDB**: este servicio emerge como una pieza destacada, aclamada por muchos como fuente esencial de exploits, vulnerabilidades y técnicas de seguridad. Esta función ha sido valorada por los profesionales de la seguridad informática, quienes encuentran en esta plataforma una herramienta útil para identificar posibles puntos de vulnerabilidad y desarrollar estrategias de mitigación.
  La plataforma también juega un papel crucial en la planificación de respuestas a incidentes de día cero, situaciones en las que se descubre una vulnerabilidad antes de que se disponga de un parche.

- **CVE**: conforman una lista de las fallas de seguridad informática que está disponible al público. Cuando alguien habla de un CVE, se refiere a una falla a la cual se le asignó un número de identificación de CVE.
  Las advertencias de seguridad que emiten los proveedores y los investigadores casi siempre mencionan al menos uno de estos identificadores. Los CVE permiten que los

[3] Agosto 2023. Evaluación de vulnerabilidades usando open vas. Link https://www.welivesecurity.com/es/recursos-herramientas/evaluacion-vulnerabilidades-openvas/

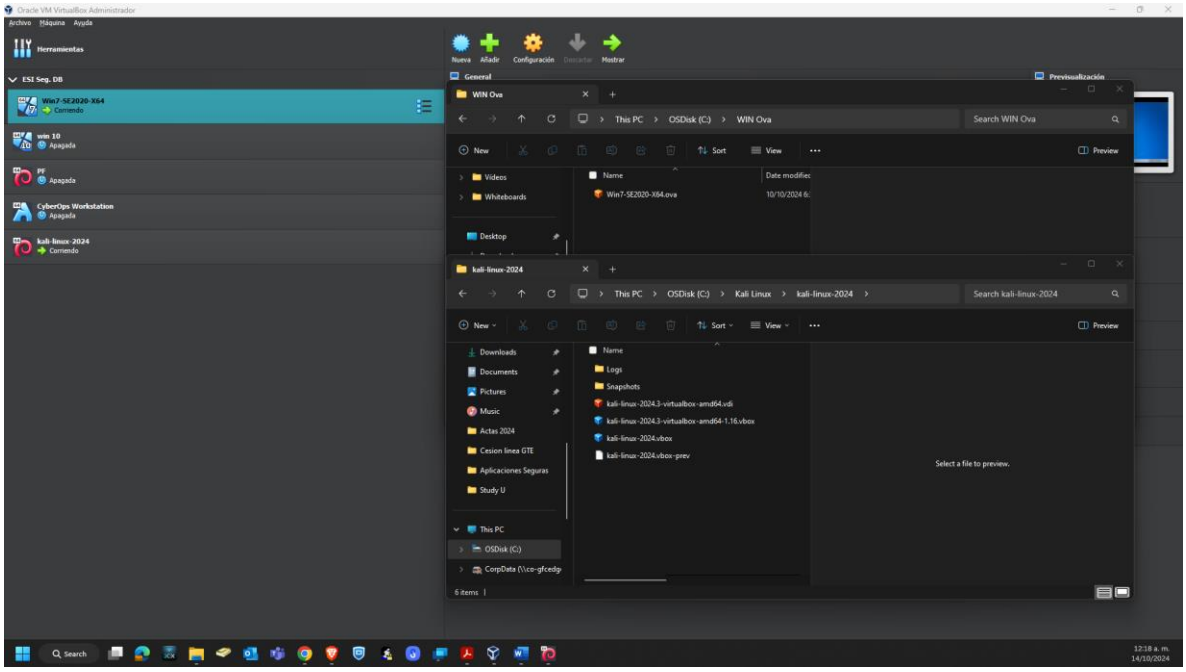
especialistas en TI coordinen sus iniciativas para priorizar y solucionar los puntos vulnerables, a fin de reforzar la seguridad de los sistemas informáticos.

4. Sobre el escenario 1, realizar la respectiva actividad:

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

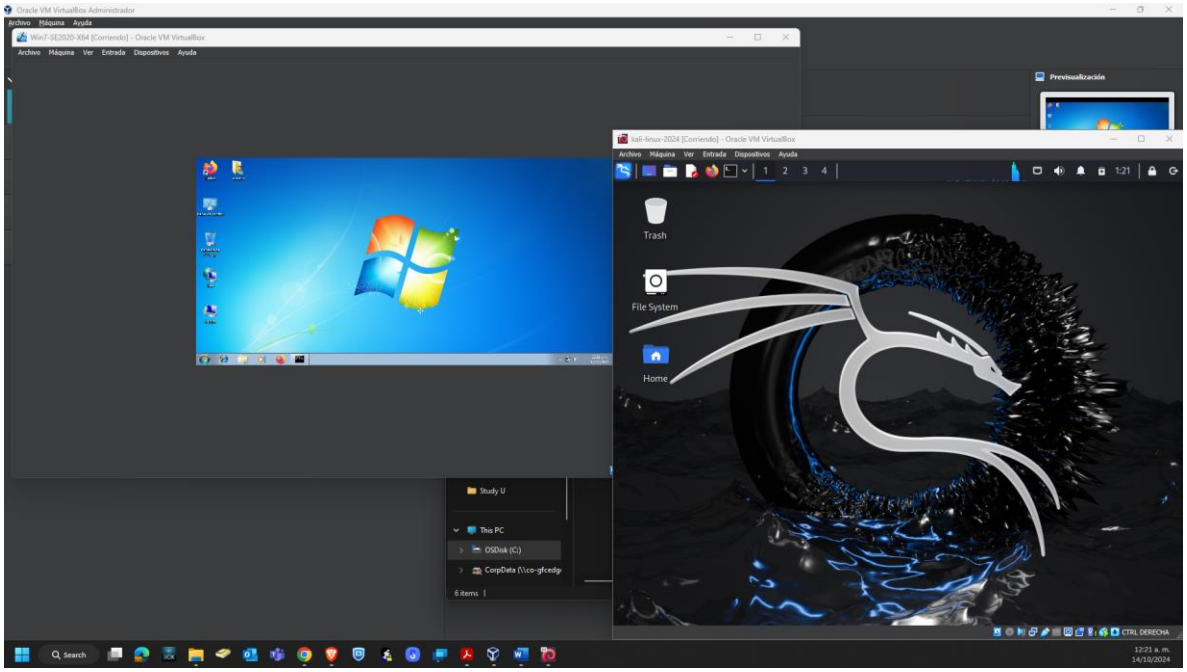
Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter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

Ilustración 6. Descarga de la aplicación virtual box y las imágenes .ova de Win 7 y Kali Linux



Fuente propia

Ilustración 7. Configuración de la imagen WIN 7 y Kali Linux



Fuente propia

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

Ilustración 8. Configuración de hardware de la maquina WIN 7

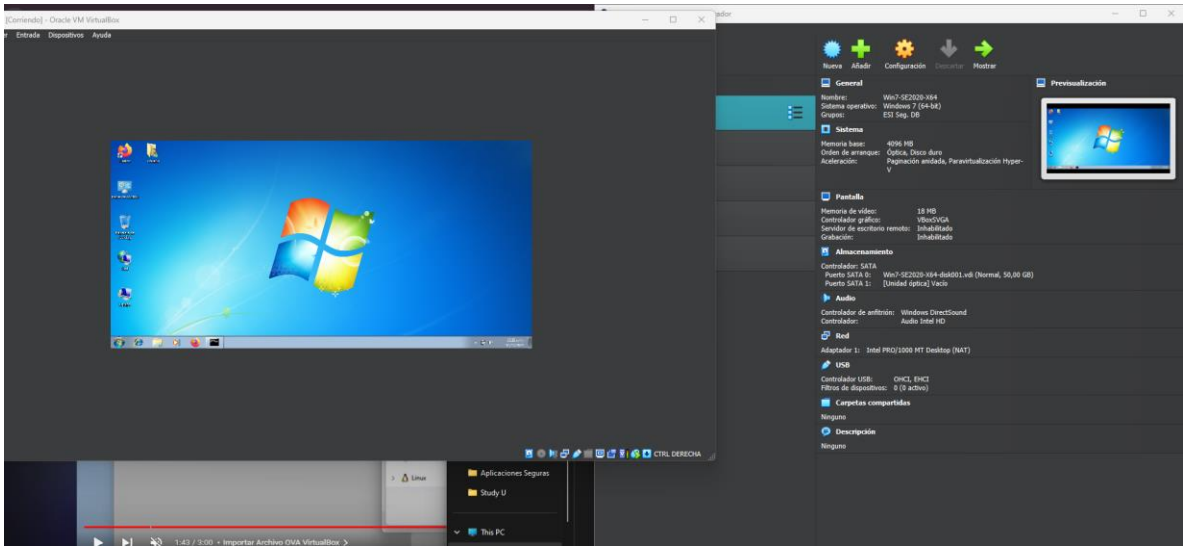
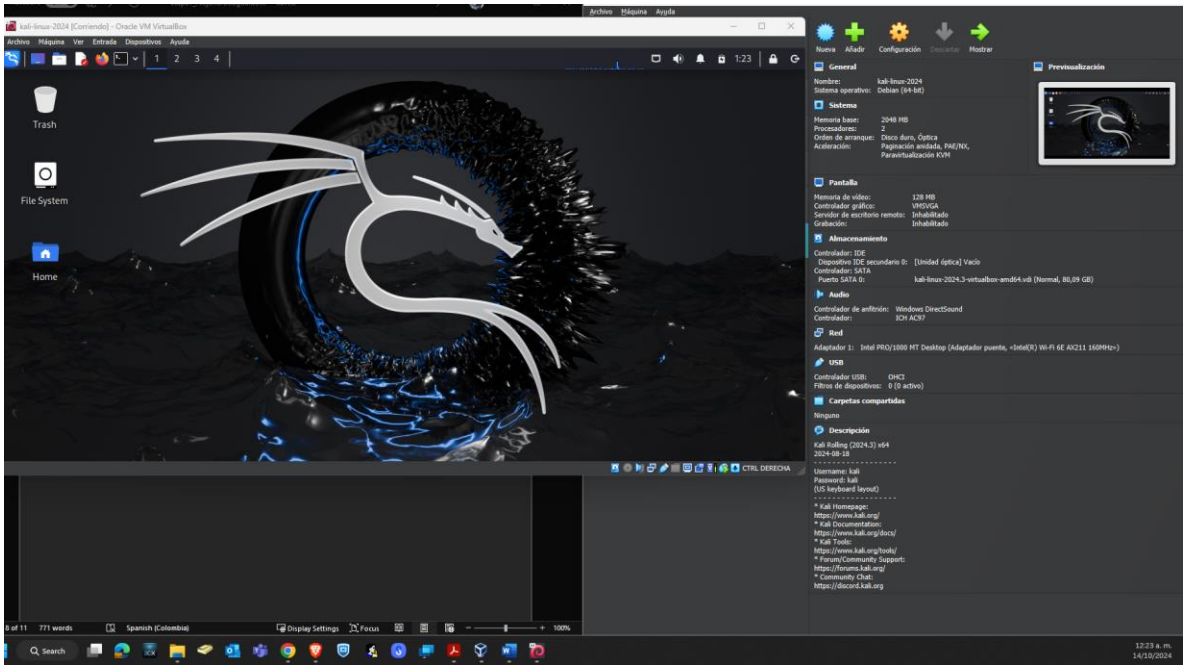
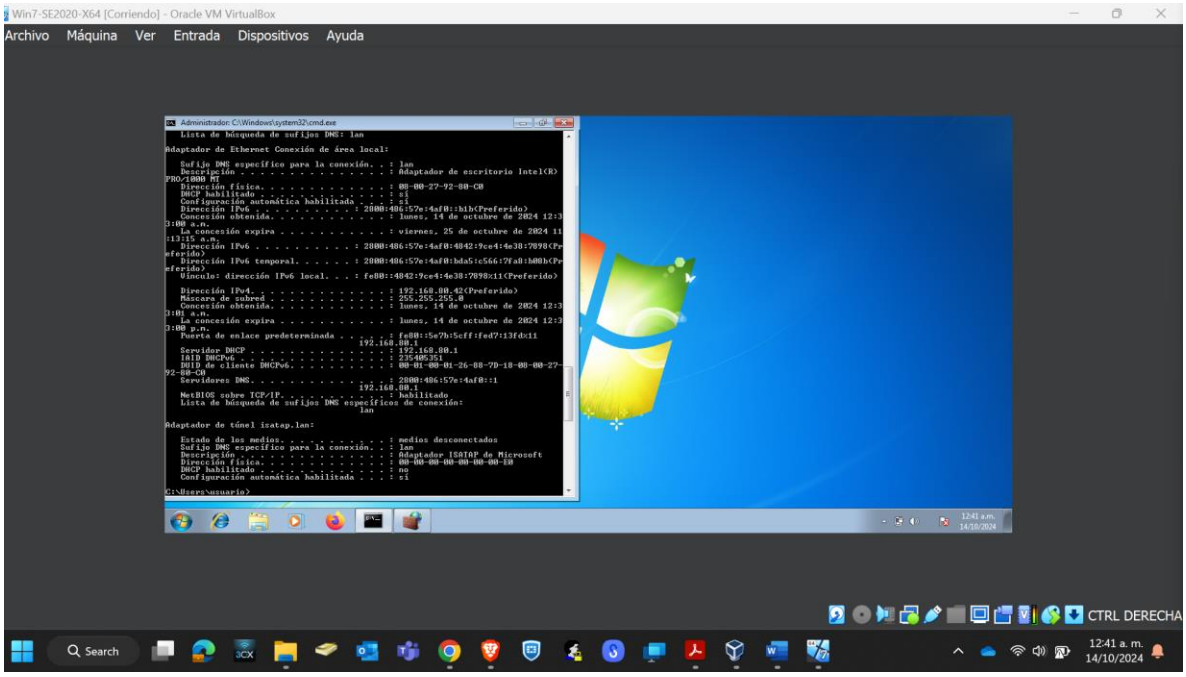

Fuente propia

Ilustración 9. Configuración de hardware de la maquina Kali Linux



Fuente propia

Ilustración 10. identificación IP de la maquina WIN 7



Fuente propia

Ilustración 11. Identificación IP de la maquina Kali Linux

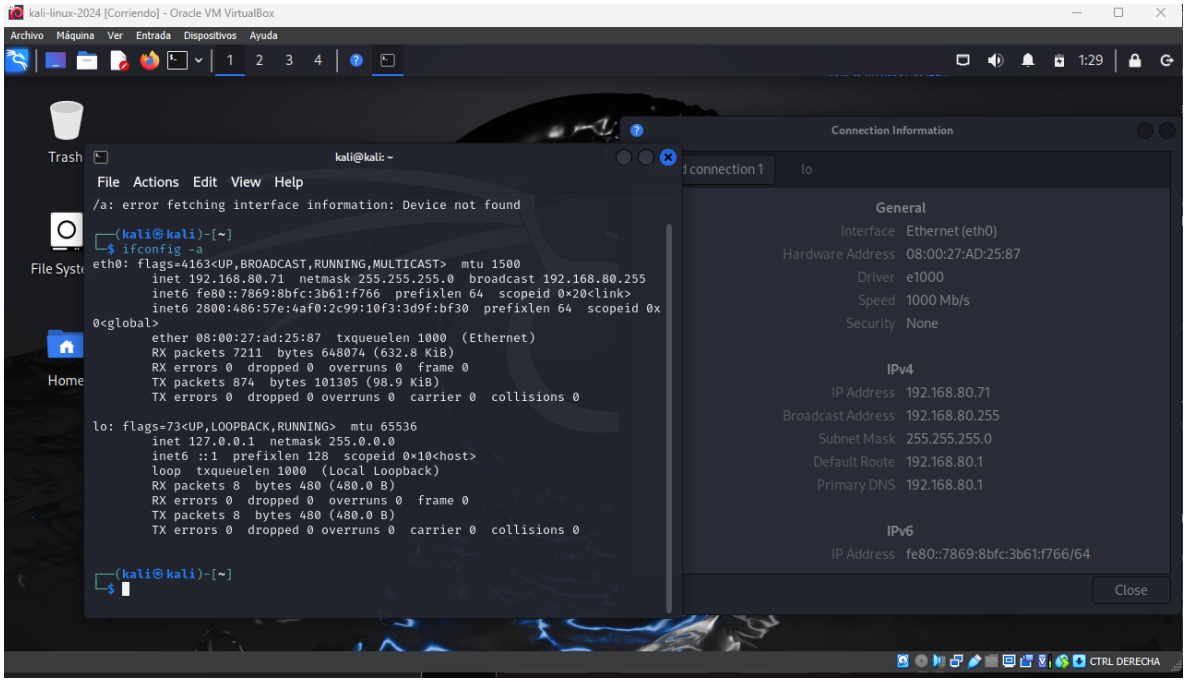
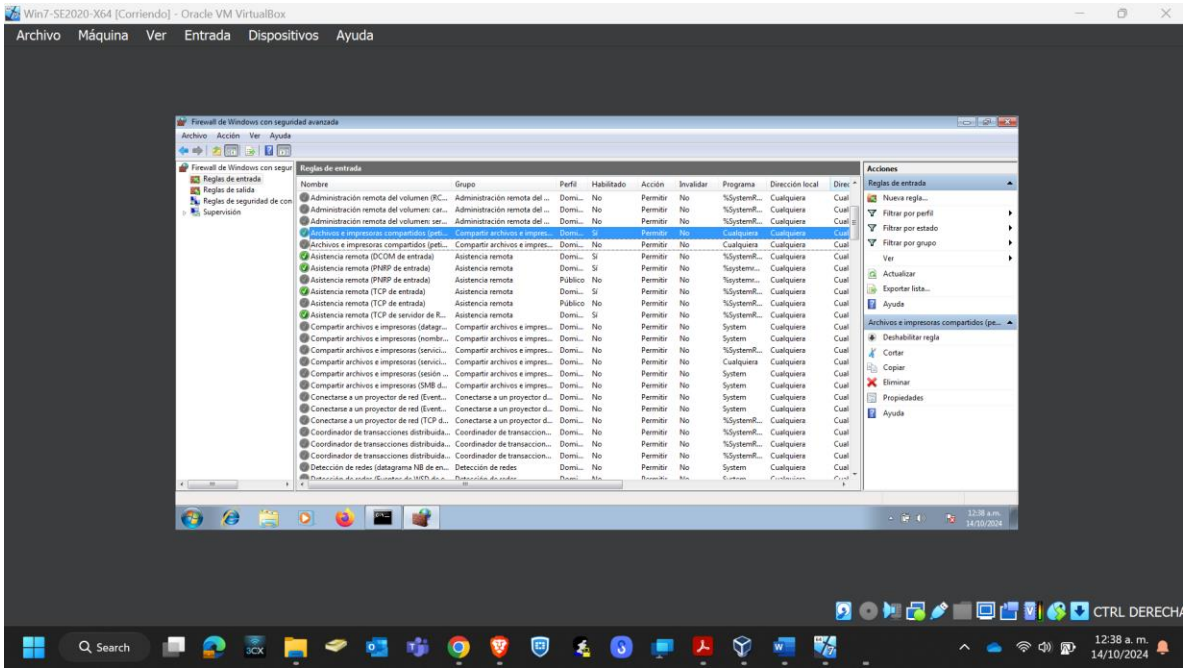
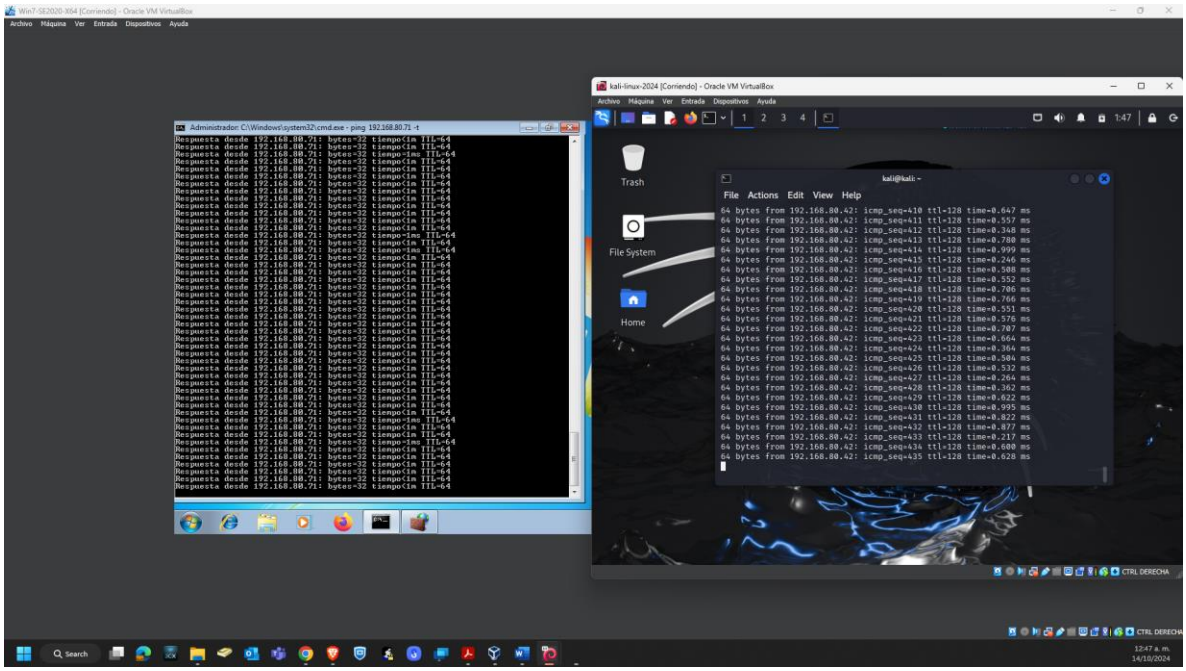


Ilustración 12. Se habilita firewall el protocolo ICMP IPV4 el paso de paquetes de ping



Fuente propia

Ilustración 13. Prueba de ping entre ambas maquinas WIN 7 y Kali Linux



Fuente propia

Cabe aclarar que se deja en ambas maquinas se deja con la configuración de adaptador puente para lograr la comunicación de ping.

6.2 ESCENARIO 2

1. Sobre el escenario 2, validar sus procedimientos ilegales y responder:

   Acorde al Anexo 2, se puede considerar que las falencias que dejo el abogado a pesar de que ya no labore para la organización CyberFort, la gerencia no se tomo el tiempo de revisar los contratos para reclutar el personal para nuevos ingresos y lo que no estaría bien es la entrega de estos mismos documentos sin modificaciones pues estaría abierto a particularidades o brechas a que futuro puede ser una facilidad o un parte contraria según para las personas que no tan buenas intenciones, no es ético, es necesario modificar el contrato y asegurar que acuerdos deben cumplir los nuevos ingresos a la organización red y blue team, pues conocerán los protocolos, procesos y además de otros lineamientos que trataran con nuevos clientes, básicamente la reputación de la organización podría darse en juego.

   Por otro lado, sobre el acuerdo Anexo 3, no es ético e ilegal:

Consideración 1. *Sobre dicha información es compartida en virtud del proceso de selección*, se debería agregar que esta información como es compartida está sujeta a un acuerdo de confidencialidad por la sensibilidad de la información.

Primera Objeto, *sobre el acuerdo de confidencialidad de que la parte receptora no debe divulgar la información confidencial sobre los procesos ilegales de Cyberfort*, éticamente esta mal pues las personas que son seleccionadas son profesionales que deben asumir un rol serio sobre el cargo asumir para cualquier d ellos dos grupos de la organización y seria ilegal conocer procesos ilegales que no están debidamente corregidos ya que estos podrían ser anunciados ante la rama judicial y quizás puedan hacerse suspensión de la organización.

Cuarta obligación, punto tres, *no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros*, seria ilegal el no informar sobre las activades de espionaje que intervenga con información de terceros, pues si el trabajo es claro que la organización debe realizar es necesario informar actividades y estar atentos a que posibles cambio se ejecuten, que interrumpen la información confidencial que esta segura y en su repositorio.

Octava obligación, en caso de información ilegal el receptor debe acudir a un abogado privado y dejar exenta de cualquier responsabilidad, no es ético dirigirse a un abogado privado, esta información que es sensible y de contenido delicado dese ser tratado con los abogados de la organización para el uso adecuado y pertinente.

2. Si la respuesta es afirmativa y usted encontró algún proceso ilegal del anexo 3 – Acuerdo: acuerdo, deberá mencionar que artículos de la ley 1273 se podría vulnerar en dicho acuerdo y especificar porque vulnera artículos de la ley 1273

Sobre el Anexo 3 de lo que se halló, lo artículos que pueden vulnerados son:

Primera Objeto, *sobre el acuerdo de confidencialidad de que la parte receptora no debe divulgar la información confidencial sobre los procesos ilegales de Cyberfort*, éticamente, **aplicaría el articulo 269H de la ley 1273, Circunstancias de agravación punitiva**, vulnera en el sentido:
8. Si quien recurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrían por tres años, la pena de inhabilitación para el ejercicio de su profesión, esto es sencillamente el saber sobre estos procesos ilegales y una auditoria del estado puede ejecutar esta ley para los responsables.

Cuarta obligación, punto tres, *no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros*, aplicaría vulnerabilidad en **el artículo 269C[1] de la ley 1273, Intercepción de datos informáticos**, estas actividades de espionaje que no se denuncian porque no tiene una orden judicial son vulnerables para la intercepción de datos informáticos, para origen, destino o que ejecuten emisiones electromagnéticas, pues esto tendría una pena a prisión de 36 o 72 meses.

Octava obligación, en caso de información ilegal el receptor debe acudir a un abogado privado y dejar exenta de cualquier responsabilidad, podría ser vulnerable con el articulo 269J de la ley 1273[2], Transferencia no consentida de activos, esto podría ser consecuente en el sentido de acudir a un abogado privado, aplicaría como transferencia no consentida por cualquier activo en prejuicio por un tercero. Tendría una pena de prisión de 48 a 120 meses, además una posible multa 200 a 1.500 salarios mínimos legales.

---

[1] Mayo 2019. Normatividad sobre delitos informáticos. Policía Nacional de Colombia. Link https://www.policia.gov.co/denuncia- virtual/normatividad-delitos-informaticos

3. Sobre el escenario 2, acerca de procesos legales responder:

   Debe argumentar su respuesta ya sea afirmativa o negativa según la argumentación que dispone COPNIA en su código de ética para ingenieros.

   Sobre las observaciones dadas del escenario y las observaciones en los contratos para el proceso de reclutamiento de futuros ingresos al equipo Blue y red Team que claramente la gerencia no reviso minuciosamente, estaría en exposición de asumir buenos beneficios para asuntos de bienestar como económicamente, calidad de vida, alimentación, transporte, salud mas prestaciones de servicio pero por otro lado la cuestión de permitir las condiciones como muestra el Anexo 3, tendría mucha exposición ante la matricula o tarjeta profesional, y estaría disponiendo en quebrantar los siguientes artículos del código Ética para Ingenieros en Copnia:

   Posible sanción a la tarjeta o matricula por un periodo de cinco años, después de que una autoría encuentra procesos ilegales del contrato y así mismo como se castiga por el debido proceso incorrecto está sujeto a una penalidad por ser actor de la ejecución y ser consecuente de que hay ilegalidad en la acción y no

es corregida como debe ser.

Por otro lado, el articulo 32 Prohibiciones generales a los profesionales, apoya que el reiterado e injustificado incumplimiento a las obligaciones laborales[3] por ejemplo apoyar algún procedimiento que no está debidamente correcto y en lo ético no está bien pues se estaría incumpliendo y no sería justo.

No obstante, otra particularidad vista que puede traer aún más consecuencias y que éticamente no se ve bien es el articulo 45[4] Régimen de Inhabilidades e incompatibilidades que afectan el ejercicio, aplicaría que una actividad que el profesional ejecute con asesores externos de mas de una empresa sin consentimiento o autorización de estas no está bien.

En pocas palabras, el escenario de la Organización CyberFort puede brindar oportunidades con buenos beneficios que tal ves sean propuestas muy convenientes en lo personal y un plus en calidad de vida, aunque la exposición de los procedimientos que demuestra el Anexo 3 trae varias consecuencias que pueden afectar legalmente a la tarjeta profesional, sanciones en que no permita ejercer para más compañías y que este tipo de actividades traen consigo consecuencias legales que podrían efectuar multas o penalidades ante el ministerio de trabajo.

4. Sobre el escenario 2, responder con Ética y mora lo siguiente:

   Hasta que punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoria de seguridad, y como se puede garantizar que este acceso no sea explotado de manera indebida

   Según lo que se tiene de la auditorias de seguridad, pueden varios tipos procedimiento para la ciberseguridad que pueden ser:

   Auditoria de Vulnerabilidades, auditoria de código, auditoria de las redes, auditoria de la web, auditoria forense y hacking ético[5].
   Se supondría que conociendo a la información clave de la organización o empresa se determina los aspectos para audita, haciendo uso de un check list sobre los controles existentes de la protección implementada para sus redes y sistemas, lo cual las acciones correspondientes para el acceso a la información sensible de las empresas de ciberseguridad tiene que tener un acceso controlado en que se implementa una gestión de accesos que garanticen que únicamente que usuarios tienen niveles acceso limitados y el personal interno de la compañía tenga consigo un acceso mas directo a la información sensible, por ello no solo es el acceso, también parte de la información debe estar

protegida con cifrado de datos para estas mismas entidades, en pocas palabras las empr4sas de ciberseguridad podrían estar a pasos cercanos de la información pero con ciertas limitaciones pues su objetivo es identificar vulnerabilidades, escanear posibles amenazas y aplicar sus técnicas de Etical Hacking.

En teoría por políticas asociadas a la gestión de acceso, se debe tener parametrizado accesos de modo lectura, escritura y a que limites tanto del almacenamiento de la información, en la red y en los sistemas, esta responsabilidad seria obtenida del administrador de cada categoría balancear los accesos que se le permita a la empresa de ciberseguridad que tenga que correr sus trabajos de análisis.

- Que mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables

De primera estancia tener sus herramientas estándar para las debidas actividades de ciberseguridad en sus clientes, estos podrían ser utilidades que permitirían la supervisión de cada integrante de la empresa:

Software antivirus, permite identificar en detalle de las conexiones del dispositivo, conexión a otros dispositivos físicos por medio de la red, físicamente o enlaces remotos. Este podría facultar a través de reportes de log de eventos que actividades ha realizado el personal de ciberseguridad si cumple con las actividades debidamente correctas en cada procedimiento de las técnicas de hacking.

Software para detención, es un agente que puede ser instalado en los equipos de cada integrante y podría analizar qué tipo de conexión se realiza por medio de web que sea una fuga de conexión a externos.

Por último, otra utilidad que puede ayudar en ser supervisor de todo tipo de actividades es el Firewall perimetral de red, por medio de reglas realizara ejecución de permitir y bloquear, quizás cuando existan intentos de acceso poco comunes se mostrara un registro de eventos que permitirá identificada el punto origen y destino para asociar si son accesos no autorización y sean una posible fuga para la información de las empresas clientes.

Con estas herramientas podrán ser útiles el tipo de trabajo que realizan los ingenieros de seguridad y así mismo se evaluara su ética en cuando a las actividades que se asignan y logren obtener los resultados esperados para la proyección de la información.

Inicialmente, como entidad tercera de ciberseguridad que estará en pro de hacer trabajos

para garantizar que sus clientes estén seguros y tengan una reacción inmediata a las amenazas vistas del día, es necesario y se exige que tenga una experiencia legal, cumplimiento e investigación para poder comunicarse de manera afectiva con los Stakeholders.

El trabajo que se debe pactar entre la organización es y la empresa de ciberseguridad, se debe tener acuerdos con clausulas de castigo y penalidades monetarias, todo ello debe ir sujeto a las leyes de la rama judicial.
Debido pues una falla o algún tipo de conducta o comportamiento, podría no solo afectar la licencia o matricula del ingeniero de seguridad que no trabaje en un determinado tiempo quedando señalado en hoja de vida, la empresa de ciberseguridad podría estar sujeta según la falta que tipo de penalidades deba pagar por incumplimiento a la confidencialidad de la información y si aun en un escenario más grave, las organizaciones podrían tener el derecho de acusar o demandar a la empresa de seguridad que podría tener afectación con el ministerio de trabajo y otras entidades.

Todo esto podría minimizarse a un cumplimiento de objetivos y estar atado a ciertas clausulas para que ambas partes estén de mutuo acuerdo y se de la respectividad de confianza que se trabaja con personal de seguridad de buenas intenciones.

6.3 ESCENARIO 3

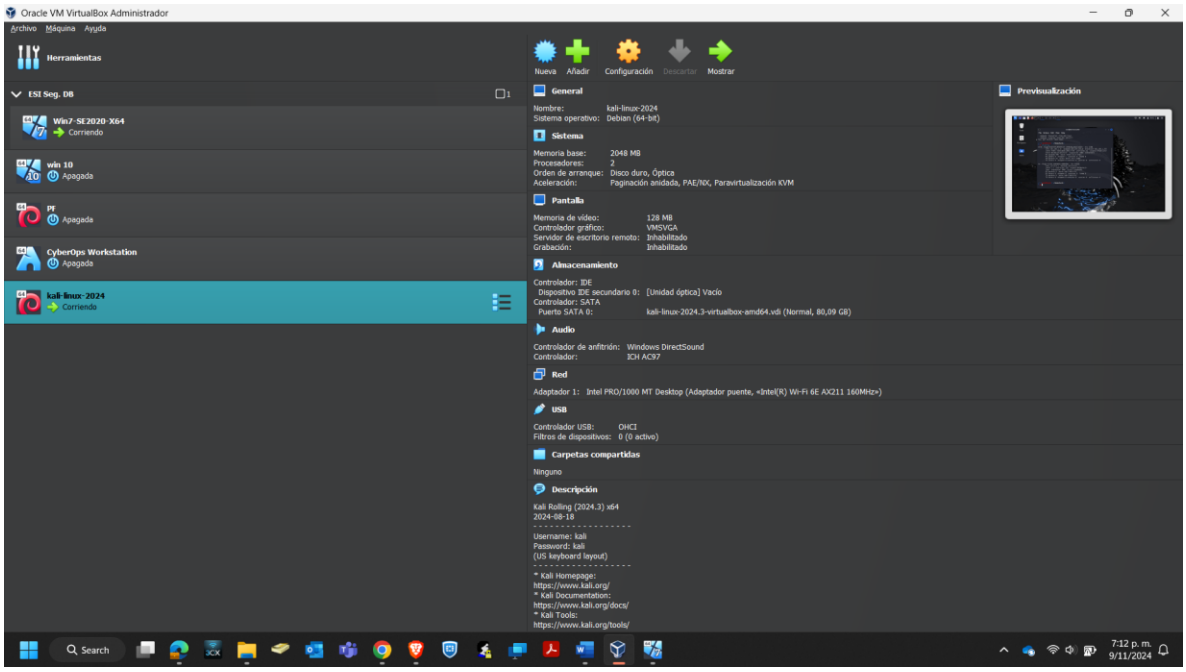
1. **Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos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

   En el presente informe de contexto académico se utilizaron las herramientas vistas durante el transcurso de la materia, pero en especial la Máquina VirtualBox versión junto a la herramienta combinado con Nmap y Metasploit Framework, así como Metasploitable2, que en este caso simula la organización para la cual estamos realizando la consulta de Pentesting.

   Una vez, contando con los permisos que la organización nos ha concedido, procedemos a intentar ingresar, aprovechando esta vulnerabilidad, obteniendo los resultados esperados para el desarrollo de la actividad.

   Una vulnerabilidad de seguridad se puede ver como el punto de partida de todo el proceso que implica la seguridad en general, su presencia puede permitir alterar el comportamiento normal de un programa (realizar algo malicioso como alterar información sensible, interrumpir o destruir una aplicación o tomar su control).

Ilustración 14. Configuración de las máquinas virtuales en virtual Box

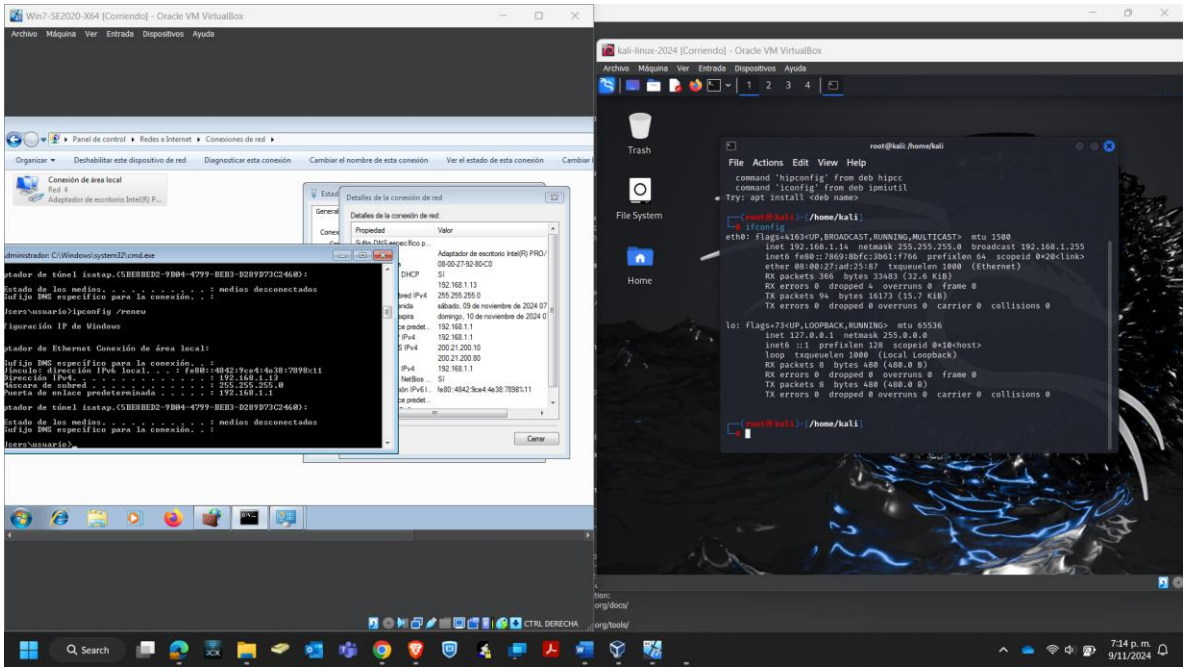


Elaboración propia

Ilustración 15. Validación que ambas maquinas estén por adaptador de puente desde virtualbox

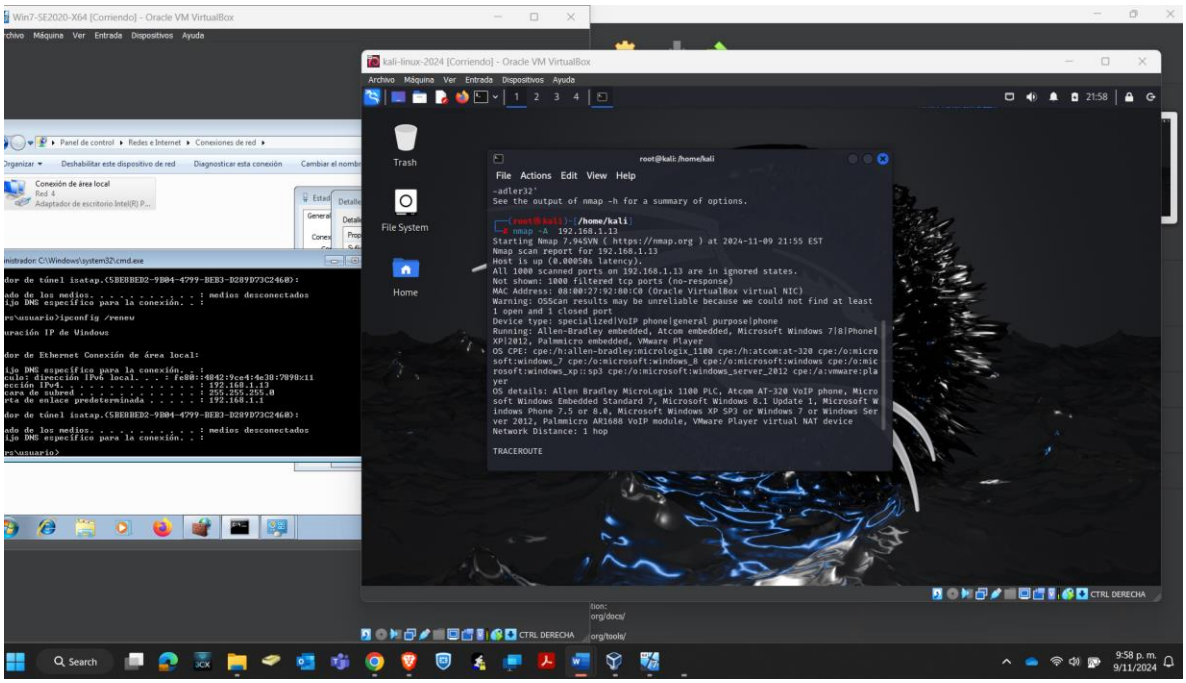
Elaboración Propia

Ilustración 16. Comprobación que tengan el mismo segmento de IP



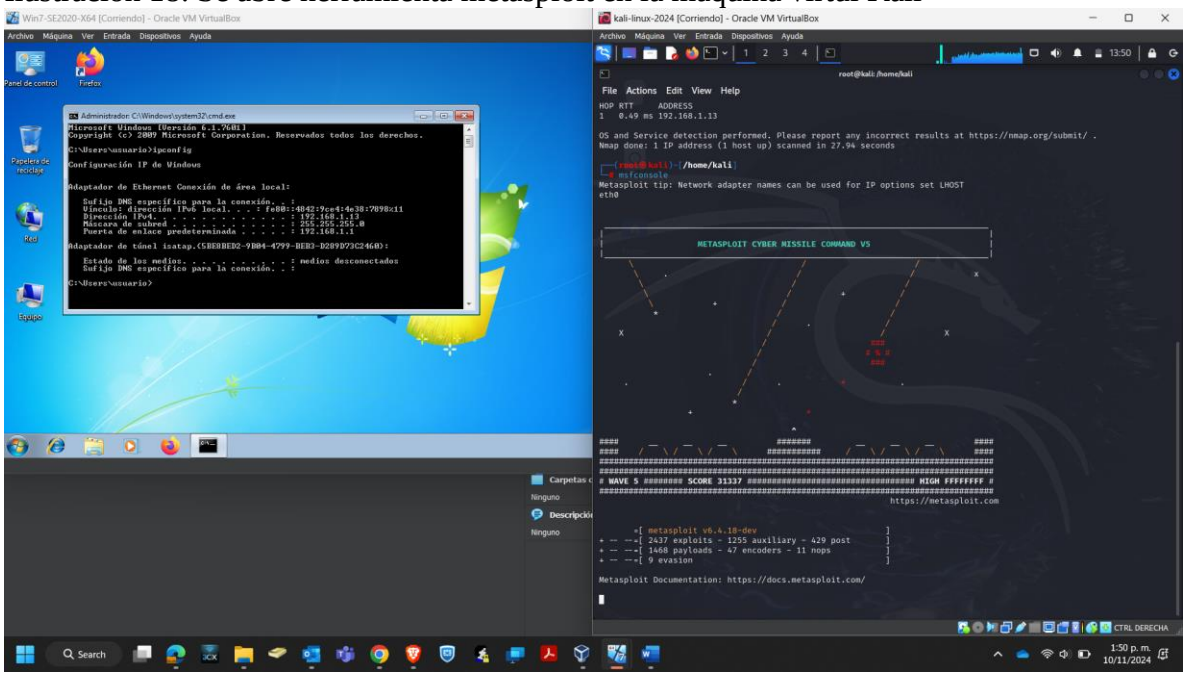
Elaboración propia

Ilustración 17. Ejecución del comando nmap -A de la IP de la maquina win 7 para analizar el rastreo de puertos



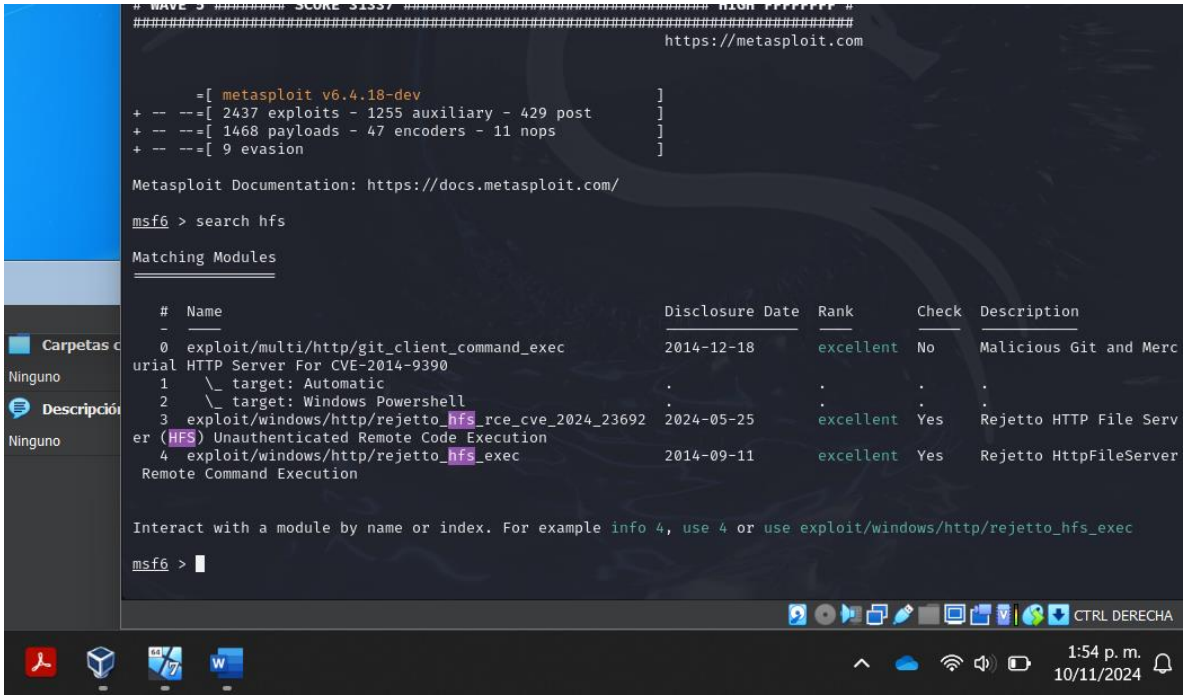
Elaboración propia

Ilustración 18. Se abre herramienta metasploit en la maquina virtul Kali



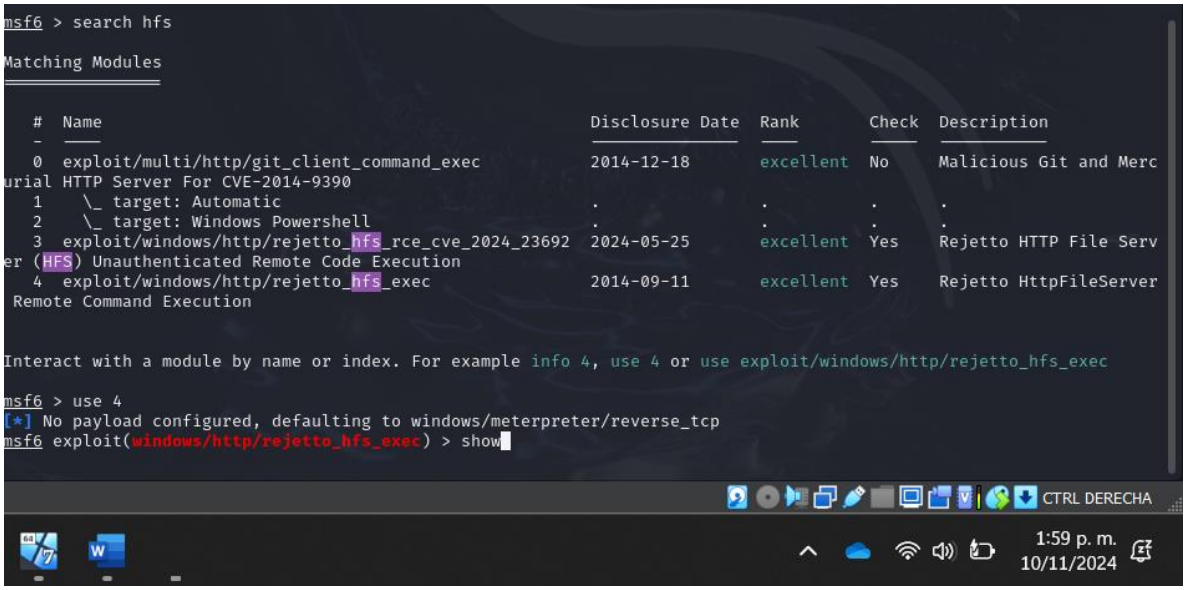
Elaboración propia

Ilustración 19. Búsqueda de un hfs en Metasploit



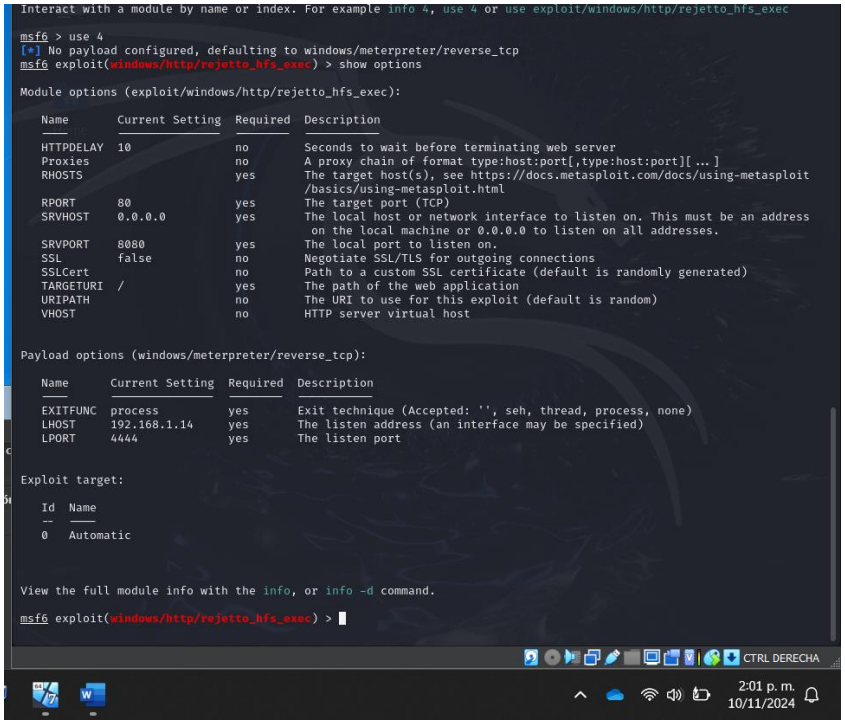
Elaboración propia

lustración 19. Selección el deploy del Windows 7



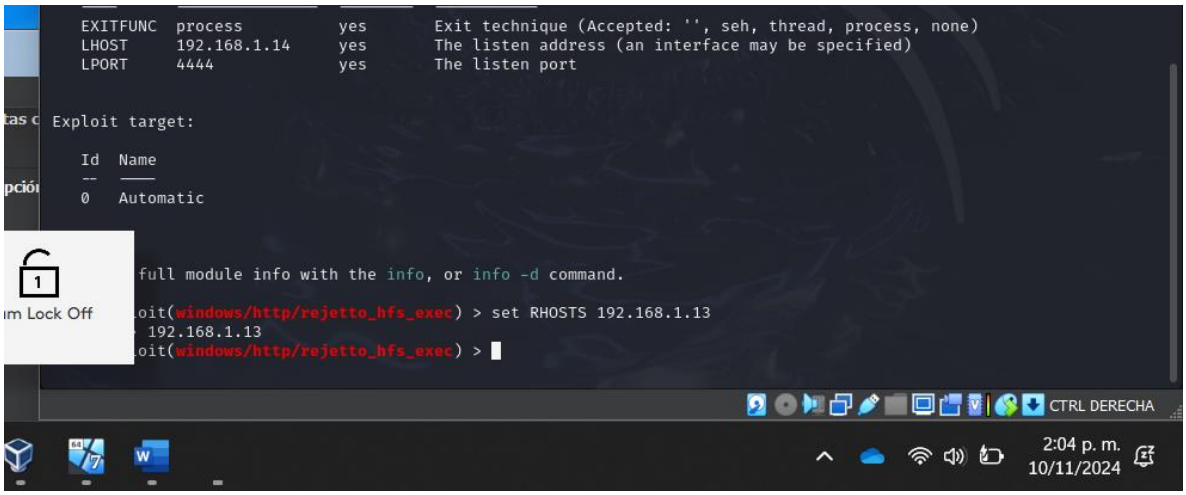
Elaboración propia

Ilustración 20. Demostración de opciones



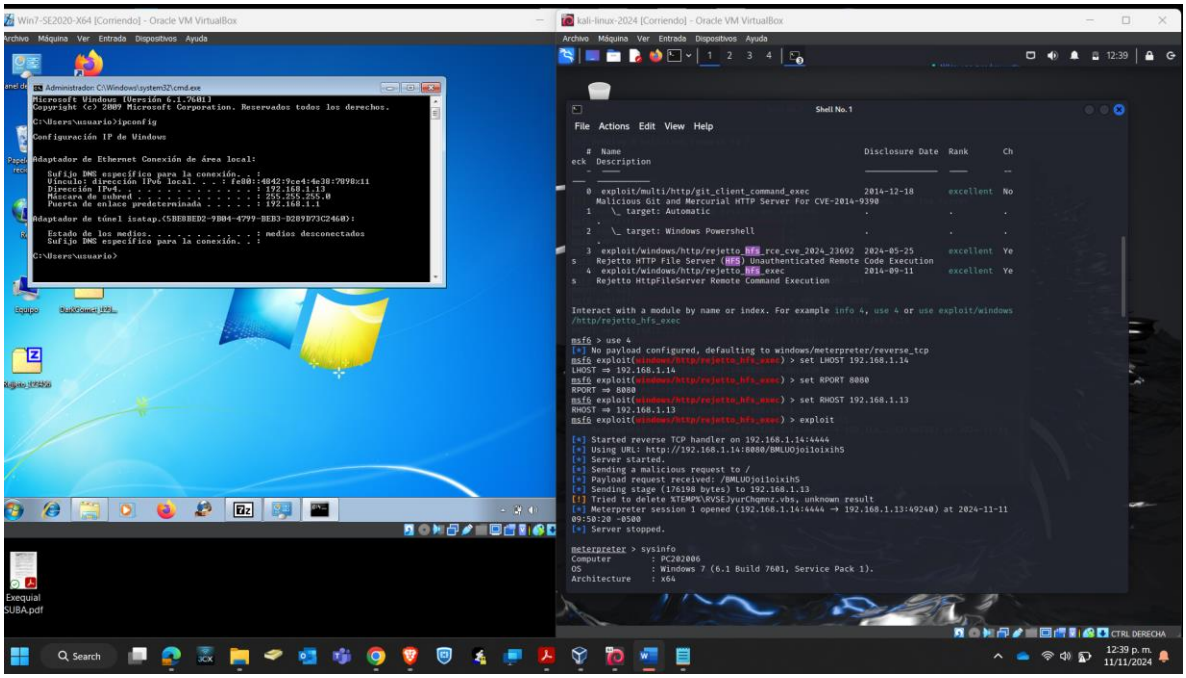
Elaboración propia

Ilustración 21. Validación del equipo remoto WIN 7



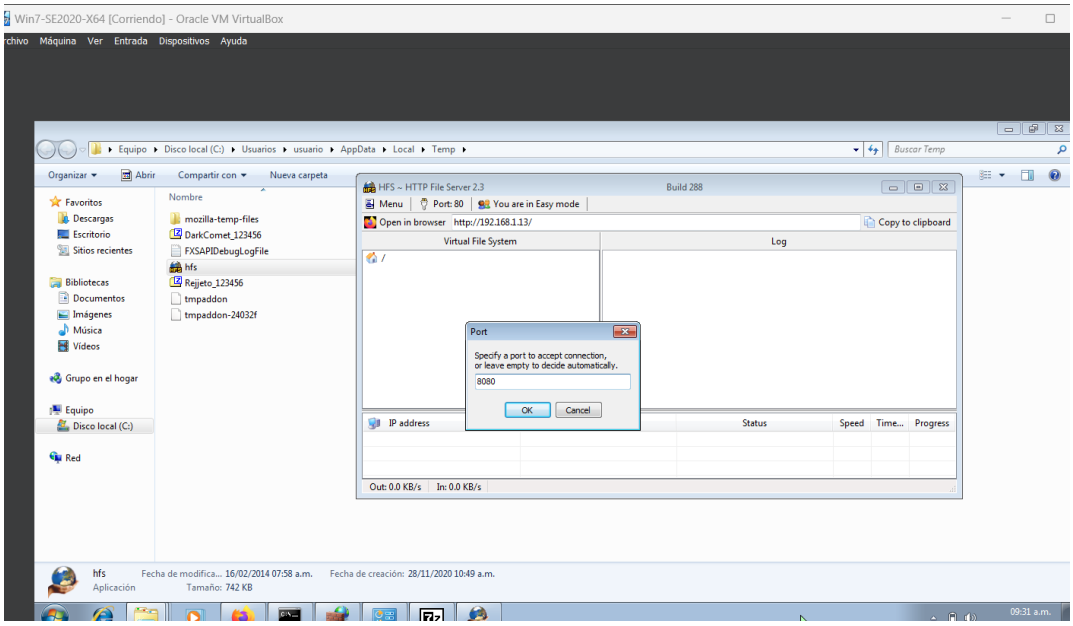
Elaboración propia

Ilustración 22. Ejecución del exploit en Metasploit



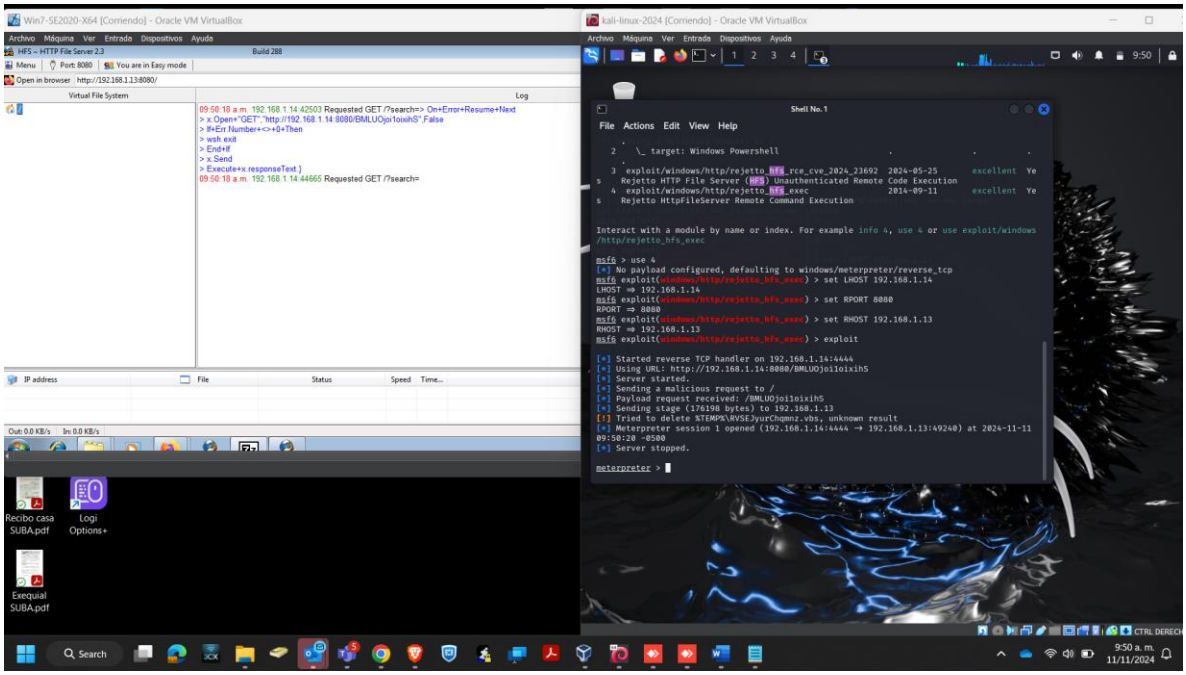
Elaboración propia

Ilustración 23. Configuración HFS en el puerto 8080



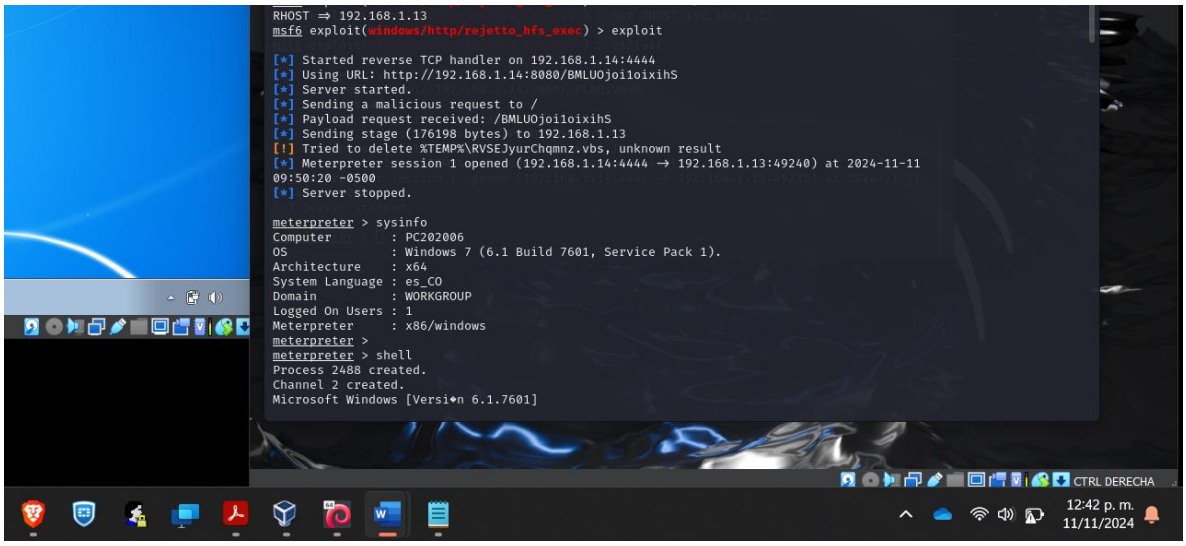
Elaboración propia

Ilustración 24. Ejecución exploit de la maquina Kali a la maquina WIN 7



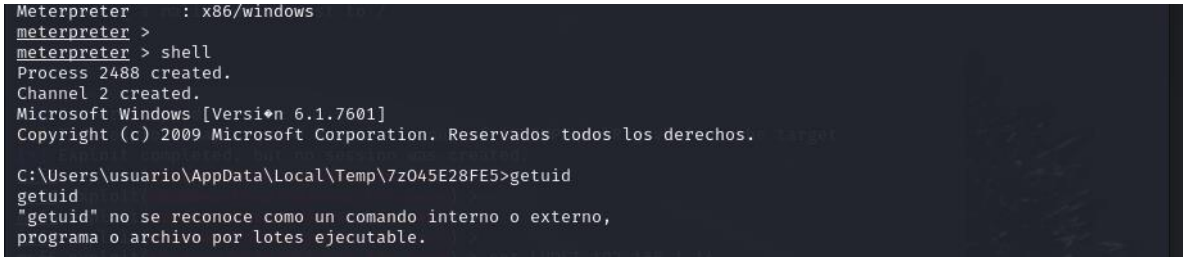
Elaboraicon propia

Ilustración 24. información del equipo win 7 atacado



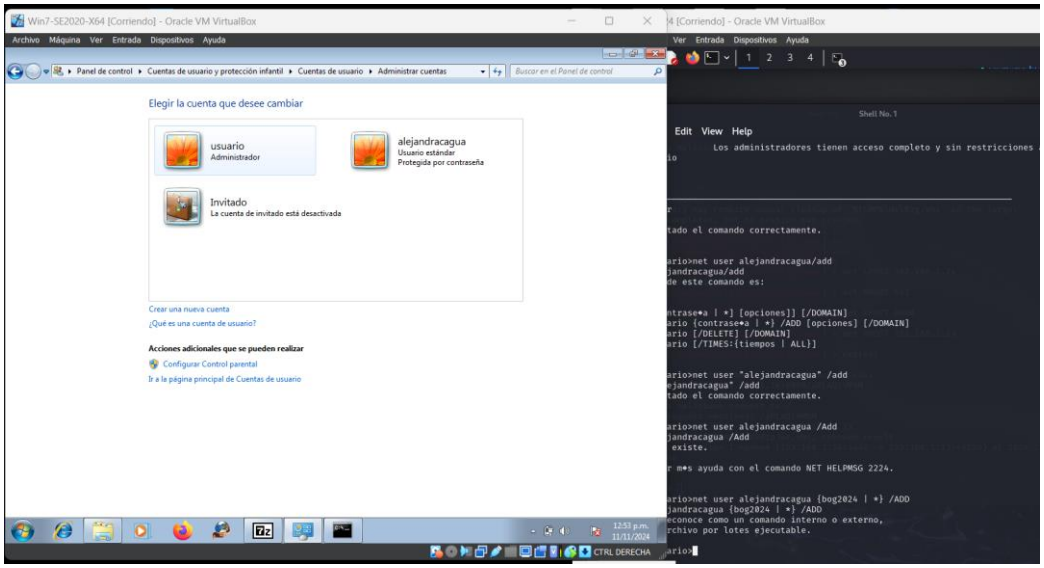
Elaboración propia

Ilustración 25. Configuración Shell en Kali Linux



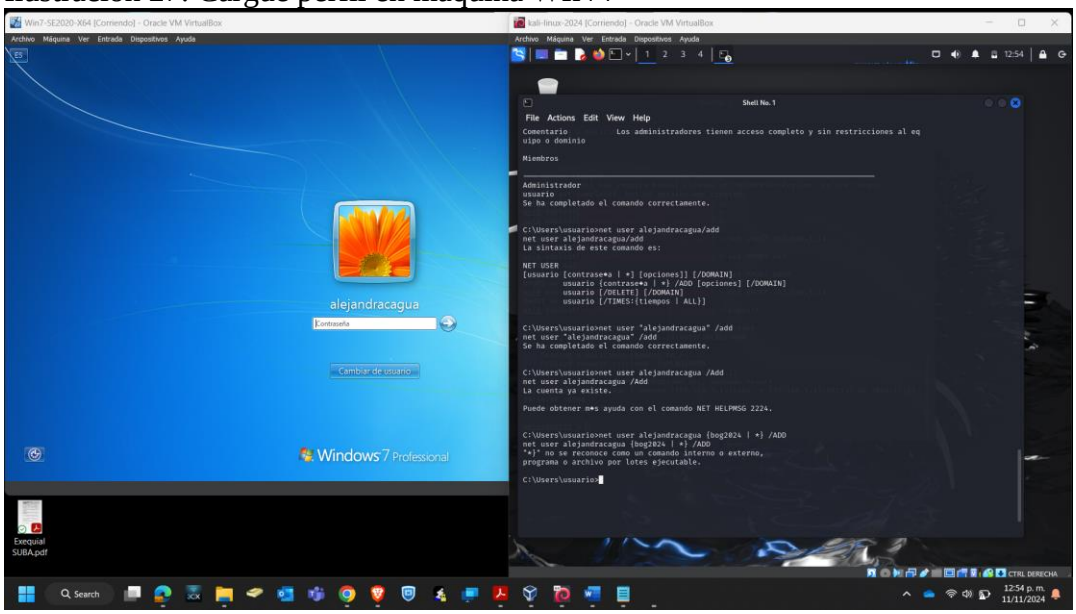
Elaboración propia

Ilustración 26. Validación de usuarios de la maquina WIN 7



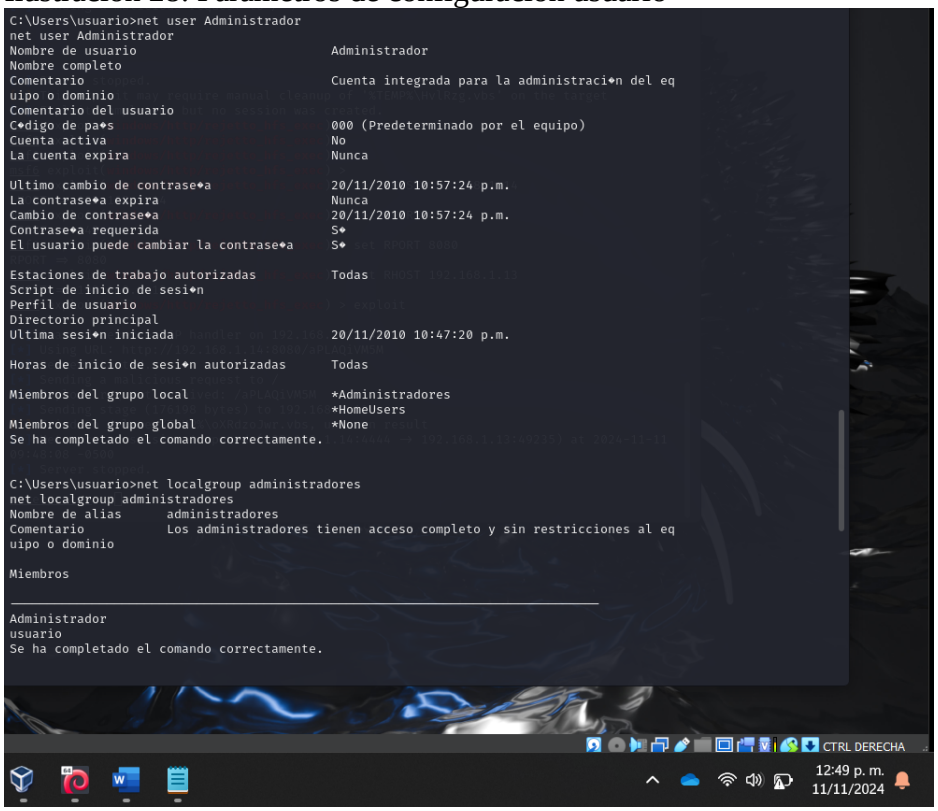
Elaboración propia

Ilustración 27. Cargue perfil en maquina WIN 7



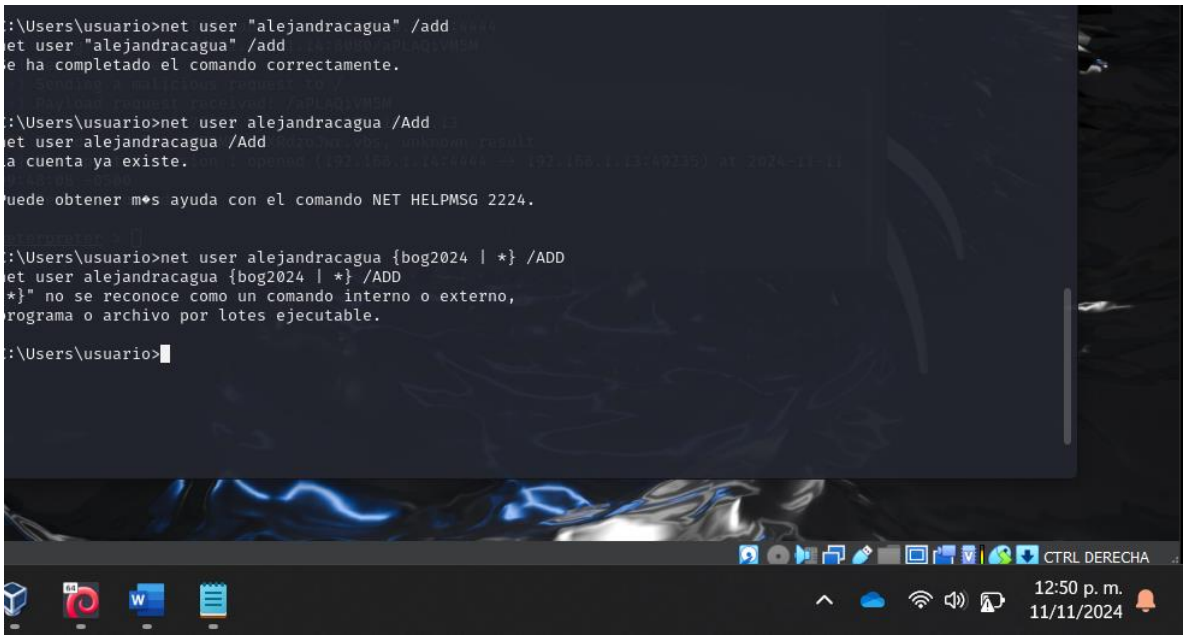
Elaboración propia

Ilustración 28. Parámetros de configuración usuario



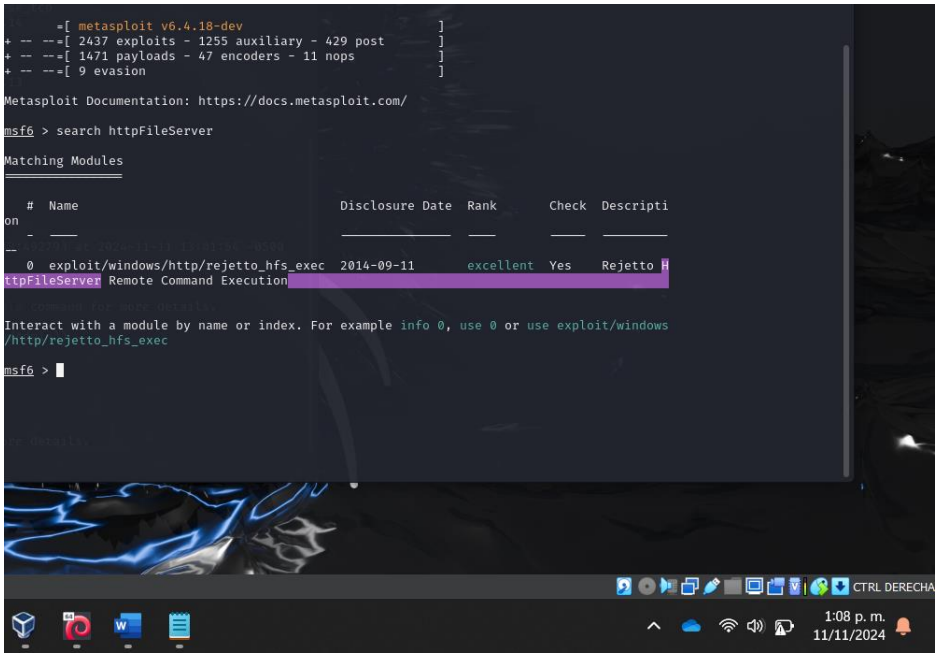
Elaboración propia

Ilustración 29. Creación usuario local en la maquina WIN7



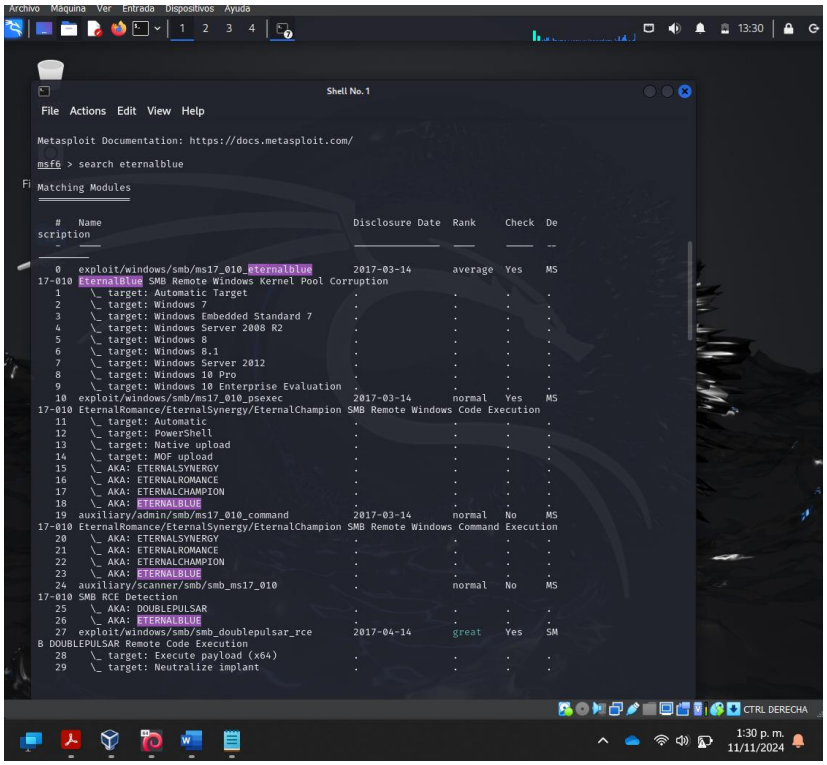
Elaboración propia

Ilustración 30. Escaneo por metasploit en búsqueda de vulnerabilidades



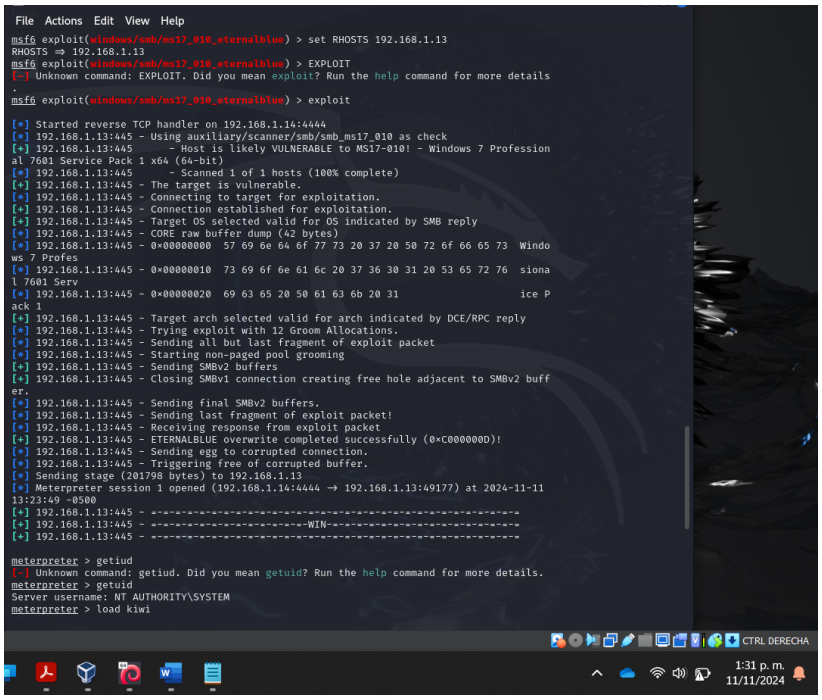
Elaboración propia

Después de haber creado el usuario, se correrá exploit para un hash
Imagen 20. Ejecución de EternaBlue



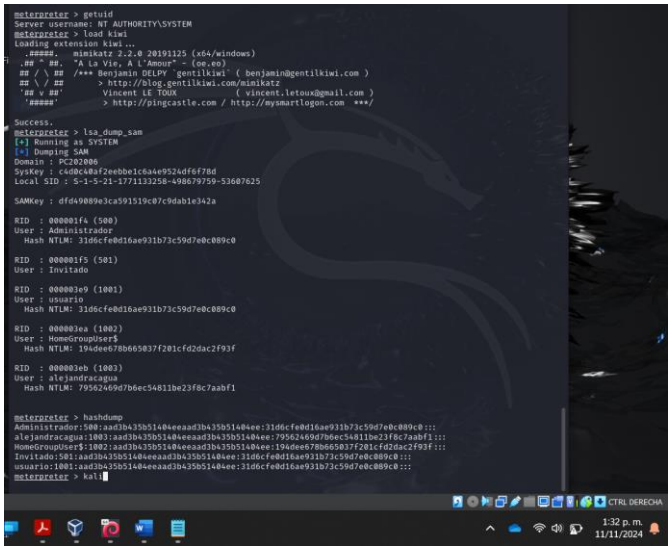
Elaboración Propia

Imagen 21. Ejecución del exploit



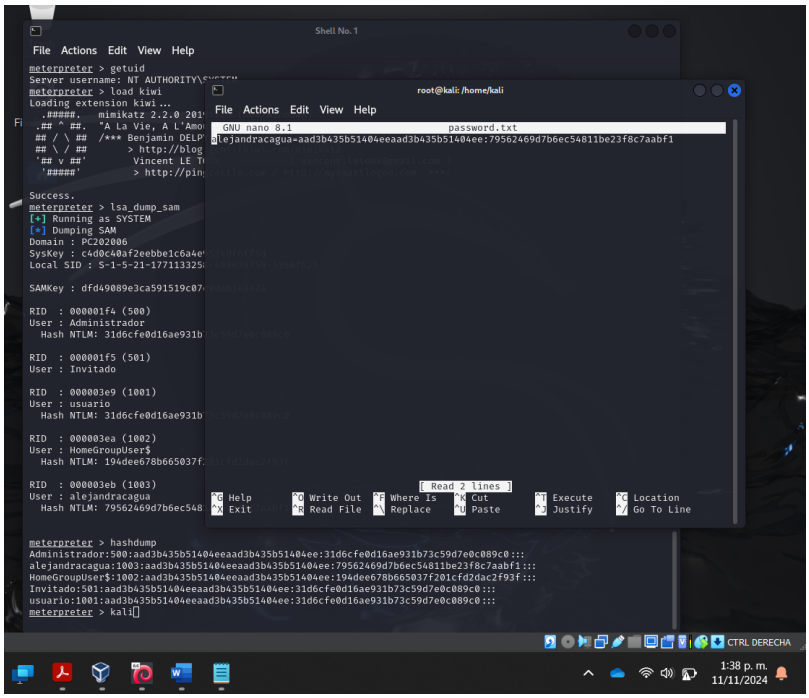
Elaboración propia

Imagen 22. Elaboración del Hash



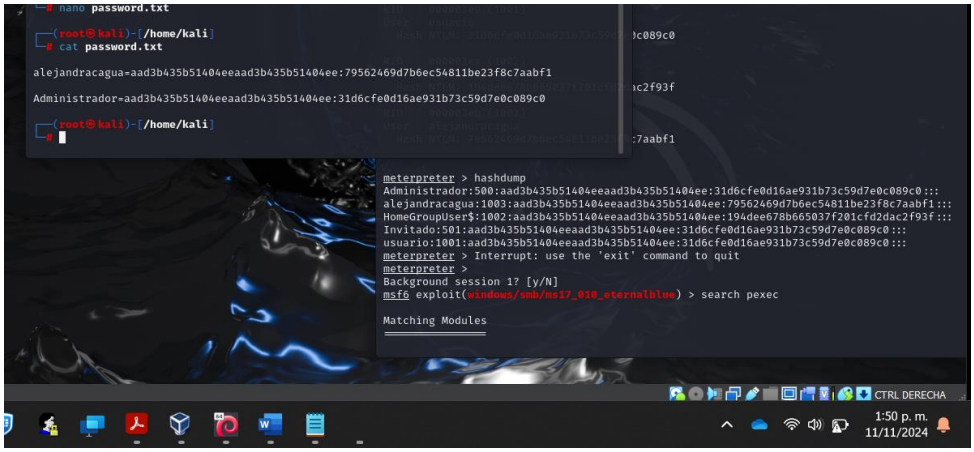
Elaboración propia

Imagen 23. Se copia hash en la terminal de Kali



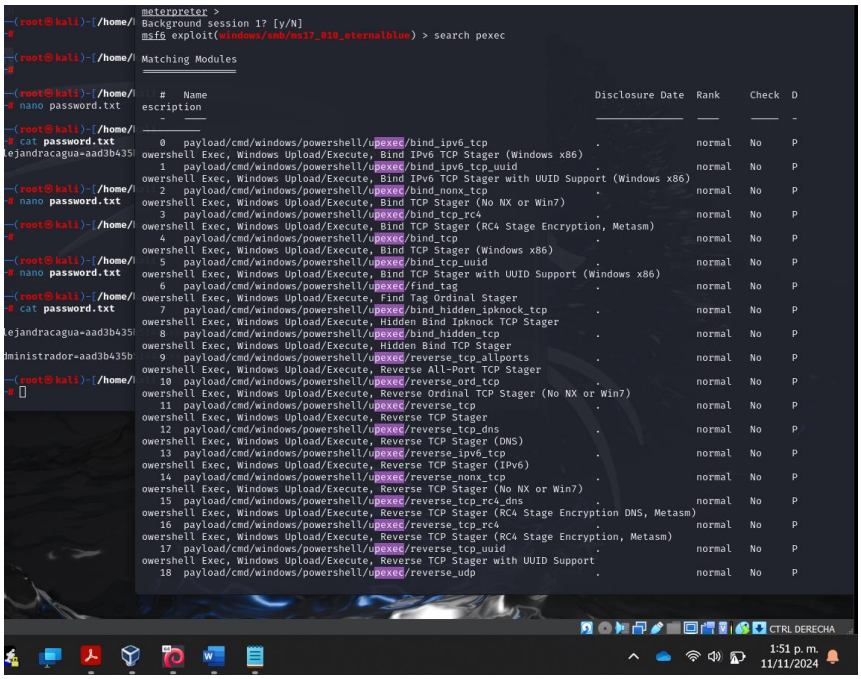
Elaboración propia

Imagen 24. Comprobación del hash con el usuario creado para la maquina WIN 7



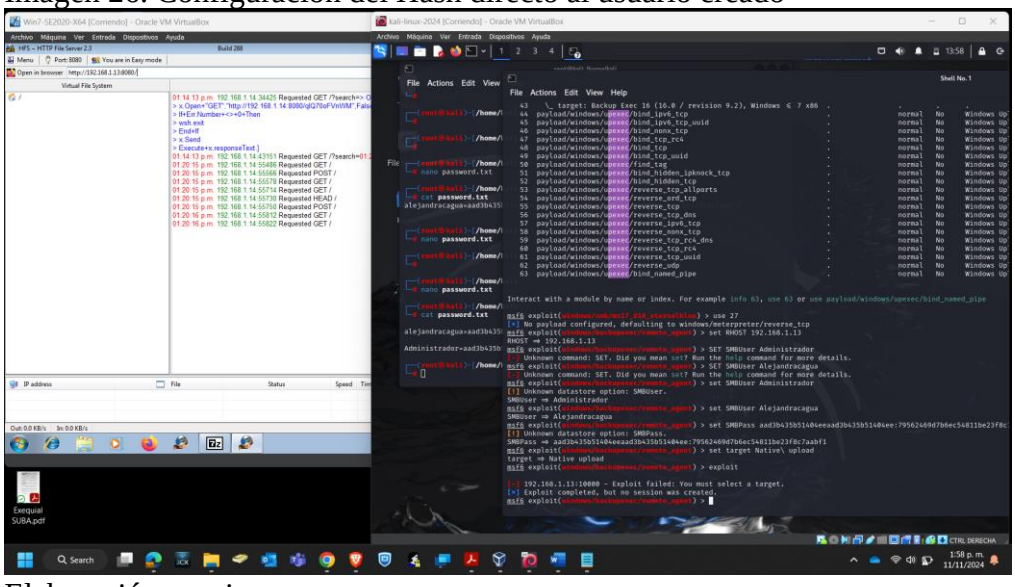
Elaboración propia

Imagen 25. Ejecución del Search Pexec



Elaboración propia

Imagen 26. Configuración del Hash directo al usuario creado



Elaboración propia

2. Sobre el anexo 4 escenario, imaginese un ataque en tiempo real y responda:

Con el propósito de evidenciar una efectiva defensa de los equipos de Blue Team, focalizados en la seguridad defensiva, protegiendo los sistemas y sobre todo los datos, contra los riesgos que representa las diferentes amenazas cibernéticas, monitoreando la red, detección oportuna y generar respuesta efectiva a los incidentes que afecten la

política de implantación de una entidad la clasificación de las vulnerabilidades y su respectiva gestión.

Analizando dichos focos se tuvo en cuenta informes estandarizados de las metodologías y las entidades, de las cuales se extrajo, lo ítems, procedimientos y funciones de estos profesionales, con el fin de clasificar y evaluar las taras para individualizar y priorizar las estrategias.

3. Sobre la falla de seguridad que puerto identifico:

A esta actividad se le conoce como pentesting que estas compuesto por dos palabras, una es penetración y la otra de test, cuyo objeto es determinar si las políticas de seguridad de la información que buscan la autenticidad, integridad y confidencialidad se conserven dentro de una organización.
Mientras el escaneo de vulnerabilidades está enfocado en la transmisión de datos y la manera en que los mismos pasan por las diferentes capas, aplicado en software y hardware cuyo fin es determinar la existencia de alguna vulnerabilidad y si la misma es interna o externa a la organización, por otra parte, una prueba de penetración puede tener otro tipo de contexto, ya que en la prueba de penetración se observa desde la implementación de las Políticas de Seguridad, confirman su eficiencia, la eficacia, por ende las mismas no son solo en software o hardware, sino que contemplan otras variables que se encuentran contenidas dentro de las políticas de la organización.

Nmap es una herramienta de mapeo de redes. En este caso nos interesa conocer los puertos que se encuentren abiertos, por lo que utilizamos las siguientes flags o argumentos:
-A : Habilita la detección de SO y de versión, es decir, va a intentar conocer el sistema operativo que está corriendo nuestro objetivo, junto al servicio asignado a cada puerto y su versión.
-p- : Escanea absolutamente todos los puertos. Por defecto, nmap sólo escanea los puertos más comunes, pero puede que haya otros que contengan información.

Para este ejercicio el puerto 443 es el puerto HTTPS por defecto, este puerto este asociado a las comunicaciones de las redes seguras. Utiliza el protocolo HTTPS, que es la versión segura de HTTP. Para este protocolo se incorpora protocolos de seguridad más fuertes.
El puerto 443 utiliza protocolos TLS para proporcionar una conexión segura entre el cliente y el servidor. De este modo, cualquier dato transmitido a través de este puerto

se encripta, lo que garantiza una conexión segura y protege la información de posibles fisgones.
Este puerto es esencial para los sitios web de comercio electrónico y banca en línea, donde se transmiten datos confidenciales como números de tarjetas de crédito y datos bancarios.

4. **Demuestre como esta falla puedo afectar a la seguridad informática según el escenario 4**

Para fortalecer los procesos que contribuya a la reducción de los riesgos, se establecieron instrumentos de recolección de información los cuales, permiten establecer los parámetros esenciales para estructurar de una manera adecuada y acorde a las necesidades, recopilando información como experto en ciberseguridad, para continuar analizando los datos recopilados, después de realizar cuantificación y la decodificación de los instrumentos de recolección de información.

El análisis se focalizándose en sus componentes tecnológicos que permitan las conexiones de los equipos terminales con los servidores y a su vez la trasmisión en tiempo real de la información.

Gestionar las debilidades del sistema, a la entidad siempre estará acompañada de soluciones oportunas que garanticen menor porcentaje de riesgo dedicado a tratar las fragilidades del sistema Windows el cual le fueron desactivados todas las herramientas de protección.

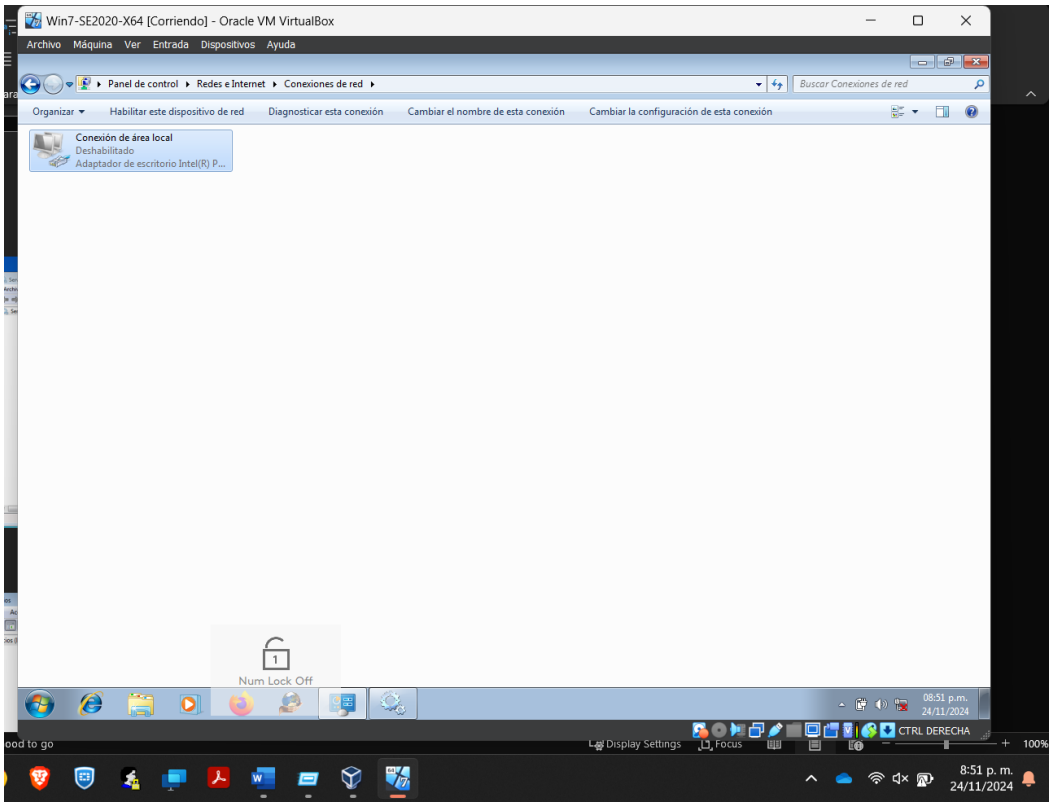
6.4 ESCENARIO 4

5. **Demostrar cómo se trataría el ataque en tiempo real**

Primero, preferiblemente aislar el equipo comprometido de la red:

Una vez detectada la red con este ataque puntual se debe proceder apagar el equipo de la red, desconectarlo físicamente de cable de red RJ45

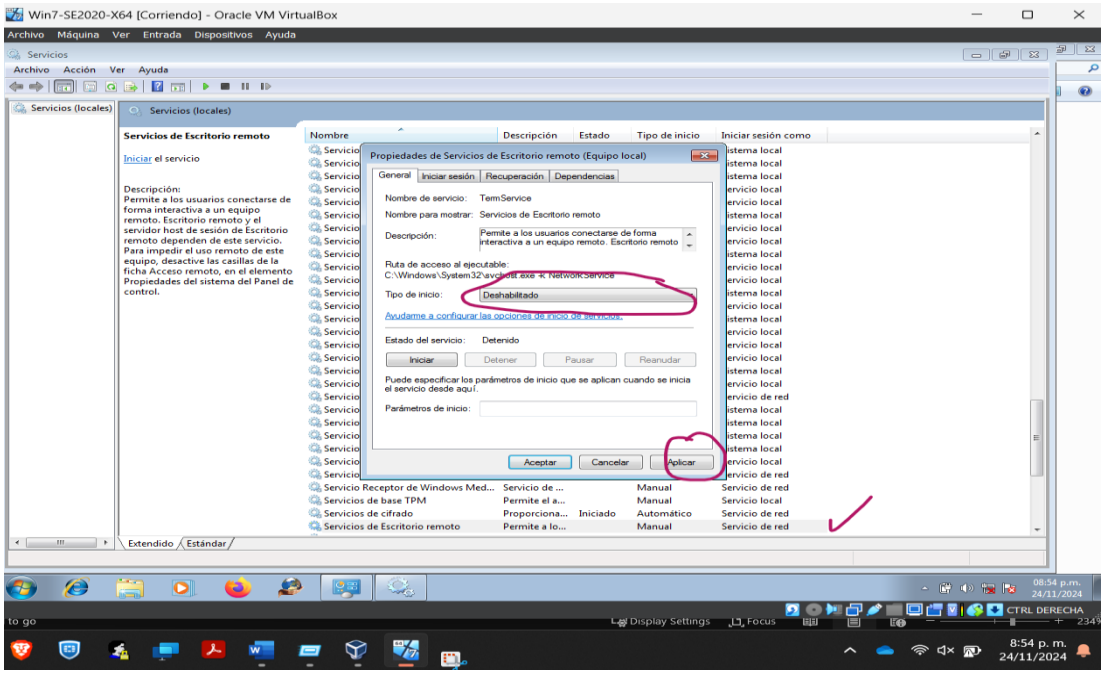
Imagen 1. Equipo afectado desconectado de la red.



Elaboración propia

Luego deshabilitar accesos remotos desde los servicios del quipo afectado.

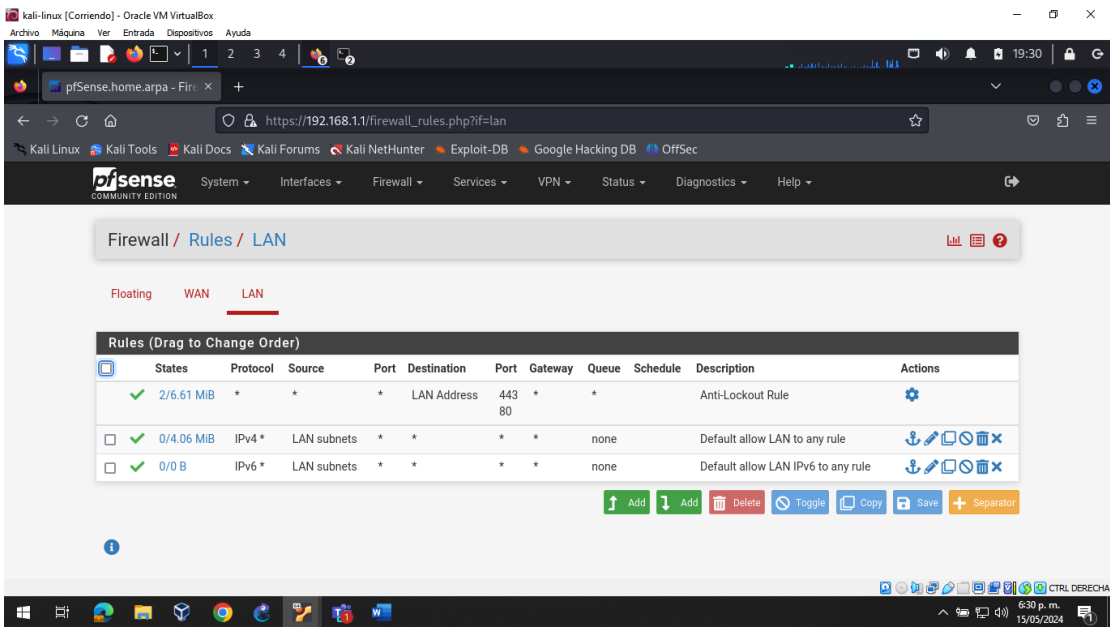
Imagen 2. Servicios en Windows 7



Elaboración propia

Por parte de la administración en redes debe configurar, limitar bloqueo y trafico de puertos

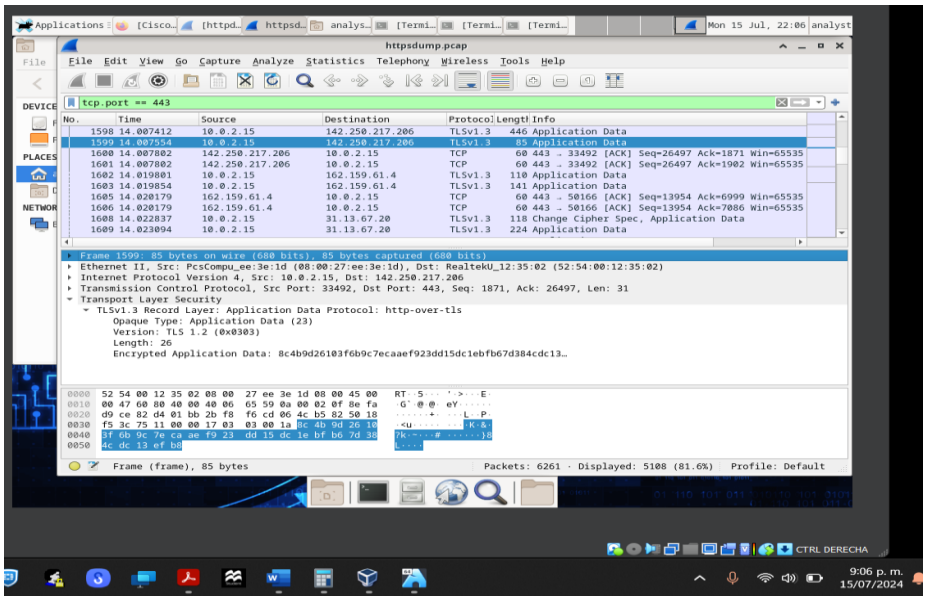
Imagen 3. Configuración desde la red LAN y WAN en el Fortinet



Elaboración propia laboratorio unad

Luego para ver el trafico de la de la red se puede usar el software Wireshark para monitorear el análisis de tráfico, conexiones sospechosas y actividad de ataques.

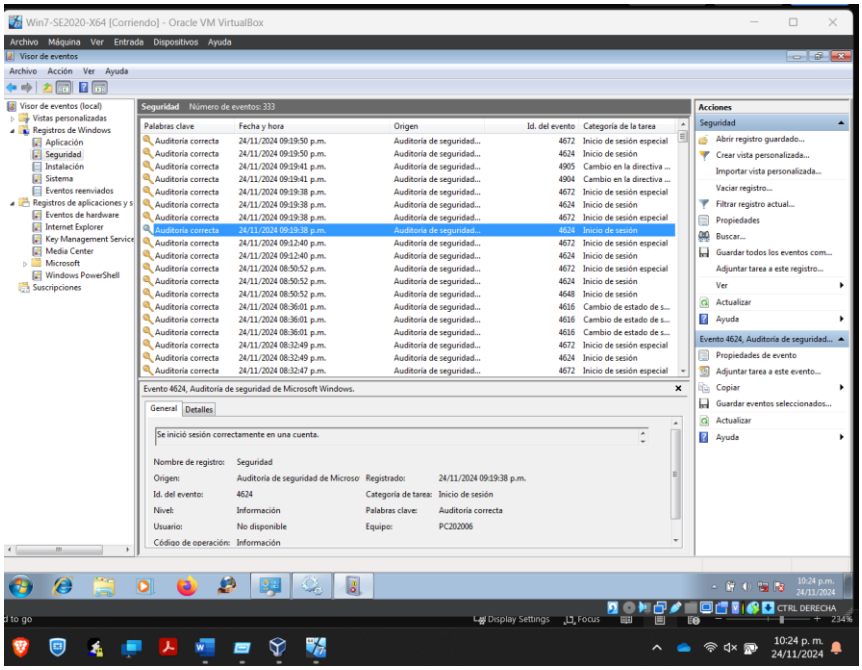
Imagen 4. Escaneo tráfico en Wireshark



Elaboración propia laboratorio unad

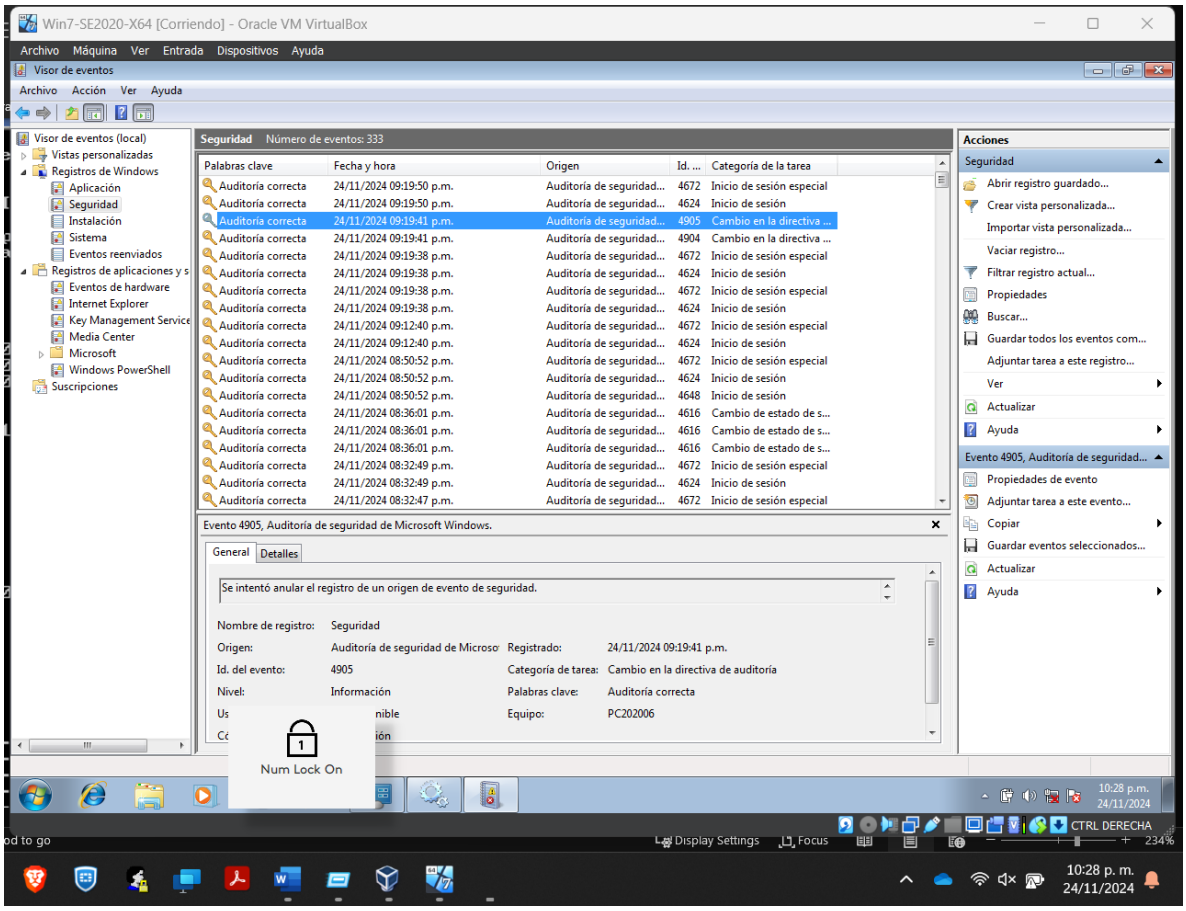
Validación de logs del sistema operativo para ver que aplicaciones compromete

Imagen 5. Registro de eventos de Windows



Elaboración propia

Imagen 6. Validación evento de cambio en la directiva de grupo

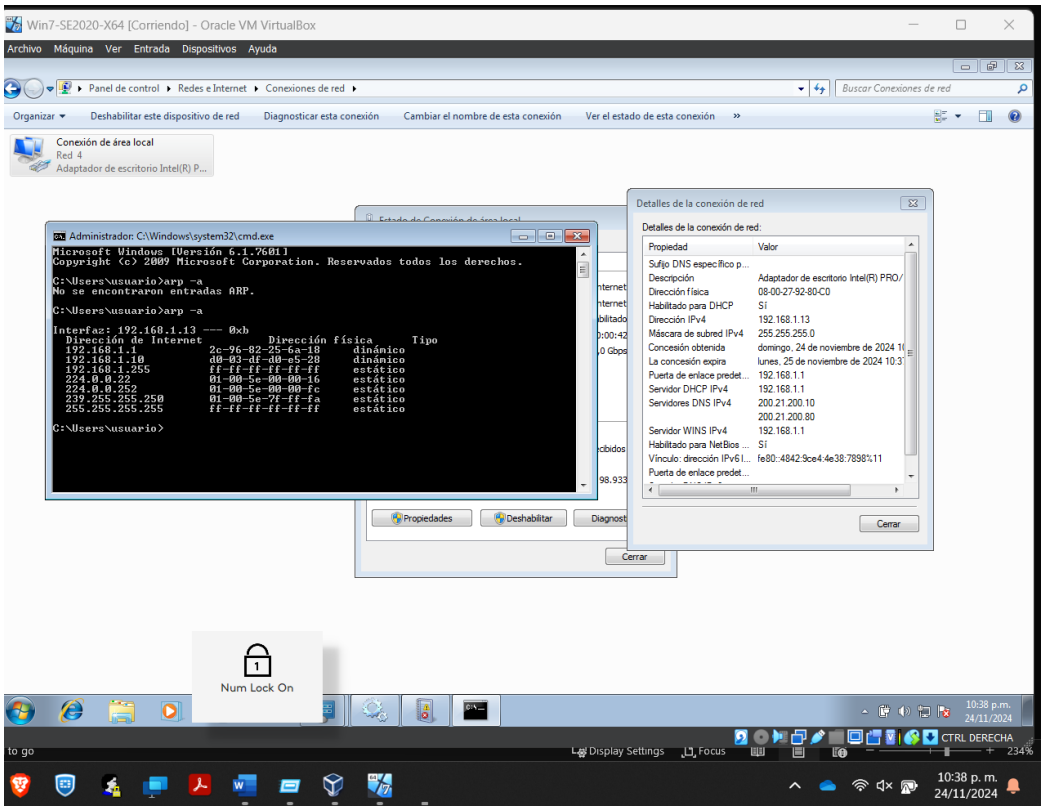


Elaboración propia

Se observa actividad del usuario creado alejandracagua con sus detalles, creación, ID de usuario y también se valida que privilegios tiene el usuario.

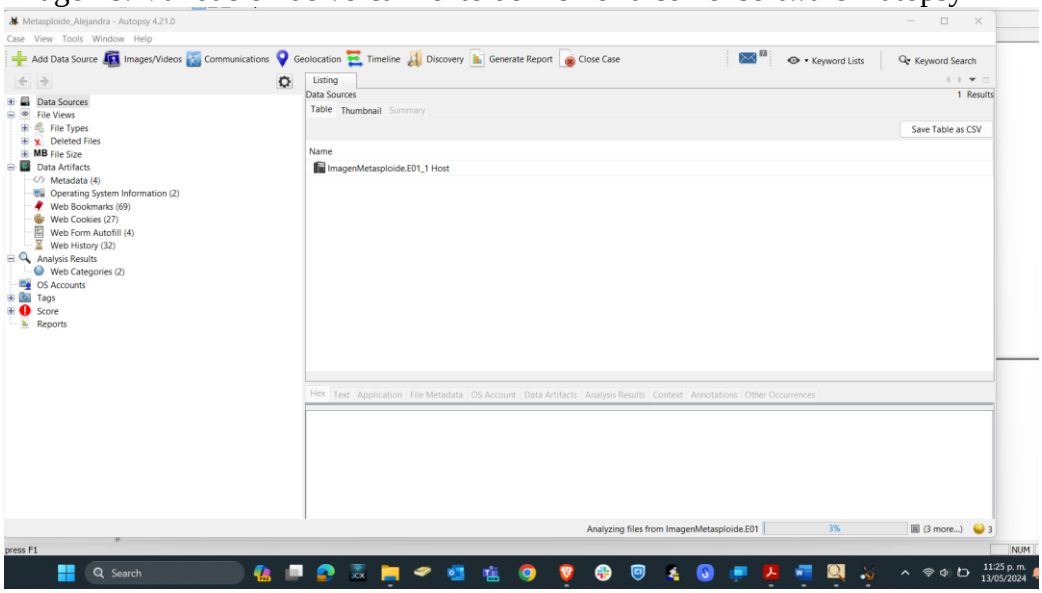
Por otro lado, después de estas revisiones se puede ver con el usuario actual de la maquina víctima, se puede usar la herramienta cmd con los comandos permite ver que el comando ARP, donde mostrara las IP y mac de los dispositivos que han comunicación en la red.

Imagen 7. Tabla ARP de la maquina victima



Elaboración propia

Imagen 8. Validación de volcamiento de memoria con el software Autopsy



Elaboración propia laboratorio UNAD.

Después de estas revisiones es importante informar el incidente, es necesario tener compartimiento con prudencia, de manera que solo se entere las personas autorizadas.

Contener los daños es de extrema importancia realizarlo de manera oportuna en la gestión de la incidencia, priorizando las acciones según la forma de ponderar los recursos afectados entre las personas, información y equipos tecnológicos.

Luego, presentar un informe a la Gerencia y Dirección de tecnología demostrando las vulnerabilidades del ataque, que recursos compromete y el porcentaje que afecte a los servicios de Tecnología.

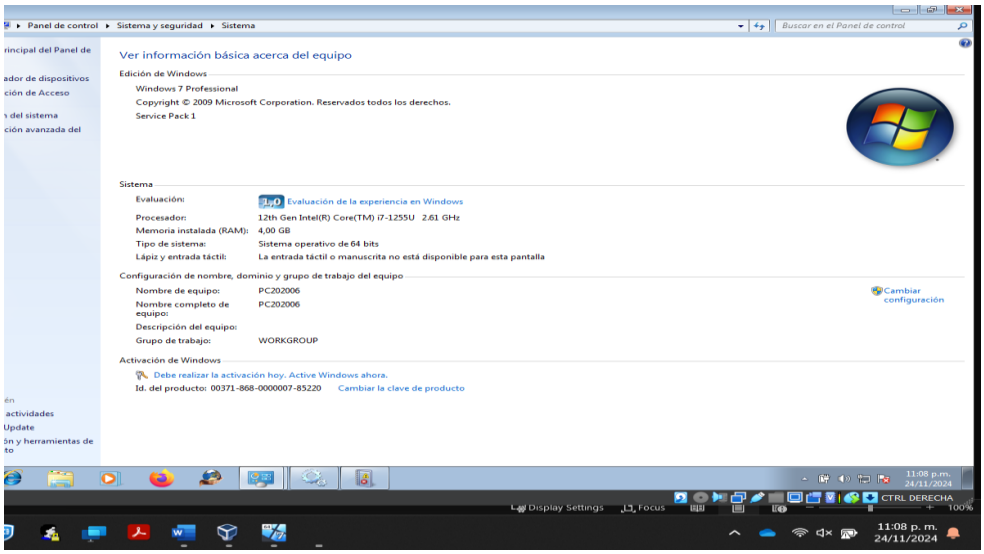
Por último, realizar las acciones que se prometieron hacer y en pate buscar medidas preventivas para tomar acciones correctivas, así mismo ver como funciona toda la arquitectura de red y servicios, para finalizar capacitar al personal sobre los nuevos cambios en ejecución.

Cabe resaltar que se debe fortalecer las políticas de seguridad que se implementen desde el directorio activo y también reglas que se configuren en el Firewall.

6. **Teniendo en cuenta el ataque ejecutado desde el ejercicio de red team, que medidas de hardenizacion propondría para que el ataque no se repita.**

Con el propósito de hardenizar las máquinas virtual con Windows, tenemos necesariamente que verificar y activar todas las herramientas de seguridad que posee el sistema operativo, Windows defender y los firewall, los cuales están pre instalados con los requisito necesarios para el propósito, en el cual se deben configurar las actualizaciones y los respectivos parches de seguridad que tiene destinados él y otorgados por Microsoft, se realiza la revisión de puertos los cuales necesariamente toca tener habilitados si el fin del equipo es mantener conexión con otros equipos y redes, se ejecutan las actualizaciones vigentes en ese entendido los atacantes no lograran utilizar ese puerto, se verifica nuevamente los sistemas de seguridad y la activación de los mismos, focalizadas en desactivar las opciones que permitían las conexiones con asistencia remota, toda vez que esta conexión fue la que permitió el ataque, de manera que a partir de ahora se instalen los parches, al realizar esta configuración se encuentran las actualizaciones requeridas las cuales son instaladas y que no tienen costo, si se quisiera una harderizacion más fuerte se podría contratar servicios de pago para obtener mayor eficiencia y eficacia.

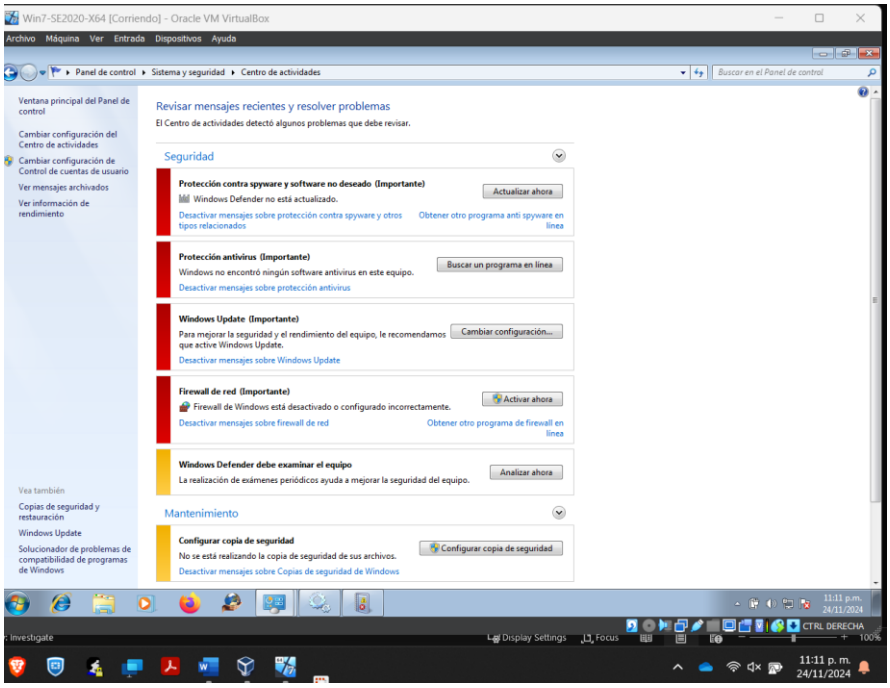
Imagen 9. Validación del sistema operativo



Elaboración propia

Se puede ver que el sistema operativo no tiene actualizaciones activas, eso hace que no pueda tener parches de actualización de seguridad, esto podría generar un riesgo de ataque ya que pueden existir vulnerabilidades que no estén corregidas y sea provechoso el estado vulnerable del sistema operativo para acceso fácil d ellos atacantes.

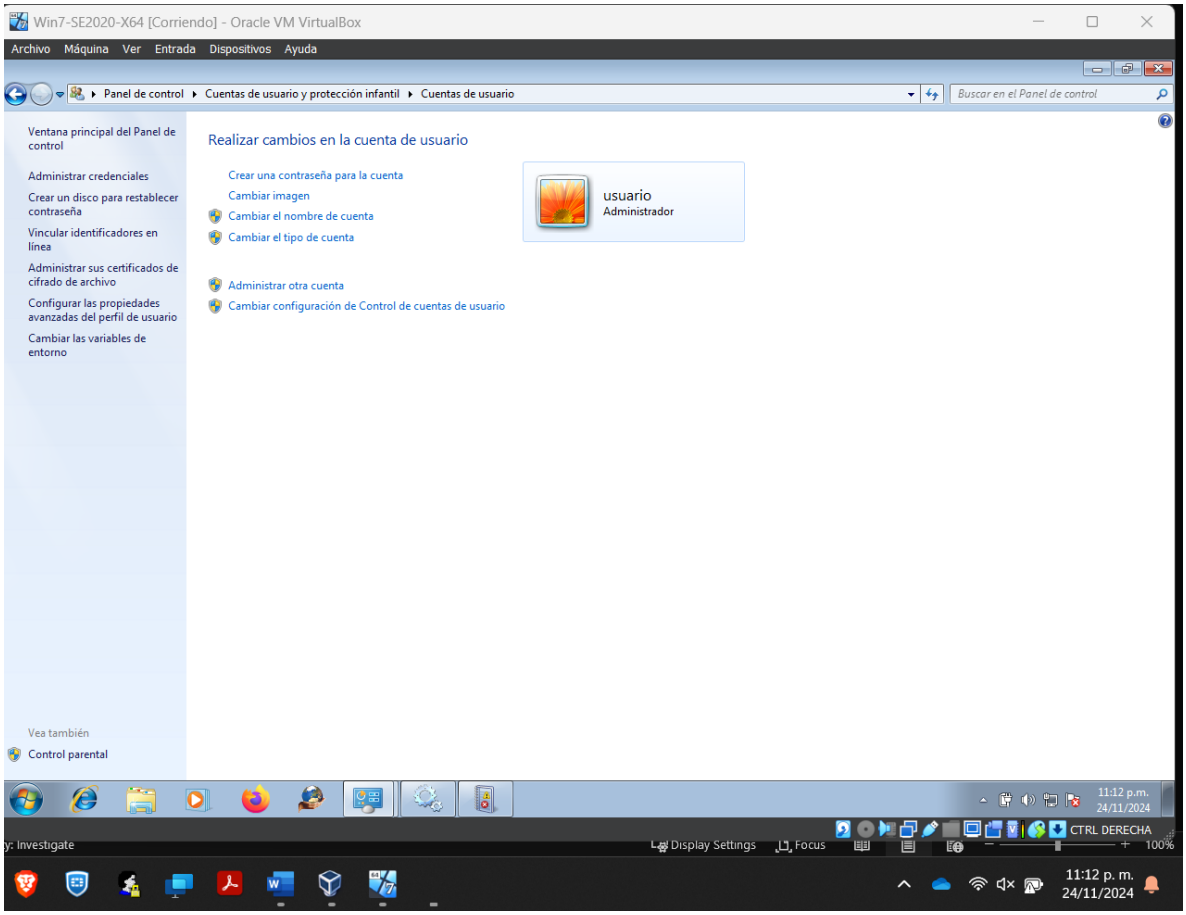
Imagen 10. Validación seguridad del Win 7



Elaboración propia

Por otro lado, la gestión de la creación de los usuarios permitirá que cada user que este creado tenga ciertos niveles de acceso como restringido, medio y usuario final.

Imagen 11. Creación de usuarios



Elaboración propia

Para tener mas encuneta podemos considerar estos aspectos para el hardening:

Tener el Firewall del Sistema operativo habilitado y funcionando que permita controlar los servicios y puertos que no son utilizados por los usuarios y los cuales funcionen como backdoors a los atacantes.

Controlar el acceso de forma remota a los equipos de los usuarios a menos que estos lo requieran para el cumplimiento de sus funciones, tener abiertos protocolos como SSH y TELNET facilitan el acceso de externos

Fortalecimiento de las políticas de seguridad y también limitación de reglas desde las configuraciones dadas en el Firewall para la red.

Capacitación a los usuarios finales sobre sus funciones, que formas de trabajo puede hacer y que limitaciones tienen desde sus usuarios.

7. **Realizar diferencias entre equipo BlueTeam y el Equipo de respuesta**

Tabla. Diferencias entre Blue team y CSIRT

Blue TEAM	***Equipo de respuesta a Incidentes informáticos***
El grupo Blue Team se encarga de proteger a la empresa de ciberataques de manera proactiva, no solo teniendo en cuenta los ataques actuales sino evaluando las posibles amenazas	El equipo de respuestas ellos reciben los reportes de incidentes de seguridad, analiza y da una respuesta al incidente.
El grupo Blue Team hace un monitoreo de los recursos informáticas a fin de encontrar patrones y novedades que puedan ser un riesgo de la información.	El equipo de respuesta hace una acción en el momento que se presenta un incidente informático, hacen una investigación de como atacar, recuperar y gestionar la vulnerabilidad detectada.
El grupo Blue Team de tal forma pueden ser recursos tanto internos como externos de las entidades contratados para la detención y corrección de vulnerabilidades.	El equipo de respuesta son básicamente un área de la compañía y gestionan las incidencias que se presenta en los recursos informáticos.

8. **Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "Center For Internet Security", usted lo utilizaría para que fin.**

Sobre el escenario que CIS demuestra, como es una organización a fines que busca que las empresas, gobiernos y personas que tengan acceso a la tecnología e información, hacen que forma de trabajo sea más practica adaptándose a ciertos estándares y buenas practicas que permiten protegerse contra ataques y amenazas digitales en un mundo que se mantiene en evolución y es cambiante, siempre la información y la tecnología va de la mano.

Controles CIS para gestionar tecnologías:

En lo que respecta a las categorías nos podemos encontrar con benchmarks de:

Sistemas operativos. Que cubren las configuraciones de seguridad de los principales sistemas: Windows, Linux, OSX.

Software de servidores. Sirven para implementar configuraciones de seguridad en los softwares de servidores más usados: Microsoft SQL Server, Nginx, MySQL…

Proveedores cloud. Se centran en las configuraciones de seguridad de las nubes más importantes: Amazon Web Services, Microsoft Azure, Google Cloud…

Dispositivos móviles. Focalizados en los sistemas operativos móviles, incluyendo, por supuesto, Android e iOS.

Dispositivos red. Recogen un conjunto de recomendaciones generales y específicas para los dispositivos red y hardware aplicables como Cisco, F5 o Palo Alto Networks.

Software de escritorio. Se ocupan de la configuración de seguridad de los programas de escritorio más usados como Microsoft Office, Google Chrome o Safari Browser.

De acuerdo a ello, si lo usaría por lo que es una herramienta muy efectiva para estructurar un esquema de seguridad de la información y con esto se podría conocer la política de seguridad de la información y así mismo tener una idea de acción afectiva y forma confiable que le permita la misma protección de cualquier amenazas y así mismo indagar nuevas amenazas a futuro,

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

Un **SIEM** es la unión de dos tecnologías como son el SIM (Security Information Management), y el SEM (Security Event Management). El SIM se encarga de administrar todo lo relacionado con la seguridad de la información y el SEM se encarga de la administración de los eventos de seguridad.

Un **SIEM** se basa en buscar dentro de todos los eventos y las tareas que se presentan en el día a día en los dispositivos de red de una empresa y de una manera eficaz y rápida contrarrestar dichos eventos inusuales para prevenir que se conviertan en una amenaza a la información.

Las principales ventajas que ofrece un SIEM son las siguientes:

- Proactividad en la resolución de incidentes de seguridad
- Rapidez en la detección de eventos e incidentes detectados
- Detección de amenazas no conocidas a través de la analítica avanzada de eventos Mayor rapidez al momento del análisis de las alertas generadas
- Detectar amenazas a través de logs históricos usando la analítica del dispositivo SIEM
- Garantiza la protección de la información y mejora las operaciones de la empresa
- Evalúa todos los activos de red mediante escaneo activo, monitoreo pasivo e inventarios de hardware y software

Las principales funciones principales que ofrece un SIEM son las siguientes:

- **Agregación de datos**: este componente permite agregar los eventos de seguridad que se utilizara en los demás componentes, los cuales vienen de muchas fuentes y se debe a estos categorizar con el fin de estimar si estos deben ser indexados o no según su importancia
- **Alertas**: Se configuran con el fin de buscar alguna actividad sospechosa y que esta genere un aviso cuando se cumplen ciertas condiciones y avisar por distintos medios sobre alguna eventualidad
- **Compliance**: Sirve para automatizar la correlación de eventos que permiten la generación de informes necesarios para temas de auditoría y control de los sistemas de información
- **Incident Response**: Son las acciones que se deben tomar al momento de presentarse un incidente, proporcionando la gestión de los incidentes, así como la colaboración y cambio de conocimiento sobre los mismos haciendo que este proceso sea más eficaz y al mismo tiempo ágil
- **Automatización SOC:** Denominado como SOAR (Security Orchestration, Automation and Response), es la parte que se integra con otros appliance de seguridad por medio de APIs y así crear playbooks y workflows de manera automática ante determinados eventos

10. Defina por lo menos 3 herramientas de contención de ataques informáticos "hardware y software" recuerde que las herramientas de contención son diferentes a las herramientas de detención

Firewall UTM

Como bien se define, es un recurso adaptable que amplifica refuerzos como estrategia de protección de datos, es un dispositivo de hardware y software que integra diversas funciones de seguridad como filtros de paquetes, proxy, sistema de detención y prevención de intrusos, protección de malware y control de aplicaciones.
Ofrece una gama amplia de características, le permite hacer más dinámico y seguro.

Para la red, tiene cuatro funciones clase que pueden ser:

Control web: transforma la gestión de la seguridad en la red, haciéndola más flexible y adaptable a las necesidades empresariales específicas. A diferencia del enfoque tradicional proporcionado por proxies web, que requieren que el administrador maneje perfiles de acceso con bases propias de URL permitidas o restringidas, este método basado en categorías ofrece un conocimiento más profundo y matizado de los sitios web, clasificándolos según su contenido.

Protección contra malware: la estrategia de protección contra malware en un firewall UTM se basa en un enfoque multicapa que puede integrarse con soluciones antivirus externas, lo cual es vital para las empresas que gestionan grandes cantidades de datos sensibles[4]. Las soluciones UTM comúnmente incluyen un antivirus integrado, ya sea desarrollado internamente o provisto por terceros, y suelen contar con una base de datos actualizada de firmas y direcciones asociadas con contenido malicioso.

Control de aplicación: Este método ofrece una gestión de acceso más efectiva a aplicaciones clave para la empresa, una ventaja especialmente significativa en ambientes donde proliferan los servicios en la nube y aplicaciones corporativas. También conocido como filtro de capa 7, el control de aplicación representa un avance importante en la seguridad de la información contemporánea, dada la disminución de la eficacia de las políticas basadas únicamente en puertos, protocolos y direcciones IP.

Prevención de intrusión: es una característica central de los firewalls UTM y opera mediante sistemas que identifican y bloquean ataques potenciales en la red. Estos sistemas emplean algoritmos de reconocimiento de patrones para identificar paquetes de datos que sugieren actividad maliciosa, permitiendo tomar medidas preventivas, como el bloqueo de dicho tráfico.

DMZ:
Es basicamente una zona desmilitarizada y es una red perimetral que protege la red del área local LAN interna contra el trafico no confiable.

es una subred que se encuentra entre la Internet pública y las redes privadas. Expone los servicios externos a redes no confiables y agrega una capa adicional de seguridad para proteger los datos confidenciales almacenados en redes internas, utilizando firewalls para filtrar el tráfico.

[4] Firewall UTM y como puede reforzar la seguridad, pagina NETDATA. LInk https://blog.netdatanetworks.com/utm-firewall

El objetivo final de una DMZ es permitir que una organización acceda a redes no confiables, como Internet, a la vez que garantiza que su red privada o LAN permanecen seguras. En la DMZ, las organizaciones normalmente almacenan servicios y recursos externos así como servidores para el sistema de nombres de dominio (Domain Name System, DNS), el protocolo de transferencia de archivos (File Transfer Protocol, FTP), correo, proxy, protocolo de voz sobre Internet (Voice over Internet Protocol, VoIP) y servidores web.

Los beneficios de usar DMZ proporcionar una red interna con una capa de seguridad adicional al restringir el acceso a los servidores y datos confidenciales. Una DMZ permite que los visitantes del sitio web obtengan ciertos servicios mientras proporcionan un búfer entre ellos y la red privada de la organización. Ofrece tales como:

Habilitación del control de acceso: las empresas pueden proporcionar a los usuarios acceso a servicios fuera de los perímetros de su red a través de Internet pública[5].
Prevención del reconocimiento: al proporcionar un búfer entre Internet y una red privada, una DMZ evita que los atacantes realicen el trabajo de reconocimiento que hacen cuando obtienen datos de objetivos potenciales
Bloqueo suplantación del protocolo IP: Los atacantes pueden intentar obtener acceso a los sistemas suplantando una dirección IP y haciéndose pasar por un dispositivo aprobado que ha iniciado sesión en una red.

Herramienta AIDE.

Es la herramienta que nos a escanear sistemas de archivos con el propósito de buscar cambios no autorizados y va generando alertas si detecta modificaciones sospechosas. Es importante si se procura la detección de intrusiones basada en el sistema de archivos.
La manera en que puede realizar esa detección de cambios es que AIDE crea una base de datos de archivos en la ejecución inicial y luego se comprueba con dicha base de datos en las siguientes ejecuciones.

Debemos tener en cuenta en esta herramienta es que la base de datos que crea inicialmente se almacena en el sistema de archivos raíz, y un atacante podría modificarla fácilmente para buscar ocultar su intrusión al sistema, es por esto por lo que se recomienda realizar una copia de la base de datos y realizar comprobaciones contra dicha copia periódicamente.

[5] Sobre DMZ. Pagina Fortinet. Link https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz#:~:text=Una%20zona%20desmilitarizada%20(demilitarized%20zone,p%C3%BAblica%20y%20las%20redes%20privadas.

6.5 APORTES DENTRO DE UNA ORGANIZACION

- La recolección de información que ayudan en establecer parámetros esenciales para s la arquitectura de una forma precisa asociando información para los expertos de seguridad, no obstante, el equipo blue teams después de que recolecte la información y la decodifique, analizar a los datos recopilados para el estudio que se necesite.

- El análisis consistió en definir cada una de las buenas y malas prácticas en el parcheo de aplicaciones, focalizándose en sus componentes tecnológicos que permitan las conexiones de los equipos terminales con los servidores y a su vez la trasmisión en tiempo real de la información,

- Brindar capacitación al personal de seguridad y de IT para dar acompañamiento a los usuarios finales sobre la utilidad de los dispositivos y accesos a la red, brindado campañas de conciencia.

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

- Las deficiencias dejaron a que las aplicaciones expuestas a ataques y vulnerabilidades, hace que sea más difícil la confidencialidad, la integridad y la disponibilidad de la data.

- Los parches en las aplicaciones, en el sistema operativo, hace que la falta de priorización, también la falta de pruebas exhaustivas, la identificación y la priorización de las vulnerabilidades, son de alto criterios estas áreas que requieren atención inmediata y constante.

- Para fortalecer los procesos que ayuden a la reducción de riesgos, se hace de los instrumentos de recolección para que los parámetros esenciales de una forma adecuada y según las necesidades, los expertos de seguridad recopilan la información harán análisis según las estrategias del equipo blue team.

- Se analizó la imperiosa necesidad de fortalecer el componente tecnológico en de los equipos de Blue Team, incluyendo servicios de almacenamiento en nube, infraestructura de fibra óptica y banda ancha, entre otras que permitan asegurar los procesos y procedimientos que se adelantan

- El brindarles conocimiento a los usuarios es importante, explicar sobre nuevas herramientas técnicas de ataque y contención, ayudar a que las actualizaciones fortalece a la capacidad de respuesta de forma sincronizado.

6.7 CONCLUSIONES QUE PERMITAN LA CONTRUCCION DEL CONOCIMIENTO DESDE EL ENFOQUE DE SEGURIDAD

- Documentar los hallazgos de las simulaciones permite que la base de conocimiento sirve como referencia para futuras estrategias.

- Según los procesos de regula miento para el cumplimiento normativo, alinear las estrategias de ciberseguridad son marcos legales que aparte de proteger a las empresas de sanciones, también fomenta la confianza de los clientas y personas interesadas.

- Sencillamente las organizaciones deben empaparse de los marcos legales, y eso hace que las estrategias deben ser revisadas constantemente en caso de un ajuste sea a medidas a las nuevas amenazas, esto podría asegurar que en pro las organizaciones estarán avanzando que los mismos atacantes.

- La gestión de los equipos debe ser realizada periódicamente analizando la eficiencia de las practicas medidas o políticas que se adoptan en una organización, con el propósito de mitigar la recurrente exposición al riesgo, de manera que se esté revisando, identificando y actualizando todos los softwares de uso de la entidad.

7. **CONCLUSIONES**

- Llevar a cabos esta implementación de este software optimiza las brechas de seguridad de los sistemas informáticos para el negocio o dependiendo del escenario, lo que mejora el rendimiento de las aplicaciones y la experiencia del usuario final.

- La información y los sistemas son recursos valiosos para las organizaciones, por tal motivo es necesario, incorporar métodos y herramientas en el análisis forense. Por otro lado, los métodos se encuentran conformados por fases para la identificación, preservación, análisis y presentación de una evidencia digital.

- La administración segura que ofrece tiene un enfoque novedoso para la provisión para la combinación de la arquitectura de seguridad.

- La virtualización del sistema operativo permite que se pueda ejecutar varias imágenes en simultáneamente, esto ayudara a comprender el escenario de la máquina para hacking a la maquina afectada en un ambiente más real.

- Al abordar estas deficiencias, el equipo de Blue Team se logró encontrar estrategias que puedan fortalecer su capacidad de respuesta, reducir los riesgos y asegurar una protección más efectiva de los sistemas.

- Tanto para los equipos Red Team y Blue Team pueden emular este tipo de ataques, practicar y aplicar el tiempo determinado para enfrentar estos ataques de la manera más eficaz con el propósito de cambiar aspectos y medir la efectividad para futuras amenazas.

- El uso de los procesos y herramientas para rastrear y controlar el uso, la asignación y configuración de privilegios administra trucos en los equipos, redes y aplicaciones.

VIDEO DE SUSTENTACION

Link [Video sustentacion AC 1019136850]
[Video sustentacion AC 1019136850 - OneDrive]

VALIDACION PLAGIO POR TURNITIN

Nota: se intentó reducir párrafos y títulos entre mas cosas.

BIBLIOGRAFÍA

- Rogelio Toledo (año 2019). Pasos esenciales para realizar un análisis de riesgo de ciberseguridad. Sitio web Grupocibernos.com. Link https://www.grupocibernos.com/blog/pasos-esenciales-para-realizar-un-analisis-de-riesgo-de-ciberseguridad

- Gobierno. Septiembre (2024). Ley 1273 de 2009 Congreso de la república de Colombia. Secretaria SENADO.gov.co. Link http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- Abril 2024. Ventajas WAN vulnerabilidades. Vulnerability Manager Plus https://www.manageengine.com/vulnerability-management/help/wan-architecture.html

- David A. Franco (2012). Metodología para la detención de vulnerabilidades en redes de datos. información Tecnológica. Sitio web https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

- Gobierno. Septiembre (2024). Ley 1273 de 2009 Congreso de la república de Colombia. Secretaria SENADO.gov.co. Link http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- David A. Franco (2012). Metodología para la detención de vulnerabilidades en redes de datos. información Tecnológica. Sitio web https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

- Mayo 2019. Normatividad sobre delitos informáticos. Policía Nacional de Colombia. Link https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos
- January 2024. Code of Ethics for the practice of engineering in general and its related and auxiliary professionals. Web site Copnia Government of Colombia. Link https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

- - Pirani (2022). Types of Cybersecurity audits. Link https://www.piranirisk.com/es/academia/especiales/auditoria-de-ciberseguridad-companies

- David A. Franco (2012). Methodology for the detention of vulnerabilities in data networks. information Technology. Sitio web https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014
-
- Hacknoid (2023). Computer security tools. Link https://www.hacknoid.com/hacknoid/5-herramientas-de-seguridad-informatica-claves-en-empresas/

- Hacking Community (2024). Technique Pass-The-Hash Dumpling of hashes. Youtube website. Link https://www.youtube.com/watch?v=UW_irHPhpFU

- Jennifer Carreño (2020). Firewall UTM y cómo puede reforzar la seguridad, Sitio web NETDATA. LInk https://blog.netdatanetworks.com/utm-firewall

- Anonimo. (2021). Sobre DMZ. Pagina Fortinet. Link https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz#:~:text=Una%20zona%20desmilitarizada%20(demilitarized%20zone,p%C3%BAblica%20y%20las%20redes%20privadas.

- Esteban Samuel (2021). Metasploit atacando a windows. Sitio web Blacktrack Academy. Link https://backtrackacademy.com/articulo/metasploit-atacando-awindows

- Snort - network intrusion detection & prevention system. (s/f). Snort.org. Recuperado el 15 de febrero de 2024, de http://www.snort.org/

- Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, 3-26. Recuperado de https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica