Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Durley Rubiela Rojas Soler

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2024

Resumen

Se presenta un informe técnico donde se contiene las estrategias Red Team & Blue Team lo cual permiten hacer frente a un incidente o evento informático en una infraestructura TI, teniendo presente el cumplimiento de normas éticas y legales con el fin de mejorar el esquema de ciberseguridad de una organización.

De igual manera da a conocer las vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión utilizando herramientas de penetración pentesting y formulando estrategias de contención mediante el análisis de vulnerabilidades y riesgos en una infraestructura TI.

Palabras clave: Incidente, ciberseguridad, Red Team, Blue Team, legales

Abstract

A technical report is presented containing the Red Team & Blue Team strategies which allow us to deal with a computer incident or event in an IT infrastructure, taking into account compliance with ethical and legal standards in order to improve the cybersecurity scheme of an organization.

Likewise, it reveals the vulnerabilities in a computer system through the use of intrusion methodologies and techniques using pentesting penetration tools and formulating containment strategies through the analysis of vulnerabilities and risks in an IT infrastructure.

Keywords: Incident, cybersecurity, Red Team, Blue Team, legal

Contenido

Glosario

Activo

Elemento percibido como valioso para una organización.

Amenaza

Cualquier circunstancia o evento que pueda afectar los activos de manera negativa.

Amenaza externa

Cualquier riesgo a la seguridad producido fuera de la organización que tenga el potencial de dañar sus activos.

Amenaza interna

Riesgo a la seguridad producido por una persona que pertenece o perteneció a una empresa o tiene una relación directa o de confianza con ella.

Auditoría de seguridad

Revisión de los controles, políticas y procedimientos de seguridad de una organización.

Autenticación

Proceso de verificar la identidad de una persona.

Autorización

Proceso de determinar si un/a usuario/a autentificado/a tiene acceso a recursos específicos en un sistema.

Autorizar

Sexto paso del RMF del NIST que se refiere a asumir la responsabilidad de los riesgos de seguridad y privacidad que puedan existir en una organización.

Confidencialidad

Propiedad según la cual únicamente las personas autorizadas pueden acceder a activos o datos específicos.

Controles de seguridad

Medidas de prevención diseñadas para reducir riesgos de ciberseguridad específicos.

Detectar

Función central del NIST relacionada con la identificación de posibles incidentes de seguridad y la mejora de las capacidades de monitoreo y respuesta.

Disponibilidad

Propiedad según la cual todas las personas autorizadas pueden acceder a activos o datos específicos.

Evaluar

Quinto paso del Marco de Gestión de Riesgos (RMF) del NIST, para determinar si los controles establecidos se han implementado correctamente

Gestión de eventos e información de seguridad (SIEM por sus siglas en inglés)

Solución de seguridad que recopila y analiza los datos de registro para monitorear actividades críticas en una organización.

Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST)

Marco de adhesión voluntaria creado en los Estados Unidos, que incluye estándares, pautas y prácticas recomendadas para gestionar los riesgos de ciberseguridad.

Marcos de seguridad

Pautas utilizadas para crear planes que ayuden a mitigar el riesgo y las amenazas a los datos y la privacidad Integridad: Cualidad que identifica los datos como correctos, auténticos y confiables.

Red Team

Es un equipo dedicado a simular ciberataques como parte de una acción controlada de ciberseguridad, con el fin de identificar brechas de seguridad y evaluar la efectividad de las medidas de seguridad existentes, así como la respuesta por parte del equipo de defensa, para la protección de los activos.

Blue Team

Es un equipo dedicado a la defensa de los sistemas de una organización contra potenciales ciberataques.

Vector de ataque

Método que se utiliza para penetrar las defensas de seguridad de un sistema informático.

Vulnerabilidad

Debilidad que puede ser aprovechada por una amenaza

Lista de Tablas

Lista de Figuras

Introducción

El siguiente trabajo está enfocado en evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales, Demostración de vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión. y en la contención de ataques informáticos mediante estrategias que permitan la mitigación de ataques informáticos el cual se está presentando en la organización CyberFort Technologies, la cual se encuentra alojada el sistema operativo de Windows 7, en uno de los equipos de cómputo, por lo que se procede a validar las falencias de seguridad informática para proceder a utilizar herramientas que permita mitigar el ataque informático, robustecer la seguridad de la información de la organización y establecer políticas de seguridad y privacidad de la información, datos personales y de los activos.

Objetivos

Objetivo General

Conocer las metodologías, herramientas y marco legal que rige dentro de los equipos Red Team & Blue Team, con el fin de proteger los activos de la organización CyberFort Technologies.

Objetivos Específicos

Identificar la normatividad relacionada a los delitos informáticos y la protección de datos personales

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

Establecer acuerdos de confidencialidad, integridad, como fortalecimiento a los procesos y procedimientos de ciberseguridad.

Ejecutar las pruebas de penetración pentesting, para identificar las vulnerabilidades que están afectando la seguridad de la información de la organización

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

Evaluar las estrategias y recomendaciones en la mitigación de vulnerabilidades.

Desarrollo del Informe

Aspectos que Aporten al Desarrollo de Estrategias de Red Team & Blue Team

A continuación se da a conocer los Conceptos Equipos de Seguridad de acuerdo con el marco legal colombiano el cual aporta al desarrollo de estrategias de Red Team y Blue Team con respecto a los delitos informáticos y protección de datos personales:

Decreto 1360 de 1989 "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor". (1989) Resuelve las reclamaciones por violación a los derechos del autor como generadores de software y dar respuesta oportuna a soluciones informáticas, mejorando la calidad de vida de las personas que son las creadoras, generando credibilidad e importancia en el buen desarrollo de nuevas aplicaciones como herramientas que facilitan la interacción de la información.

Ley 599 de 2000 "Por la cual se expide el Código Penal." Art.195 Acceso abusivo a un sistema informático. (2000, 2000) Cuando ingresa a un sistema de información sin autorización ocasionando daños irreparables a la información logrando vulnerar los datos sin importar las consecuencias que se puedan presentar.

Ley 679 de 2001 Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. (2001, 2001) Se establece la prohibición de información con respecto a menores de edad porque atenta contra la integridad del menor y esto puede crear múltiples consecuencias y afectaciones irreparables, esta ley permite establece la penalización a los delincuentes que continúen realizando estos delitos contra los menores de edad.

Ley 842 de 2003 “Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética

Profesional y se dictan otras disposiciones" (2003, 2003). Establece los deberes, derechos, prohibiciones, inhabilidades e incompatibilidades a los ingenieros en general, afines o auxiliares ejercen su profesión con honestidad, respeto, compromiso y lealtad, de lo contrario están expuestos a perder definitiva la tarjeta profesional, que inhabilita continuar laborando, de igual manera se realiza la penalización por la falta que haya realizado en su momento.

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. (Policía, 2009) Establece todos los delitos informáticos como: Acceso abusivo a un sistema informático, Obstaculización ilegítima de sistema informático o red de telecomunicación, Interceptación de datos informáticos., Daño Informático., Uso de software malicioso., Violación de datos personales., Suplantación de sitios web para capturar datos personales, Circunstancias de agravación punitiva, Hurto por medios informáticos y semejantes, Transferencia no consentida de activos, los cuales son adquiridos por el mal uso de la información, por descuido, desinformación o porque son muy confiados al entregar información sin medir las consecuencias, cuando acceden sin autorización a los equipos informáticos, cuando suplantan una página web o el usuario de una persona en el robo de información confidencial o porque no utilizan herramientas que permitan la protección y seguridad de la información contra estos delitos informáticos los cuales afectan la confidencialidad, integridad y disponibilidad de los datos y la parte financiera. Esta ley también establece la penalización de acuerdo con cada uno de los delitos anteriormente descritos, los cuales en su mayoría están entre 48 y 96 meses y su multa es de 100 a 1000 SMLMV

La siguiente tabla contiene las características de los artículos de la Ley 1273 de 2009 (Contabilidad, 2010)

Tabla 1

Relación de los Artículos de la Ley 1273 De 2009

Artículos	Descripción	Condena
269A Acceso abusivo a un sistema informático"	Se comete cuando aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos	Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.	Se cometen cuando bloquean en forma ilegal un sistema o impiden su ingreso, a cuentas de correo electrónico de otras personas, sin su autorización	Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes., siempre que la conducta no constituya delito sancionado con una pena mayor.
269C: Interceptación de datos informáticos.	Se comete cuando obstruyen datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático	prisión 36 a (72) meses
Artículo 269D: Daño Informático.	Se produce cuando una persona que sin estar autorizado modifica, altera, daña, elimina, destruye o suprime datos del programa o documentos electrónicos y se hacen en los recursos de TIC	Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
269E: Uso de software malicioso.	Se produce cuando se adquieren distribuyen, envían, introducen o extraen del país software o programas de computador que produce daños en los recursos TIC	Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículos	Descripción	Condena
269F: Violación de datos personales	Se produce cuando sin estar facultado sustrae, envía, vende, divulga, compra o emplea datos personales almacenados en medios magnéticos	Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
269G: Suplantación de sitios web para capturar datos personales.	Se produce cuando una página web es similar a la de una entidad y envía correos electrónicos (spam) como ofertas de empleo y personas inocentes suministran información personal y claves bancarias y el delincuente informático ordena transferencias de dinero a terceros.	Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes., siempre que la conducta no constituya delito sancionado con pena más grave.
269H: Circunstancias de agravación punitiva:	1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de	Las penas se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

Artículos	Descripción	Condena
	inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.	
Hurto por medios informáticos y semejantes.	Se comete cuando manipulan un sistema de información, una red de sistemas electrónicos, telemáticos u otro medio semejante o suplantación a un usuario ante sistemas de autenticación y de autorización establecidos	Las penas señaladas en el artículo 240 de este Código. De 3 a 8 años
269J: Transferencia no consentida de activos.	Se comete cuando utilizando algún truco o manipulación informática efectúa la transferencia no autorizada de cualquier activo en perjuicio de un tercero en provecho propio. Este delito también se denomina estafa electrónica, igual manera se presenta cuando fabrica, introduce o facilita programas de computador para cometer los anteriores delitos	Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Fuente. Autoría propia

Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales." (Colombia, 2012)**.** Establece el tratamiento de los datos personales y las garantías constitucionales con respecto a la protección, la disponibilidad, la confidencialidad, la integridad y la seguridad de la información de las personas, que no permitan la alteración, fraude, perdida si su respectiva autorización.

Análisis Sobre el Ejercicio de Pentesting

Para identificar las vulnerabilidades de seguridad en las aplicaciones, redes y sistemas de información se utilizan las pruebas de penetración como herramienta de seguridad para identificar las debilidades que se puedan presentar en el flagelo o robo de información. Para evaluar la seguridad se requieren de las 5 fases de las proceso que realiza el pentesting iniciando

con el Reconocimiento el cual es la recopilación de la información como por ejemplo: Fuentes de información, Direcciones IP de servicios tercerizados, Existencia de redes inalámbricas, Dirección física de la empresa, Rangos de direcciones IP asignados, entre otras, con el fin delimitar las áreas a evaluar y poder generar estrategias de ataque que sean eficientes al mitigar la vulnerabilidad que se presente, para esta fase se utiliza la herramienta Nmap, que realiza el escaneo detallado del sistema utilizando los comandos[-sV] intenta determinar la versión del servicio en el objetivo, [-O] informa el sistema operativo en el objetivo, entre otros, segunda fase es el Escaneo el cual permite realizar a fondo la evaluación de todos los elementos que están involucrados desde su inicio hasta su final verificando el estado dinámico y estático del sistema, para esta fase se utiliza la herramienta Nmap, la cual permite realizar un escaneo de la red para identificar los dispositivos activos utilizando el comando [-iL] indica el listado de redes o equipos a escanear > nmap –iL hosts.txt, , [-p] lista los puertos que se desean escanear, la tercera fase es la Evaluación de vulnerabilidades se realiza la identificación sobre las posibles debilidades a las vulnerabilidades encontradas que pueden ser detonadas por un atacante informático, para esta fase se utiliza la herramienta Nmap, la cuarta fase es la Explotación se realiza cuando el evaluador ha identificado las vulnerabilidades a explotar predominando las siguientes tareas como son: la detección de barreras de protección, detección de módems activos, detección de servicios activos, detección de equipos activos, entre otros, para esta fase se utiliza como herramienta Metasploit,la, cual identifica y evalúa las vulnerabilidades de los sistemas objetivo para ejecutar los exploits de las vulnerabilidades. y la quinta etapa es el Informe el cual entrega detalladamente los hallazgos encontrados de las vulnerabilidades que se explotaron con el fin de mitigar los riesgos de seguridad, tener en cuenta las recomendaciones para robustecer la seguridad.

Explicación de las Herramientas y Servicios Utilizados en Ciberseguridad

Metasploit. Es una herramienta basada en el lenguaje Ruby que brinda una estructura completa para el desarrollo, la aprobación y la ejecución de exploits contra objetivos remotos, esta herramienta es muy valiosa ya que permite ser utilizada por los piratas informáticos éticos y los ciberdelincuentes en la investigación de vulnerabilidades sistemáticas en servidores y redes. Debido a su software de código abierto es fácil de usar en diferentes sistemas operativos su primera su historia inicia en el año 2003, El Proyecto Metasploit fue adquirido por Rapid7 en 2009, El cual ha desarrollado una edición comercial de Metasploit – Metasploit Pro. Que permite a los usuarios la automatización total de las pruebas de penetración, junto con otras funciones avanzadas, que incluyen: (CIBERSEGURIDAD, s.f.)

- Explotación manual
- Evasión de antivirus e IPS / IDS
- Pivote de proxy
- Módulos posteriores a la exploración
- Limpieza de sesión
- Reutilización de credenciales
- Ingeniería social
- Generador de carga útil
- VPN pivotante
- Validación de vulnerabilidades
- Pruebas de aplicaciones web.

Su funcionamiento de basa en diferentes interfaces por ejemplo de gráficos, consola y líneas de comandos: (CIBERSEGURIDAD, s.f.)

- MSFConsole (Metasploit Framework Console): Permite a los usuarios acceder a Metasploit Framework a través de una interfaz de línea de comandos interactiva.
- MSFWeb: una interfaz basada en navegador que permite a los usuarios acceder al marco de Metasploit.
- Armitage: desarrollado por Raphael Mudge en 2013, A, es una interfaz gráfica de usuario basada en Java que permite a los equipos de seguridad colaborar compartiendo su acceso a hosts comprometidos.
- RPC (llamada a procedimiento remoto): permite a los usuarios manejar mediante programación Metasploit Framework utilizando servicios de llamada a procedimiento remoto (RPC) basados en HTTP. Además del Ruby nativo de Metasploit, los servicios RPC pueden operar a través de otros lenguajes, como Java, Python y C.

Hay tres bibliotecas de Metasploit, las cuales permiten a los usuarios ejecutar exploits sin escribir código adicional.: (CIBERSEGURIDAD, s.f.)

- REX: habilita las tareas más básicas; contiene Base64, HTTP, SMB, SSL y Unicode.
- MSF Core: proporciona una API común y define Metasploit Framework.
- Base de MSF: proporciona una API fácil de usar.

La siguiente tabla contiene los comandos que se utilizan en consola de metasploit: (Lazaro, 2020)**:**

Tabla 2

Listado de Comandos de Metasploit

Comando	Descripción
show exploits	Mostrar todos los exploits del Framework.
show payloads	Mostrar todos los payloads del Framework.
show auxiliary	Mostrar todos los módulos auxiliares del Framework.
search [cadena]	Búsqueda por cadena
search type:[exploit, payload, auxiliary, encoder, post] [cadena]	Búsqueda por tipo y cadena
info	Muestra información acerca de un exploit cargado.
use [cadena]	Carga el exploit indicado.
LHOST	Variable local host
RHOST	Variable host remoto
set [parámetro] [valor]	Graba en el parámetro el valor indicado.
setg[parámetro] [valor]	Graba en valor para el parámetro indicado de forma global.
show options	Muestra las opciones de un exploit.
show targets	Muestra las plataformas objetivo del exploit.
set target [número]	Especifica un objetivo concreto de los posibles.
set payload [payload]	Especifica un payload a usar..
show advanced	Muestra las opciones avanzadas.
set autorunscript migrate -f	Migra el proceso a un hilo independiente de forma automática.

Comando	Descripción
check	Comprueba si un objetivo es vulnerable a un exploit.
exploit	Ejecuta un exploit
exploit -j	Ejecuta un exploit en background.
exploit -z	No interactúa con la sesión después de acceder con éxito
exploit -e encoder	Especifica el encoder a usar con el payload
exploit -h	Muestra la ayuda para el exploit especificado
sessions -l	Muestra la lista de sesiones disponibles
sessions -l -v	Muestra la lista de sesiones disponibles en modo verbose
sessions -s [script]	Ejecuta un script específico en todas las sesiones de meterpreter activas.
sessions -K	Mata todas las sesiones activas
sessions -c cmd	Ejecuta un comando en todas las sesiones activas
sessions -u sessionID	Actualiza una shell de Win32 a una consola de meterpreter
db_create [nombre]	Crea una base de datos
db_connect [nombre]	Crea y se conecta a una base de datos
db_nmap	Usa y carga los resultados de Nmap en una base de datos
db_autopwn -h	Muestra la ayuda para usar db_autopwn.
db_autopwn -p -r -e	Ejecuta db_autopwn contra todos los puertos encontrados, usa una shell reversa y los explota.

Comando	Descripción
db_destroy	Elimina la actual base de datos
db_destroy [usuario]:[contraseña]@[host]:[puerto]/[base_de_datos]	Borra una base de concreta

Fuente. Autoría propia

Nmap. es una herramienta de escaneo de redes y código abierto se utiliza mucho en pruebas de penetración y auditorias de seguridad, utiliza una interfaz gráfica llamada Zenmap. Es un programa que es compatible con sistemas operativos Windows, Linux y también macOS,

Utiliza diferentes tipos de estructuras de paquetes a través de protocolos de capa de transporte como:

TCP (Transmission Control Protocol). Es un estándar de comunicaciones que permite la comunicación de programas y dispositivos a través de la red.

UDP (User Datagram Protocol). Envía información de forma rápida al usuario sin esperar a que este compruebe y establezca la conexión.

SCTP (Stream Control Transmission Protocol). Reúne las características de TCP y UDP agregando el manejo de la congestión y la tolerancia a fallos.

ICMP (Internet Control Message Protocol). Permite que las pasarelas y sistemas envíen informes de problemas a la máquina que envía el paquete.

NMAP utiliza una serie de comandos para escanear y monitorizar una red. Por ejemplo, para realizar un escaneo utilizando direcciones IP se tendrá que introducir el siguiente comando:

nmap 192.168.1.56 (para un host) o nmap -F 192.168.1.56 (para un análisis rápido).

nmap 192.168.1.56 192.168.1.57 192.168.1.58 (para varios host).

nmap 192.168.1.56-100 (para un rango de direcciones IP).

nmap 192.168.1.* (para escanear y analizar toda la red).

Para realizar un escaneo utilizando el nombre de host:

nmap serverq.nombredehost.com.

Principales Usos de Nmap (REDES ZONE, s.f.)

Algunos de los usos más comunes para Nmap son:

Escaneo de Puertos. Se puede utilizar para realizar el escaneo de puertos abiertos en la red. Lo cual nos da la posibilidad de identificar posibles puntos en los que un atacante puede atacar nuestra red.

Detección de Sistemas. Se puede utilizar para encontrar sistemas activos en una red. Esto puede incluir servidores y dispositivos de red.

Detección de Servicios. Es posible detectar los servicios que se están ejecutando en la red, lo cual nos ayuda en muchos casos a detectar vulnerabilidades. Podremos identificar servicios como HTTP, Telnet, FTP, SSH, entre otros muchos. Esto lo que permite es proporcionar información muy detallada sobre los softwares que están siendo ejecutados, incluso las versiones de estos.

Mapeo de Redes. Esto puede incluir varios factores como la ubicación de un dispositivo o la topología de la propia red. Así será mucho más sencillo crear un mapa visual de toda la infraestructura, identificando los dispositivos y como están conectados.

Pruebas de Seguridad. Se pueden realizar pruebas de penetración y evaluaciones de seguridad. Esto nos permite identificar vulnerabilidades en los sistemas o la red. Esto está directamente ligado al escaneo de puertos.

Monitorización. Tiene la capacidad de realizar una monitorización de la disponibilidad de los servidores o dispositivos de la red. Lo cual nos ayuda a ver si están funcionando de la forma correcta.

Estado de los Puertos

Hay diferentes opciones que se deben conocer, ya que el estado actual en el momento de realizar el escaneo puede variar. Por lo tanto, se pueden considerar las siguientes alternativas:

Open. una aplicación está activamente aceptando conexiones TCP o UDP. El puerto está abierto y se puede utilizar, los pentesters podrán utilizar este puerto abierto para explotar el sistema. Es el estado por defecto si no tenemos ningún firewall bloqueando accesos.

Closed. un puerto que está cerrado es accesible porque responde a Nmap, sin embargo, no hay ninguna aplicación funcionando en dicho puerto. Es útil para descubrir que un host está levantado, o como parte de la detección de un sistema operativo. De cara al administrador del sistema, es recomendable filtrar estos puertos con el firewall para que no sean accesibles. De cara al pentester, es recomendable dejar estos puertos "cerrados" para analizar más tarde, por si ponen algún servicio nuevo.

Filtered. en este estado Nmap no puede determinar si el puerto está abierto, porque hay un firewall filtrando los paquetes de Nmap en dicho puerto. Estos puertos filtrados son los que aparecerán cuando tengamos un firewall activado. Nmap intentará en varias ocasiones intentar conectar, lo que hace que el escaneo de puertos sea bastante lento.

Open| Filtered. Nmap no sabe si el puerto está abierto o filtrado. Esto ocurre porque el puerto abierto no envía ninguna respuesta, y dicha falta de respuesta podría ser por el firewall. Este estado aparece cuando usamos UDP y IP, y utilizamos escaneos FIN, NULL y Xmas.

Closed \| Filtered. en este estado no se sabe si el puerto está cerrado o filtrado. Solo se usa este estado en el IP Idle Scan.

Tipos de Escaneos

En el momento de monitorizar o llevar a cabo una auditoría de seguridad se pueden dar diferentes tipos de escaneos desde Nmap que son interesantes conocer como:

Fin. este tipo de escaneo te ayudará a saber si el host está tras un firewall.

Sondeo de Lista. esta alternativa tiene como objetivo el de conseguir los nombres de equipo de los diferentes dispositivos que están conectados a una red en concreto, y sin que sea necesario enviar un paquete para conseguir este propósito, ya que lleva a cabo resolución inversa de DNS.

Tcp Connect. este escaneo puede servir para llegar a realizar con éxito una conexión completa de todos los puertos.

Ping-Arp. en este caso, estamos ante una opción más útil con la que se puede saber si el host está activo en la red mediante Ping o incluso para conseguir algún dato más específico sobre los host que están activos con Arp.

Open Vas. Es un software libre, el cual puede detectar más de 100.000 vulnerabilidades en redes de manera interna y externa, de igual manera realizar el escaneo de vulnerabilidades completo, detectando diferentes problemas que pueden ser graves en dispositivos en red o pueden ser de bajo riesgo para el usuario, se desarrollo en el año 2009 por la empresa Greenbone Networks, realiza diversas funciones como:

- Ajustes personalizados de rendimiento para exploraciones a gran escala.
- Pruebas autenticadas.
- Cuenta con protocolos industriales y de Internet de alto y bajo nivel.
- Desarrollado en un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad.
- Pruebas no autenticadas.

Características

Ofrece una explotación de vulnerabilidades y su gestión es una de las tareas más importantes, tiene Licencia Pública General de GNU (GNU GPL). tiene aplicaciones que ofrecen servicios y son útiles. y características que se destacan son:

- Una comunidad que ofrece bastante tutoriales y apoyo a la hora de explotar vulnerabilidades, por su web y por otros foros como Reddit por ejemplo.
- Extensa y definida documentación.
- Posibilidad desde línea de comandos y en modo gráfico con una interfaz con utilidades y repleta de datos de interés, capaz de sacar informes de interés.

Servicios en Línea

ExploitDB. Esta aplicación web recopila bases de datos públicas que contienen herramientas para aprovechar vulnerabilidades conocidas, y los usuarios contribuyen a estas. Los profesionales de pruebas de penetración de todo el mundo pueden descargar, consultar y utilizar estos recursos de forma gratuita para mejorar la calidad de sus auditorías de seguridad.

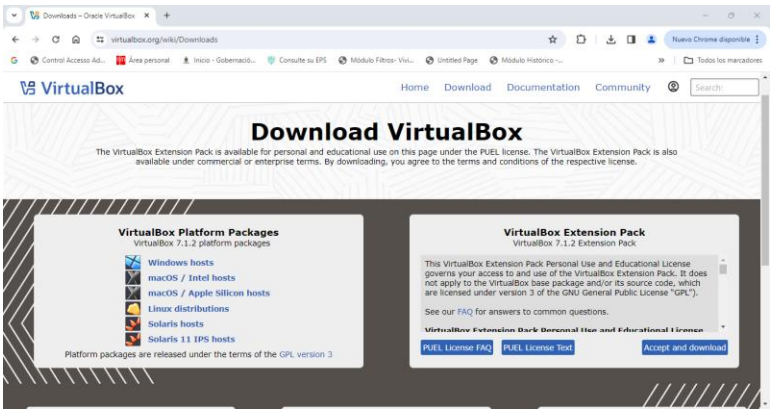
CVE. Las vulnerabilidades son defectos en el software que permiten a los hackers acceder ilegalmente a redes y sistemas, y propagar malware. Esto les permite hacerse pasar por administradores con pleno acceso a los recursos de la empresa. Esto podría permitir que el atacante se mueva sigilosamente por las redes, recopilando datos confidenciales, credenciales de usuario e información del cliente.

Evidencia de la Implementación del "Banco de Trabajo" en su Entorno Local

Paso A. Descargar la herramienta virtualizadora "VirtualBox" en su última versión., se procedió a ingresar al link https://www.virtualbox.org/wiki/Downloads, para realizar la descarga del programa:

Figura 1

Descarga VirtualBox

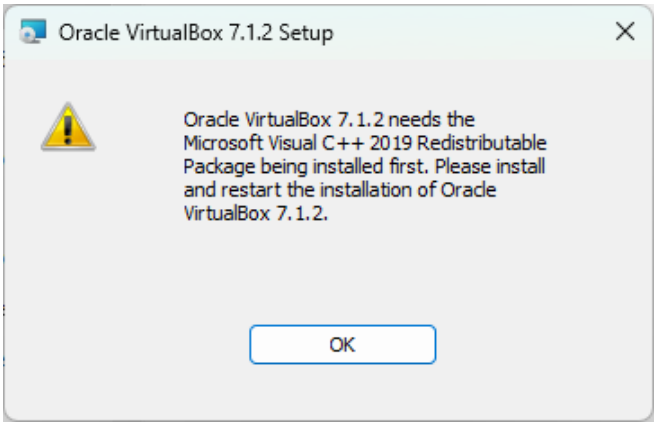


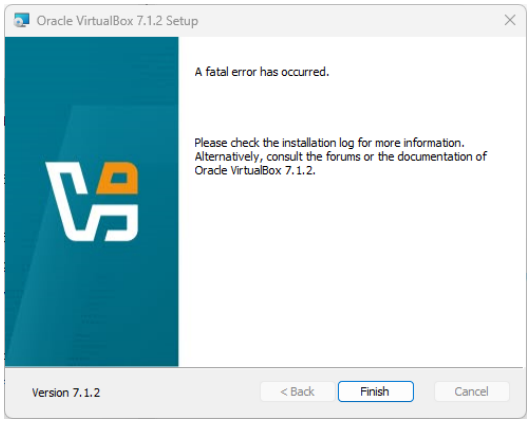
Fuente. Autoría propia

Se realiza la instalación, pero se muestra un error de instalación debido a que mi sistema operativo es Windows 11

Figura 2

Instalación VirtualBox





Fuente. Autoría propia

Se realiza la descarga del archivo vc_redist.64.exe, para proceder a instalar la máquina virtual VirtualBox

Figura 3

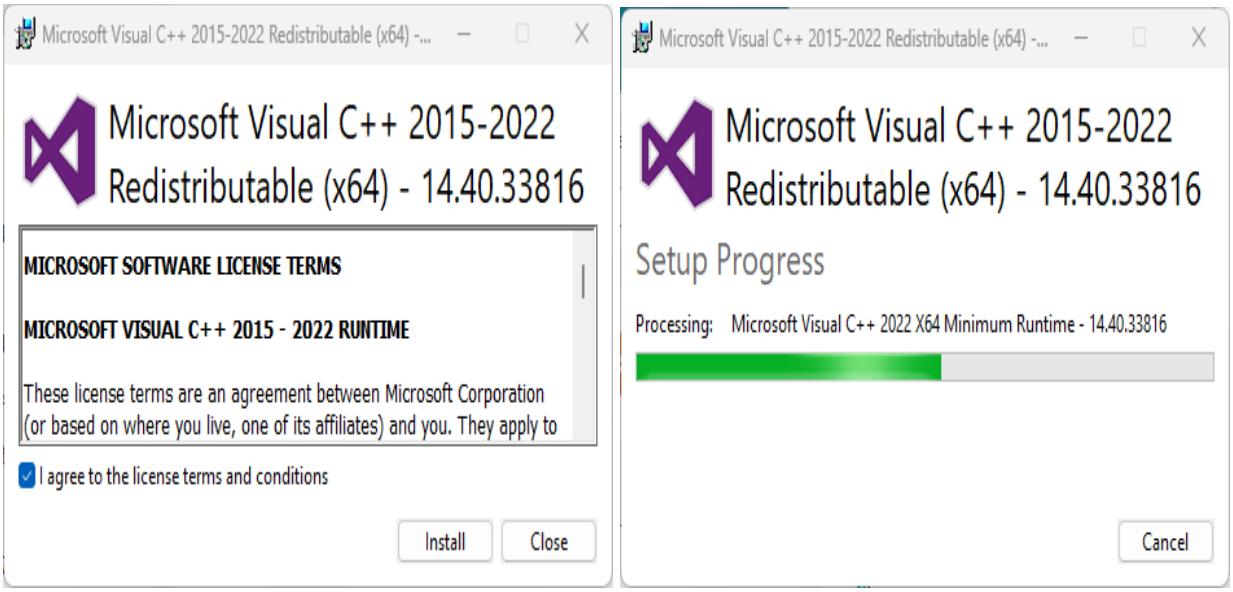
Descarga archivo vc_redist.64.exe

Fuente. Autoría propia

Se procede a ejecutar como administrador el archivo vc_redist.64.exe

Figura 4

Instalación Archivo vc.redist.64.exe

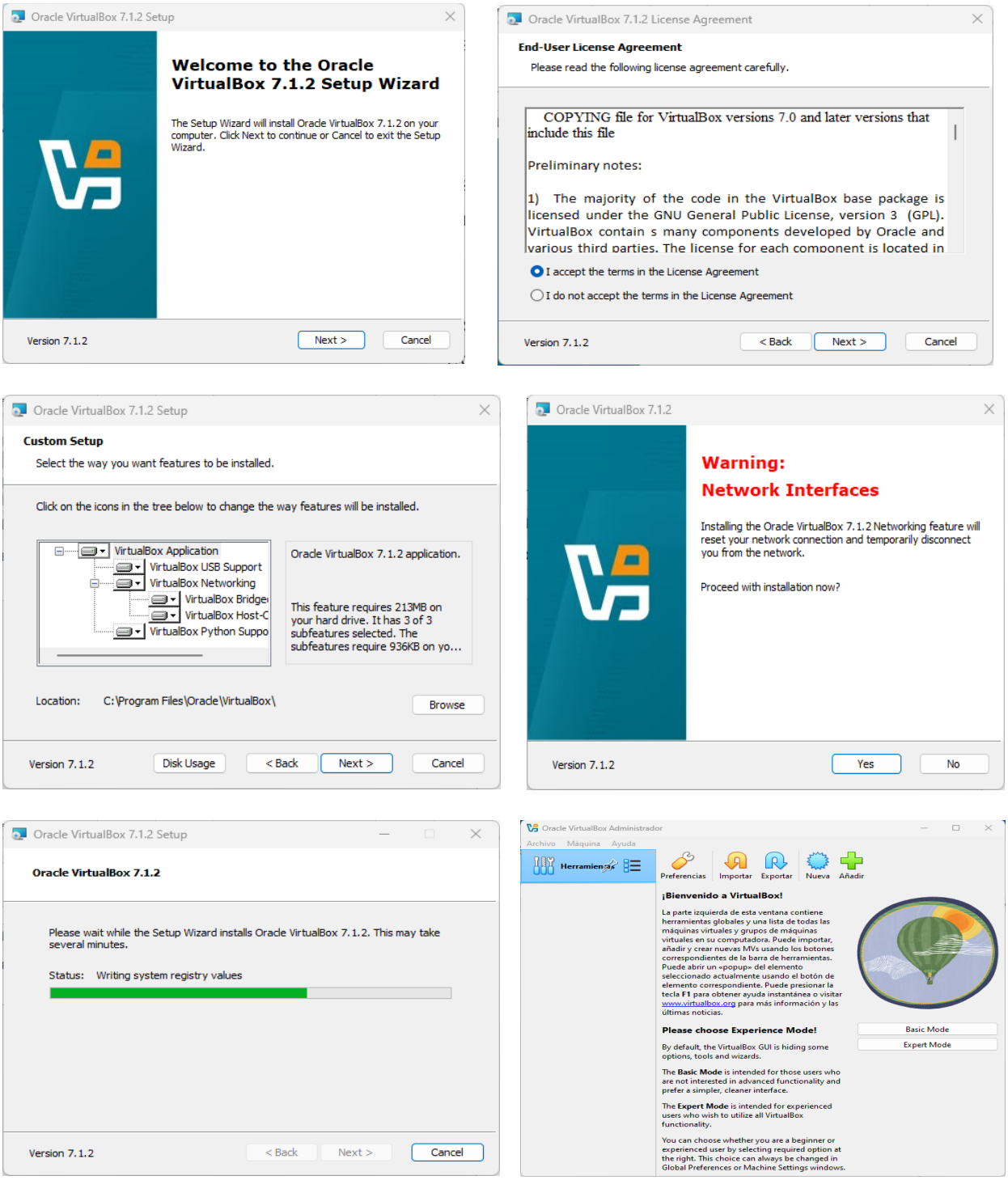


Fuente. Autoría propia

Se instala la máquina virtual VirtualBox

Figura 5

Instalación Máquina Virtual VirtualBox



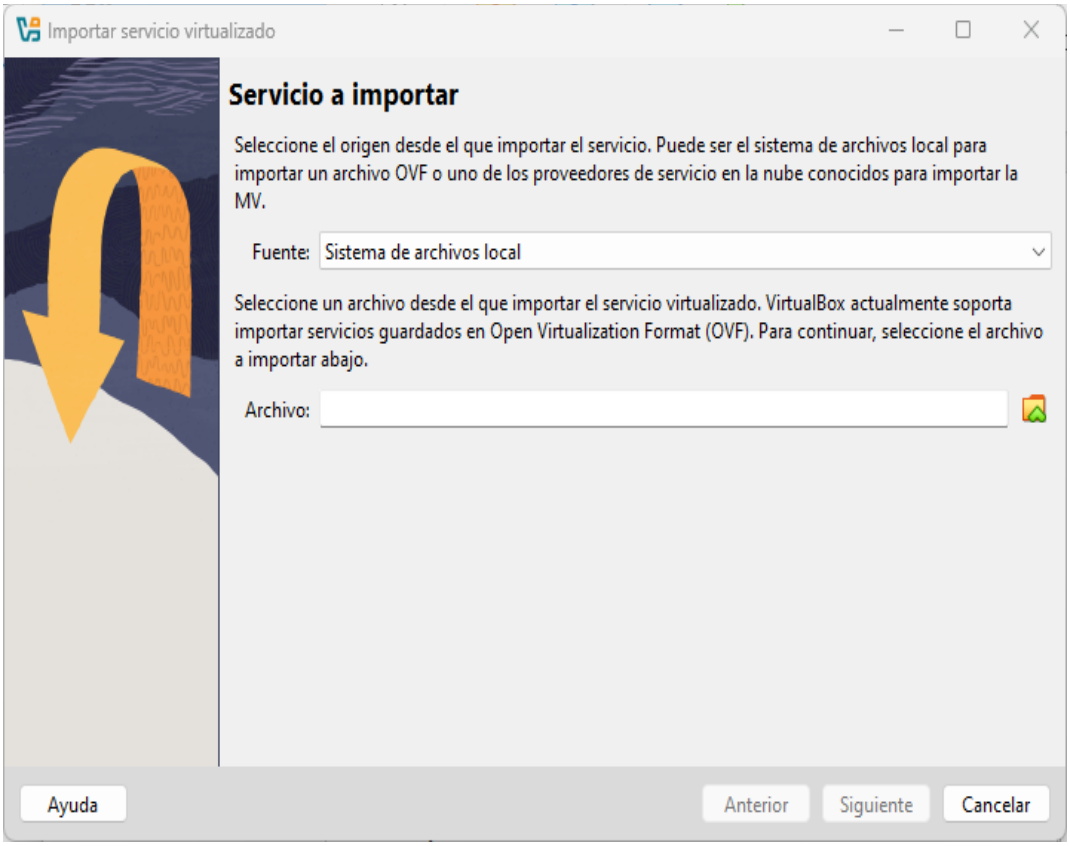
Fuente. Autoría propia

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

Se realiza la descarga de los archivos para el banco de trabajo del enlace https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/luis_zambrano_unad_edu_co/EkdfOBYMt0tDh-vNUeGND5QBlfEmt6nCQG0fsWnuXr8E9Q?e=cN102a

Figura 6

Descargar Archivos Banco de Trabajo

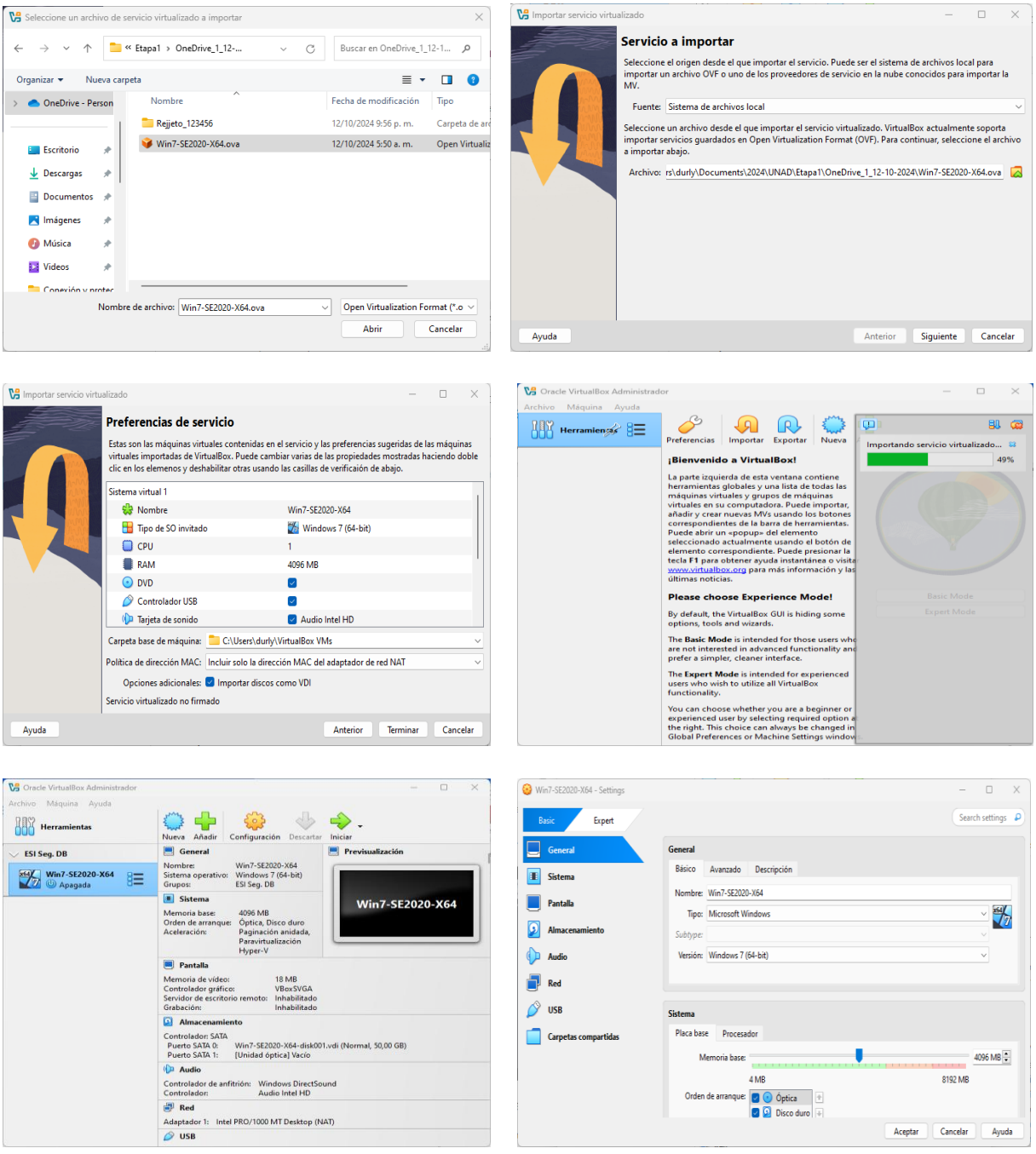


Fuente. Autoría propia

Intalación del sistema operativo de Windows 7 en la máquina virtual VirtualBo, en donde se importa del archivo Win7-SE2020-X64.ova a la máquina virtual VirtualBox

Figura 7

Instalación del Sistema Operativo Windows 7 en la Máquina Virtual Virtualbox

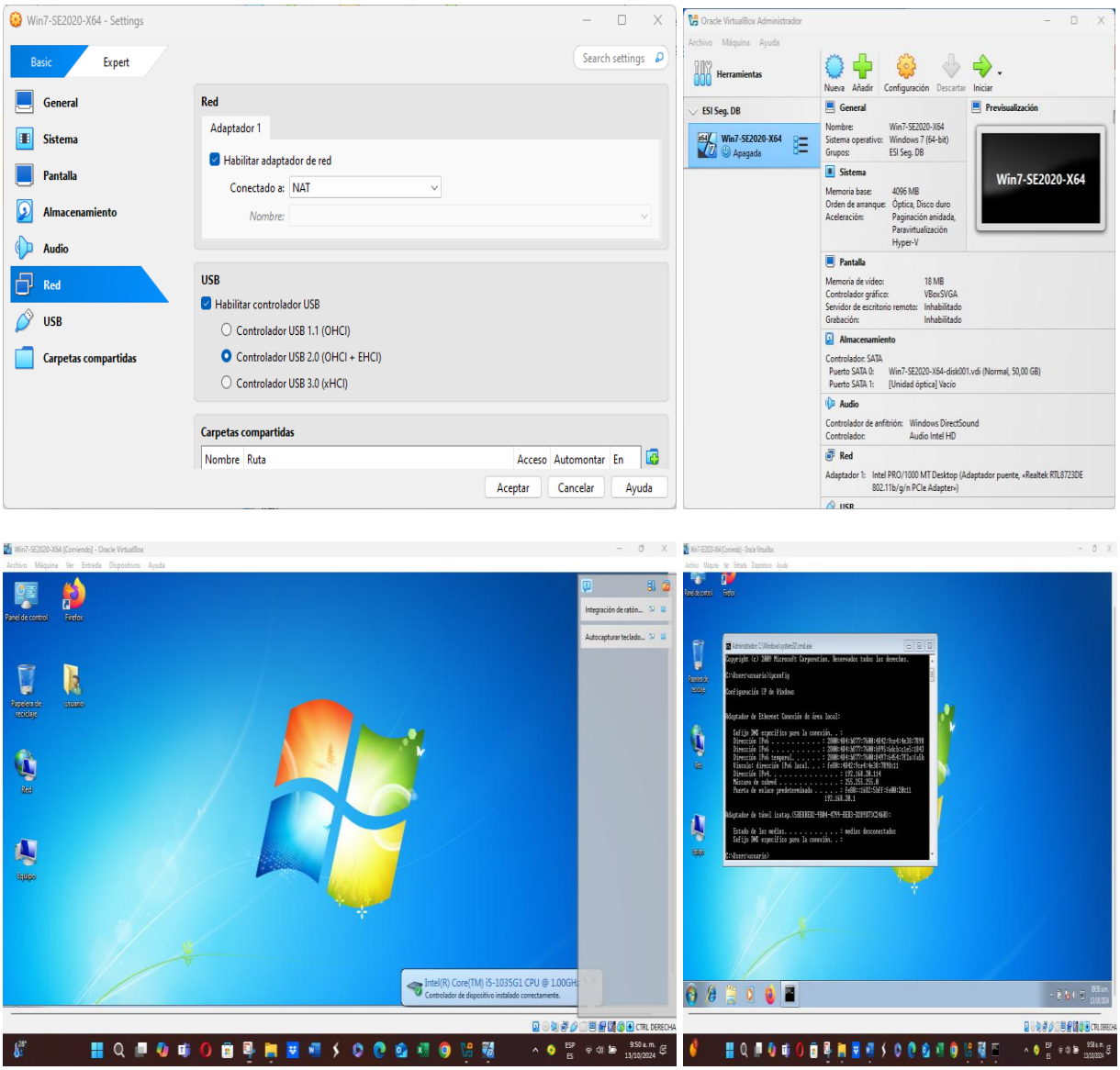


Fuente. Autoría propia

Cambiar el adaptador de red, de NAT a Adaptador puente

Figura 8

Cambio del Adaptador de Red, de NAT a Adaptador Puente

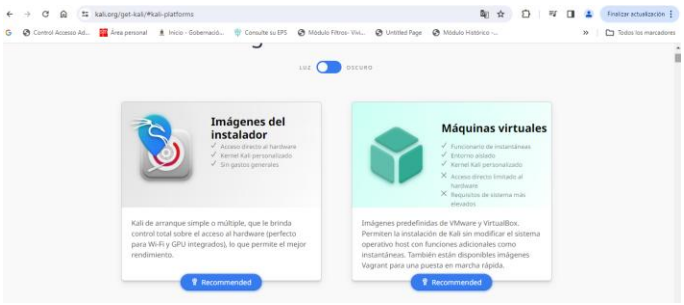


Fuente. Autoría propia

Instalación de Kali Linux, se procede a ingresar a la página web https://www.kali.org/get-kali/#kali-platforms, como se evidencia en la siguiente imagen, en el cual se selecciona Máquinas virtuales

Figura 9

Descargar la Instalación de Maquina Virtuales Kali Linux

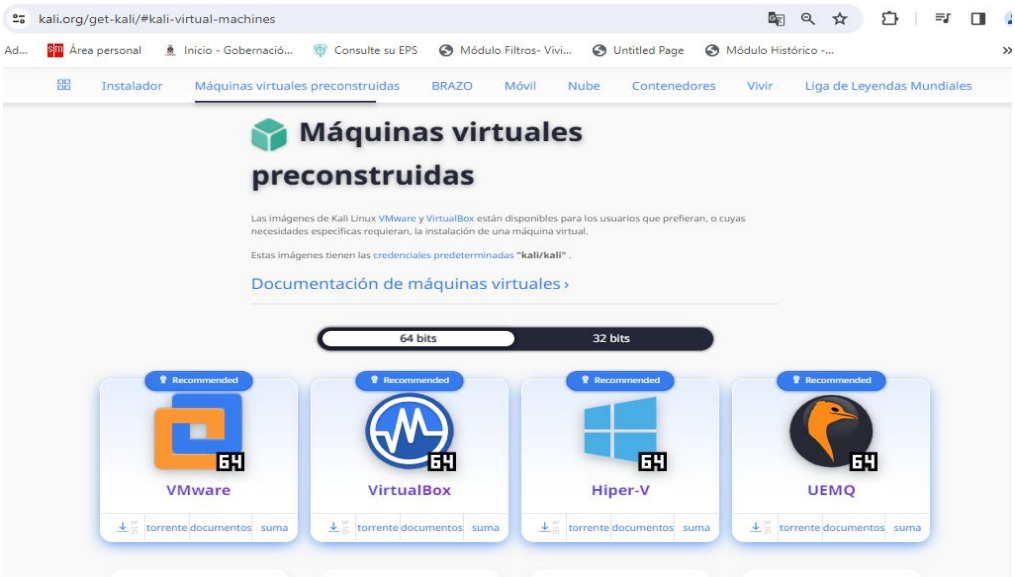


Fuente. Autoría propia

Se selecciona VirtualBox de 64 bits para proceder con la descarga de la imagen de Kali Linux, como se evidencia en la siguiente imagen:

Figura 10

Descargar Kali Linux

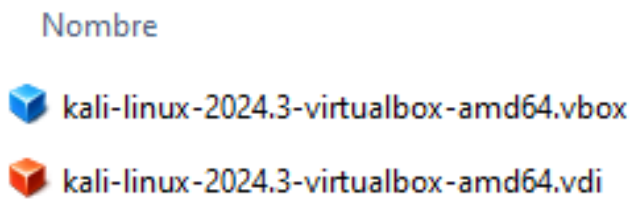


Fuente. Autoría propia

Archivos descargados de Kali Linux, para proceder a su instalación en la máquina virtual VirtualBox:

Figura 11

Archivos de Instalación de Kali Linux

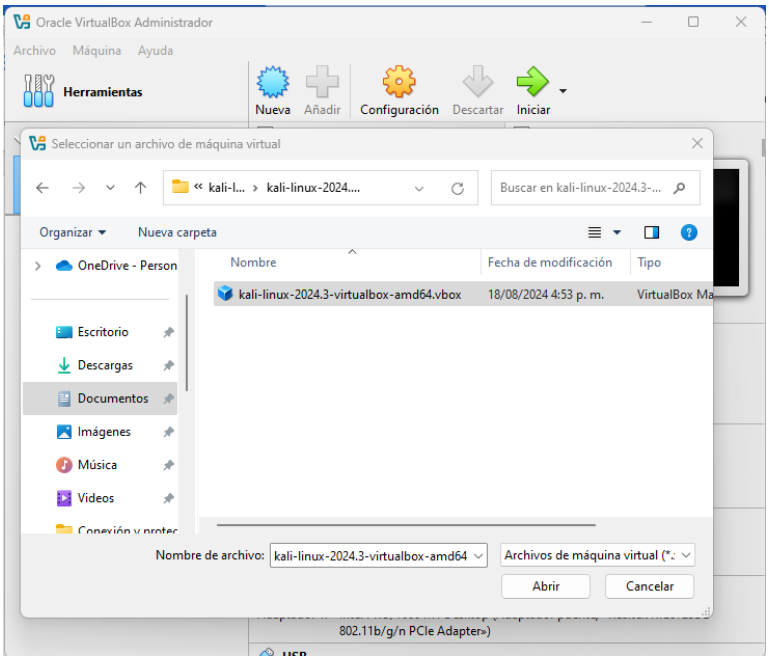


Fuente. Autoría propia

Para su instalación de Kali Linux, se ingresa a la máquina virtual VirtualBox, se elige la opción de añadir, en donde se despliega una ventana para abrir el archivo kali-linux-2024.3-virtualbox-amd64.vbox, como se evidencia en la siguiente imagen:

Figura 12

Instalación de Kali Linux

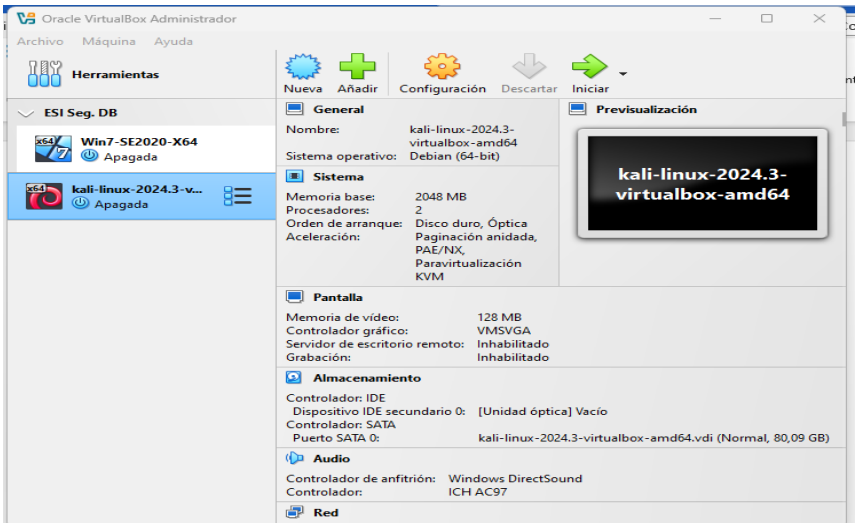


Fuente. Autoría propia

Instalación de Kali Linux en la Máquina virtual VirtualBox el cual se procede al menú iniciar para encender el sistema operativo Kali Linux:

Figura 13

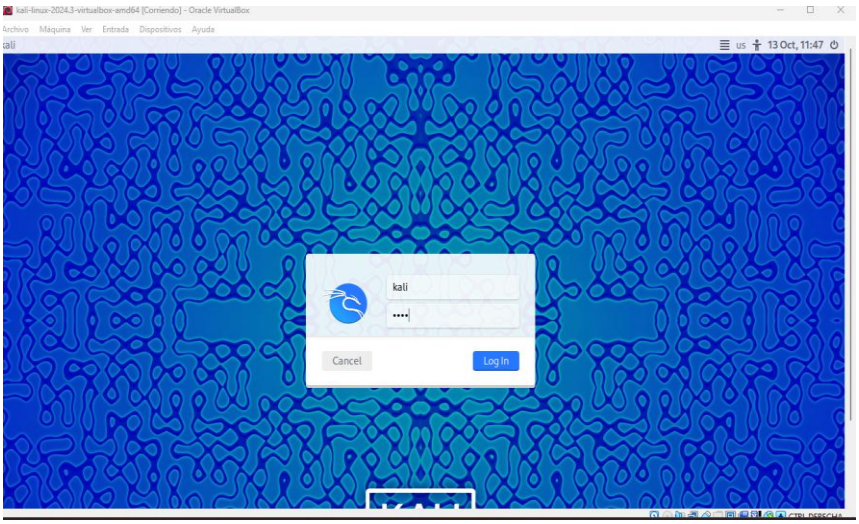
Instalación de la Máquina Virtual Kali Linux en la Máquina Virtualbox



Fuente. Autoría propia

Figura 14

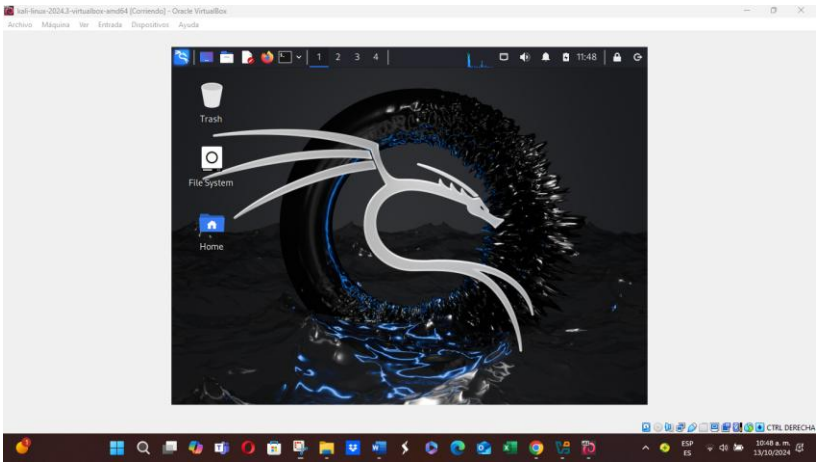
Ingreso al Sistema Operativo Kali Linux



Fuente. Autoría propia

Figura 15

Entorno Kali Linux

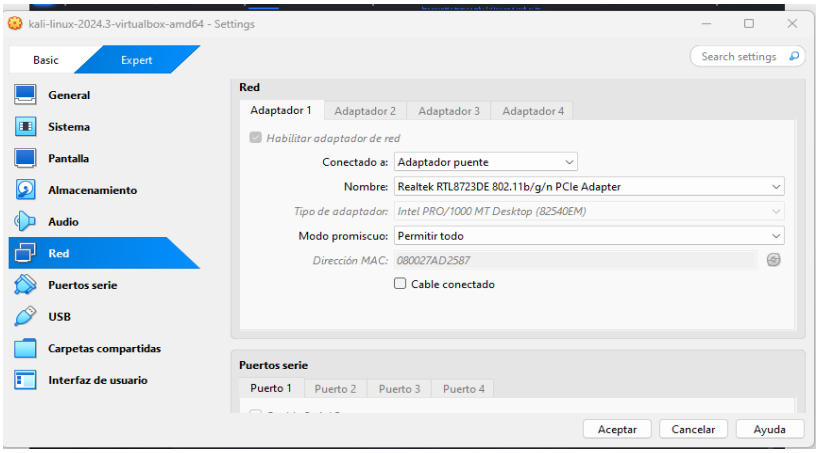


Fuente. Autoría propia

Configuración de Red, procede a seleccionar Adaptador puente, como se evidencia en la siguiente imagen:

Figura 16

Adaptador Puente

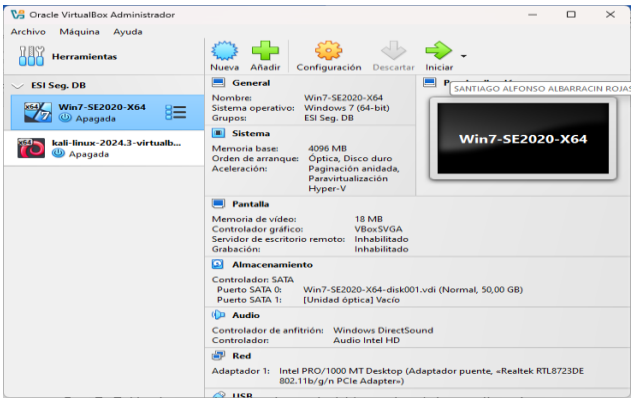


Fuente. Autoría propia

Paso C. Validación de la comunicación de las máquinas Windows con la máquina de Kali Linux, Ingreso al sistema operativo de Windows 7 con el fin de verificar la dirección de red

Figura 17

Validación de Máquinas Virtuales

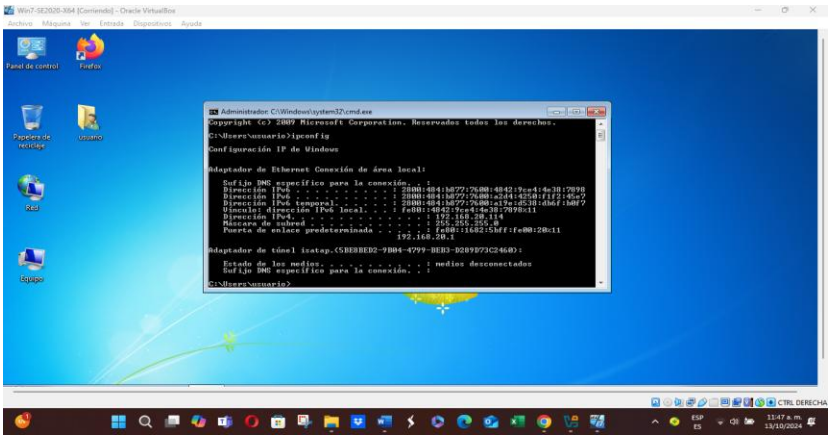


Fuente. Autoría propia

Busca de la dirección ip del sistema operativo de Windows 7, mediante el símbolo del sistema el cual se le da el comando ipconfig arrojado la dirección ip 192.168.20.114, como se evidencia en la siguiente imagen:

Figura 18

Ip del Sistema Operativo de Windows 7

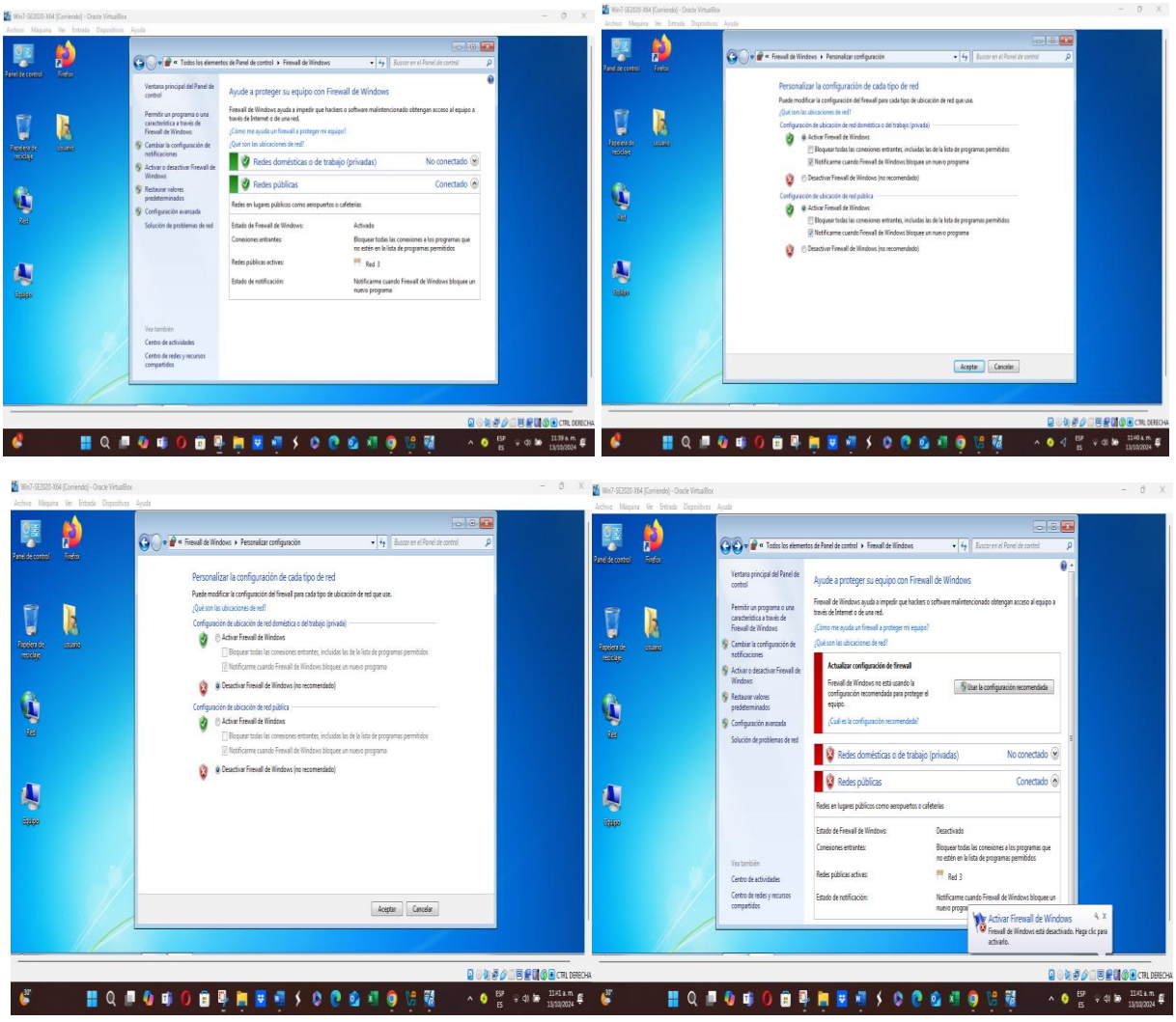


Fuente. Autoría propia

Ingreso al sistema operativo Windows 7 para proceder a realizar la comunicación con el equipo host, para proceder a realizar la comunicación se procede a desactivar el firewall

Figura 19

Desactivar el firewall

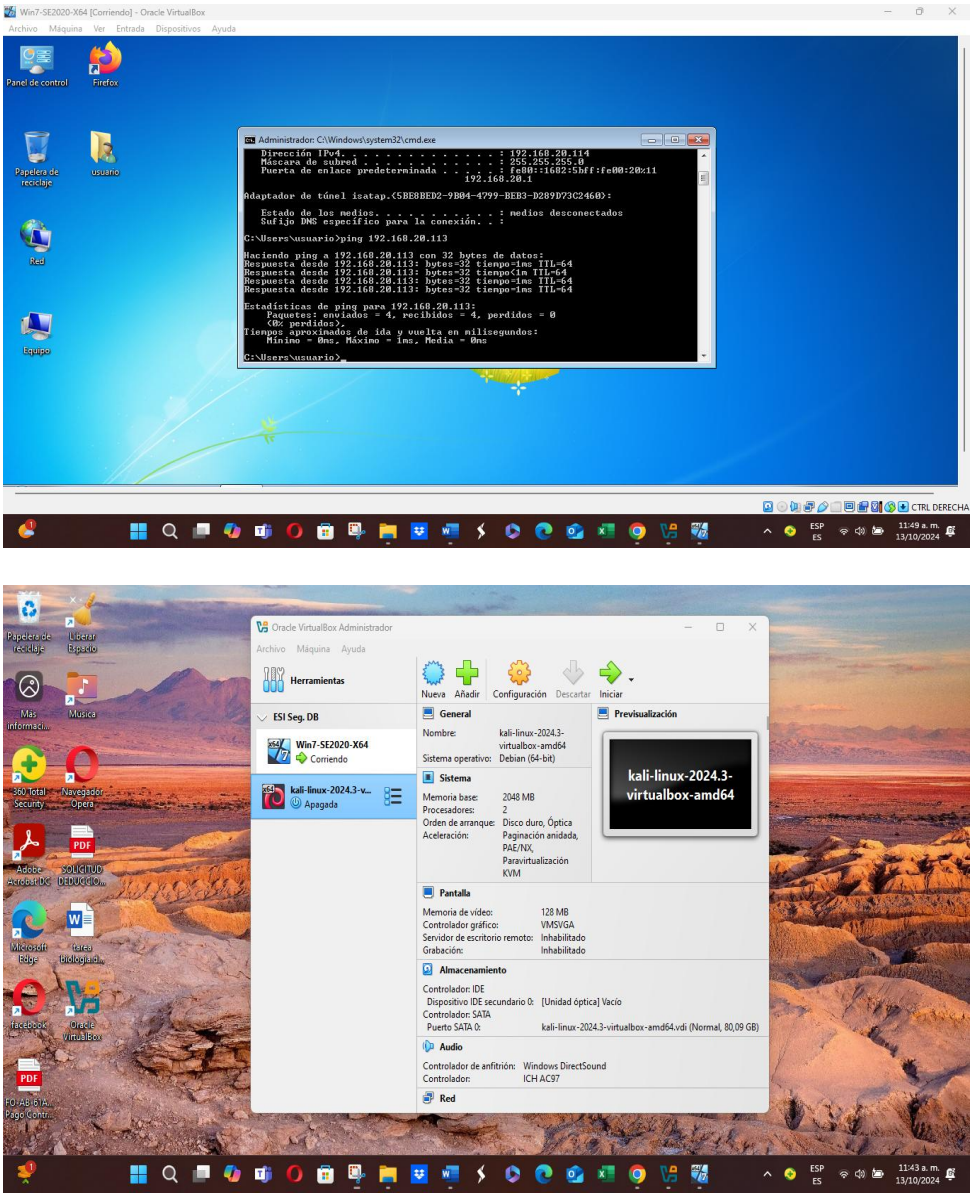


Fuente. Autoría propia

Conectividad de sistema operativo Kali Linux mediante la dirección ip 192.168.113 con el sistema operativo Windows 7 a la dirección ip 192.168.114

Figura 20

Conectividad de Sistema Operativo Kali Linux

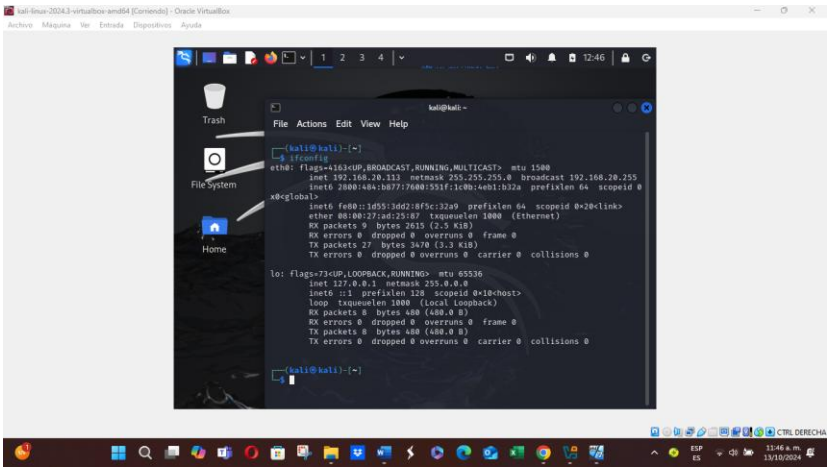


Fuente. Autoría propia

Busca de la dirección ip del sistema operativo de Kali Linux, mediante el símbolo del sistema el cual se le da el comando ifconfig arrojado la dirección ip 192.168.20.113, como se evidencia en la siguiente imagen:

Figura 21

Comando Ifconfig Arrojado la Dirección Ip 192.168.20.113

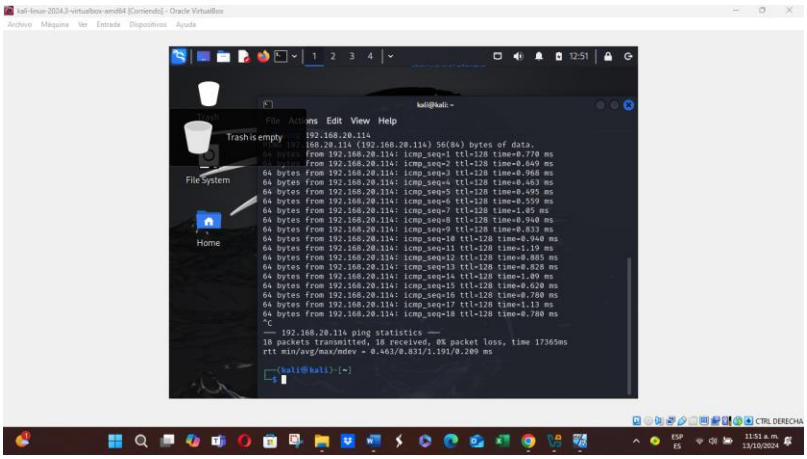


Fuente. Autoría propia

Conectividad de sistema operativo Windows 7 mediante la dirección ip 192.168.114 con el sistema operativo Kali Linux a la dirección ip 192.168.113

Figura 22

Conectividad de sistema operativo Windows 7

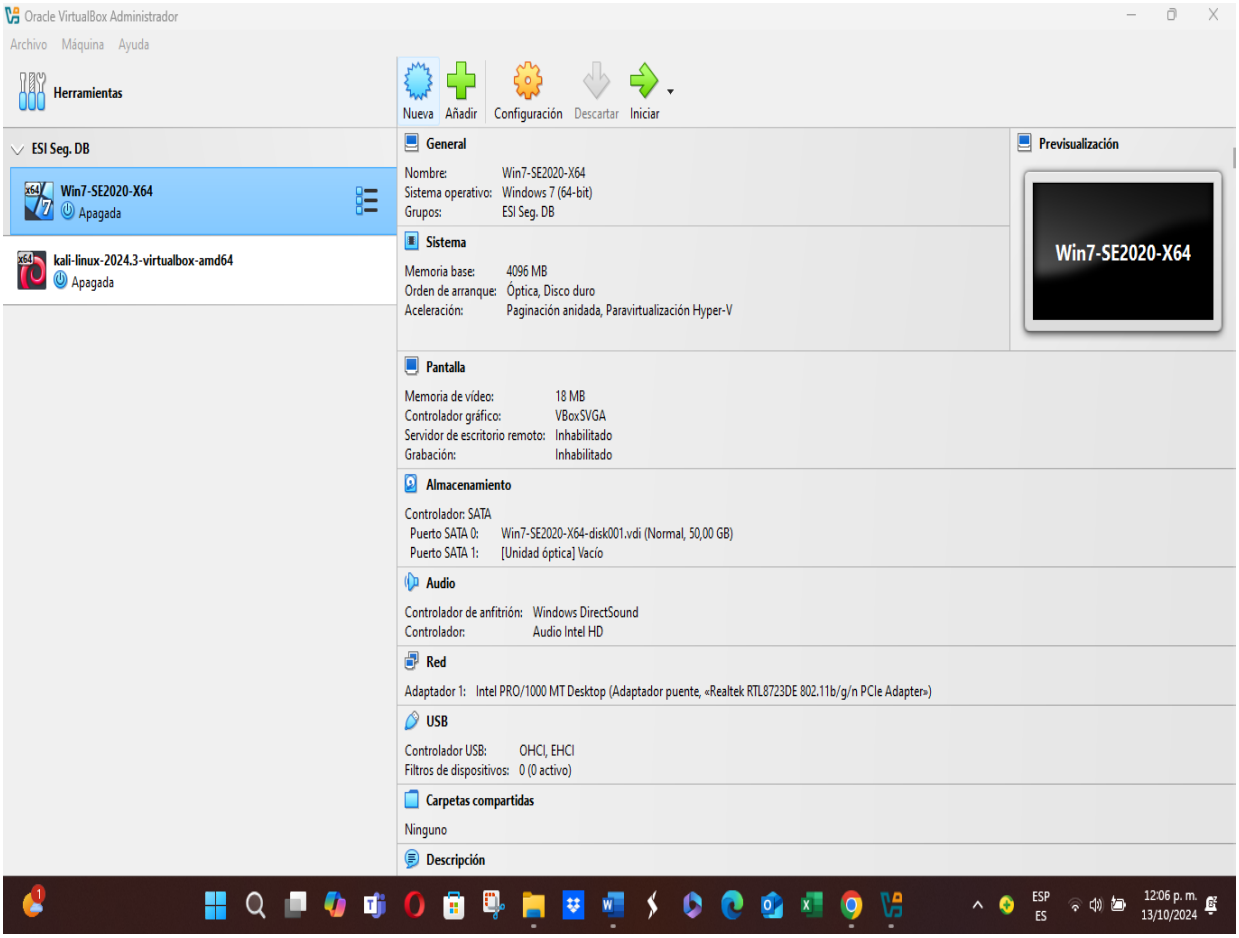


Fuente. Autoría propia

Paso D. Se realizan los respectivos printscreen el montaje del banco de trabajo y se evidencia el detalle de las características técnicas de hardware del sistema operativo Windows 7, sistema, almacenamiento, audio, red:

Figura 23

Características Técnicas de Hardware del Sistema Operativo Windows 7

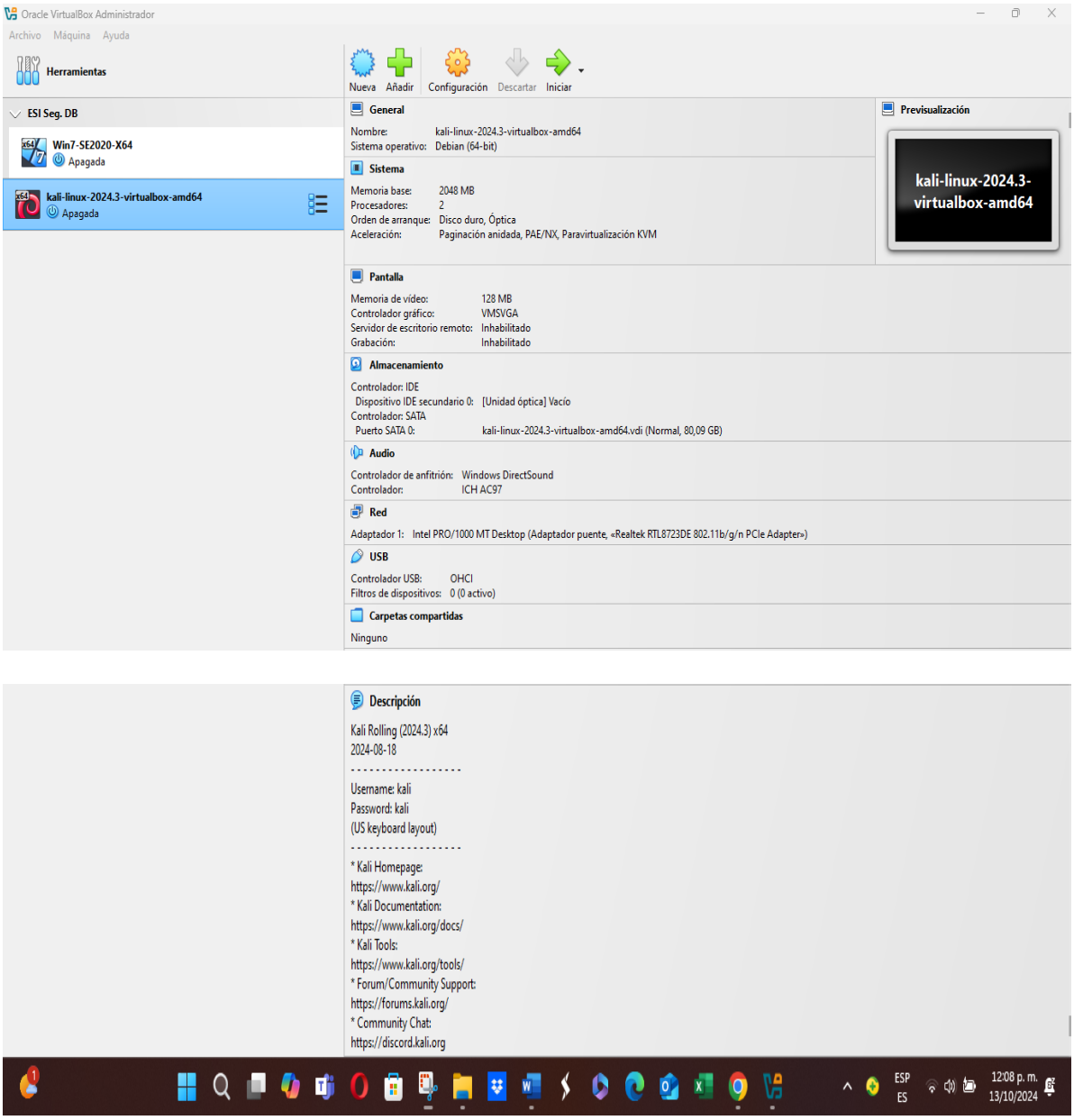


Fuente. Autoría propia

Se realizan los respectivos printscreen el montaje del banco de trabajo y se evidencia el detalle de las características técnicas de hardware del sistema operativo Kali Linux, sistema, almacenamiento, audio, red:

Figura 24

Características Técnicas De Hardware del Sistema Operativo Kali Linux

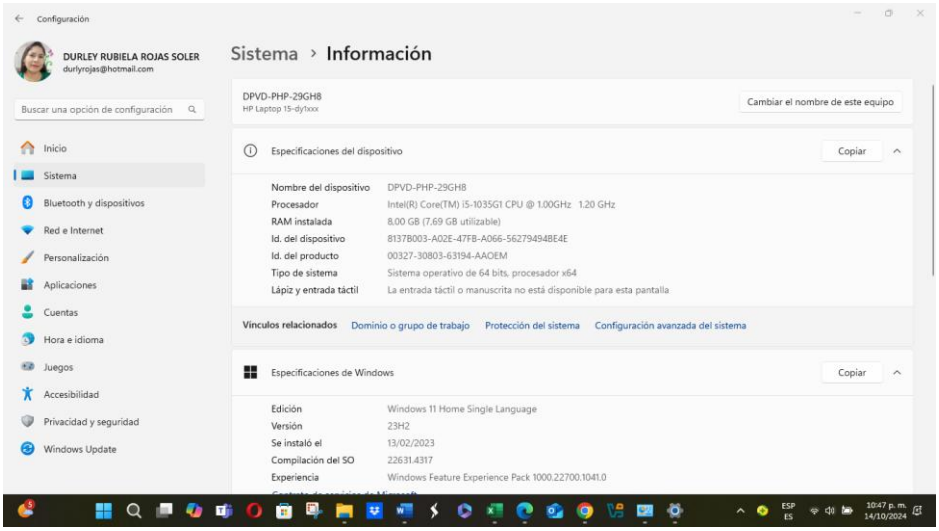


Fuente. Autoría propia

Se evidencia el detalle de las características técnicas de hardware del sistema host, sistema operativo Windows 11, procesador, RAM instalada:

Figura 25

Características Técnicas de Hardware del Sistema Host



Fuente. Autoría propia

Análisis de Acuerdo Desde el Punto de Vista Legal y No Ético

Se evidencia que la organización CyberFort Technologieses, no cuenta con herramientas, ni instrumentos de control que le permitan identificar anomalías y vulnerabilidades en los procesos y los procedimientos de la organización, con respecto a la contratación del personal, ya que se encontró con la situación de utilizar un contrato que no cumple con las normas legales y éticas que se deben de tener, debido a que el contrato utilizado, fue creado por un abogado que fue despedido por la organización por haber cometido procesos ilícitos, lo cual hace que el documento no sea confiable y que no cumpla con los protocolos de confidencialidad, por lo que se activa la alarma de mejorar la debilidades que la organización tiene, lo cual puede afectar sus bienes, capacidad productiva o patrimonio, por lo que tiene que establecer planes de mejora continua y en cumplir con la protección y seguridad de la información establecida en la Ley 1273

de 2009 de acuerdo al capítulo I sobre la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.

De acuerdo con el anexo3 se da a conocer el acuerdo de confidencialidad del personal a contratar y a la organización CYBERFORT TECHNOLOGIES, es un acuerdo ilegal, debido a que fue elaborado por el abogado despedido por realizar actos delictivos, lo que hace que el documento no sea confiable para poderlo utilizar como referencia.

Análisis en Relación a la Vulneración de la Ley 1273 Argumentando Cualquier Proceso Ilegal

Es ilegal ya que afecta la integridad y la ética de la organización CYBERFORT TECHNOLOGIES, por lo que el documento no está bien elaborado, y no está legalmente constituido, ya que se encontraron las siguientes falencias: No se evidencia la cláusula séptima, la cual es una falla muy grave al faltar información que lo documente, de igual manera en la cláusula 2 del numeral 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 de información, accesos abusivos a sistemas informáticos". está vulnerando e infringiendo la Ley 1273 de 2009 (Policía, 2009) de acuerdo con los siguientes artículos: Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, el cual se comete por las debilidades en los procedimientos y la vulnerabilidad en el acceso a los sistemas de información

el Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, 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, siempre que la conducta no constituya delito sancionado con una pena mayor, el cual se comete cuando sin autorización de la persona se realizan chuzadas a la información, el Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses, el cual se comete cuando se obstruyen sin autorización en su sitio de origen, en el destino o en el interior de un sistema informático y el Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, 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. el cual se produce cuando sin estar facultado vende, compra, sustrae, envía, divulga o emplea datos personales almacenados en medios digitales.

Análisis de la Propuesta Laboral, Teniendo Presente en Cuenta la Revisión Desde el Punto de Vista Legal y Ético

La respuesta a la propuesta laboral es negativa, teniendo en cuanta que no estoy de acuerdo con el proceso de contratación, porque no es confiable, ejemplo en la cláusula 4

Obligaciones de la parte receptora: 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros. Se estaría infringiendo el código de ética COPNIA (Copnia, 2015), de acuerdo con el capítulo II de los deberes y obligaciones profesionales, artículo 31 DEBERES GENERALES DE LOS PROFESIONALES. uno de los deberes generales es: 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, y en el artículo 32 las PROHIBICIONES GENERALES A LOS PROFESIONALES., una prohibición general es: Solicitar o aceptar comisiones en dinero o en especie por concepto de adquisición de bienes y servicios para su cliente, sociedad, institución, etc., para el que preste sus servicios profesionales, salvo autorización legal o contractual

Análisis del Caso "Ciberespionaje y Ética en Cyberfort Technologies" Desde su Posición Teniendo en Cuenta los Aspectos Legales y Éticos

Se puede evidenciar una falta gravísima encontrada en la auditoria de seguridad realizada en enero de 2024 a la organización CyberFort Technologies en sus sistemas de comunicaciones gubernamentales, en donde se detecta un software malicioso llamado "ShadowEye", que ilícitamente ha robado información confidencial, capturado correos electrónicos de los usuarios, entre otros, el cual pone en riesgo la confianza, integridad y ética en la prestación de sus servicios de protección de infraestructura crítica y asesoramiento en seguridad digital a gobiernos y corporaciones de América latina, de la organización y a la penalización por estar infringiendo la ley 1273 de 2009 (Policía, 2009) con respecto al espionaje cibernético el cual está contemplado en los siguientes artículos:

Tabla 3

Descripción De La Normatividad En El Caso Cibernético

Caso Cibernético	Artículos	Descripción	Condena
La organización CyberFort no cuenta con mecanismos de defensa, ni acuerdos de confidencialidad en sus sistemas de información, por lo que infringe el artículo 269A	269A Acceso abusivo a un sistema informático"	Se causa cuando aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos al interior de la organización o empresa.	Pena de Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
Los empleados de CyberFort accedieron a comunicaciones sensibles y documentos estratégicos relacionados con temas de defensa, política exterior y negociaciones comerciales, sin la autorización de los clientes, por lo que infringen en el artículo 269B	269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.	Se causa cuando bloquean en forma ilegal un sistema o impiden su ingreso, a cuentas de correo electrónico de otras personas, sin su autorización	Pena de Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes., siempre que la conducta no constituya delito sancionado con una pena mayor.
Los empleados de CyberFort accedieron a	269C: Interceptación de datos informáticos.	Se causa cuando obstruyen datos sin autorización legal, en su sitio de origen, en el destino	Pena de Prisión 36 a (72) meses

Caso Cibernético	Artículos	Descripción	Condena
comunicaciones sensibles y documentos estratégicos relacionados con temas de defensa, política exterior y negociaciones comerciales, sin consentimiento de los clientes, por lo que infringen en el artículo 269C		o en el interior de un sistema informático	
La organización CyberFort no cuenta con herramientas de pentestig que permitan identificar con tiempo el software maligno llamado "ShadowEye", tenía la capturar correos electrónicos, y robar documentos confidenciales, sin autorización de los clientes, por lo que infringe el artículo 269D	Artículo 269D: Daño Informático.	Se cauda cuando una persona que sin estar autorizado modifica, altera, daña, elimina, destruye o suprime datos del programa o documentos electrónicos y se hacen en los recursos de TIC	Pena de Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Caso Cibernético	Artículos	Descripción	Condena
La organización CyberFort no cuenta con herramientas de pentestig que permitan identificar con tiempo el software maligno llamado "ShadowEye", por lo que se evidencia las debilidades en los sistemas de información, lo que infringe el artículo 269E	269E: Uso de software malicioso.	Se causa cuando se adquieren distribuyen, envían, introducen o extraen del país software o programas de computador que produce daños en los recursos TIC	Pena de Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
Los empleados de CyberFort vendieron la información obtenida en mercados de la darknet y a empresas rivales en la industria de defensa y tecnología, por lo que infringen el artículo 269F	269F: Violación de datos personales	Se causa cuando sin estar facultado sustrae, envía, vende, divulga, compra o emplea datos personales almacenados en medios magnéticos	Pena de Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
Los empleados de CyberFort accedieron a comunicaciones	269G: Suplantación de sitios web para capturar datos personales.	Se causa cuando una página web es similar a la de una entidad y envía correos electrónicos (spam) como	Pena de Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios

Caso Cibernético	Artículos	Descripción	Condena
sensibles, por lo que puede estar infringiendo en el articulo 269G		ofertas de empleo y personas inocentes suministran información personal y claves bancarias y el delincuente informático ordena transferencias de dinero a terceros.	mínimos legales mensuales vigentes., siempre que la conducta no constituya delito sancionado con pena más grave.
Los empleados de CyberFort vendieron la información obtenida en mercados de la darknet y a empresas rivales en la industria de defensa y tecnología, por lo que están obteniendo provecho para ellos, por lo que infringen el artículo 269H	269H: Circunstancias de agravación punitiva:	1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por	Las penas se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

Caso Cibernético	Artículos	Descripción	Condena
		tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.	
Manipulación a los sistemas de información de la organización CyberFort Technologies, por las debilidades que tiene en sus sistemas informáticos, se aplica el artículo 269I	269I: Hurto por medios informáticos y semejantes.	Se causa cuando manipulan un sistema de información, una red de sistemas electrónicos, telemáticos u otro medio semejante o suplantación a un usuario ante sistemas de autenticación y de autorización establecidos	Las penas de prisión señaladas en el artículo 240 de este Código. De 3 a 8 años
Los empleados de CyberFort sin autorización transfirieron información en mercados de la darknet y a empresas rivales en la industria de defensa y tecnología, infringiendo el artículo 269J	269J: Transferencia no consentida de activos.	Se causa cuando utilizando algún truco o manipulación informática efectúa la transferencia no autorizada de cualquier activo en perjuicio de un tercero en provecho propio. Este delito también se denomina estafa electrónica, igual manera se presenta cuando fabrica, introduce o facilita programas de computador para cometer los anteriores delitos	Pena de Prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Fuente. Auditoria propia

Al sustraer y vender información en mercados de la darknet y a empresas rivales en la industria de defensa y tecnología los empleados están incumplimiento el código de la ética profesional (Copnia, 2015), contemplados en el capitulo II en el artículo 33 Deberes generales de los profesionales b) Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados, lo cual se convierte en una falta gravísima y en la cancelación de la matricula profesional para seguir ejerciendo su profesión.

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida? Las empresas no deben, ni pueden tener acceso a información sensible de sus clientes, ni tampoco pueden suministrar la información en las auditorías internas, porque vulneran el principio de la confianza y seguridad de la información.

Las auditorías internas en los sistemas de información son necesarias y útiles porque permiten identificar y controlar de manera oportuna las vulnerabilidades que se puedan presentar, como se evidenció en el anexo 7 escenario 2. Que por medio de la auditoria interna a los sistemas de información se detectó el software malicioso, el cual fue mitigado y eliminado.

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?. Los mecanismos que se deben contemplar en cualquier organización, empresa o usuario sobre ciberseguridad son políticas de seguridad y protección de la información y de datos personales, las cuales están contempladas en la Ley 1273 de 2009, También se deben establecer mecanismos de detección de vulnerabilidades utilizando

equipos Red Team & Blue Team, los cuales permiten mitigar a tiempo las vulnerabilidades y ataques informáticos que se puedan presentar. Pruebas de pentesting las cuales nos permiten identificar las vulnerabilidades de seguridad en los sistemas de información, redes y aplicaciones a tiempo y poderlos mitigar. De igual manera establecer los acuerdos de confidencialidad y establecer en los planes de mejora continua las auditorias internas, las cuales permiten controlar y evaluar las falencias que se puedan estar cometiendo y puedan estar afectando a la organización en la prestación de los servicios.

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? Realizando las respectivas denuncias penales a las entidades competentes encargadas de salvaguardar la protección, la seguridad de la información y datos personales, por el incumplimiento a la Ley 1273 de 2009 y al código de ética sobre el abuso de confidencialidad, integridad y disponibilidad de los datos informáticos, con el fin de que sean aplicadas las sanciones y penas de prisión acorde al delito informático, cometido por el ciberespionaje, robo de información, entre otros.

¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente? Mejorando los procesos y procedimientos de seguridad de la información, estableciendo políticas de seguridad y protección de la información y datos personales, acuerdos de disponibilidad, confidencialidad, integridad de la información. Cumpliendo con la Ley 1273 de 2009 como respaldo en la mitigación de los delitos informáticos y protección a los datos personales, en el cumplimiento al código de ética de los profesionales para la prestación de sus servicios, en utilización de herramientas que permitan identificar a tiempo las vulnerabilidades en implementar periódicamente auditorías internas, las cuales nos permiten evidenciar las falencias y debilidades en que se está fallando para poder implementar la mejor continua a los

procesos y poder recuperar la confianza y credibilidad de la empresa en la prestación de sus servicios a su clientes.

Informe de Herramientas y Procedimientos Utilizados Para Dar Solución al Escenario de Red Team de Acuerdo a los Pasos del Pentesting

Se identificó al interior de la organización en uno sus equipos de cómputo una vulnerabilidad que es la fuga de información, para dar solución a esta situación se procede a utilizar las pruebas de penetración pentesting, como herramienta de seguridad, la cual nos identifica las debilidades que se están presentando en el robo de información, por tal motivo para evaluar la seguridad de la organización se requiere aplicar las 5 fases del proceso que realiza el pentesting, el cual se describe en la siguiente tabla:

Tabla 4

Las 5 Fases del Proceso que Realiza el Pentesting,

Fases	Descripción	Escenario	Herramientas
1. Reconocimiento	Recopilación de la información ejemplo: Fuentes de información, Direcciones IP de servicios tercerizados, Existencia de redes inalámbricas, Dirección física de la empresa, Rangos de direcciones IP asignados, entre otras, con el fin delimitar las áreas a evaluar y poder generar estrategias de ataque	Se realiza recopilación de información de los sistemas de información de la organización para poder detectar el sistema objetivo, por lo que se ha identificado un reconocimiento activo el cual se procede a revisar y evaluar.	Para esta fase se utiliza la herramienta Nmap, que realiza el escaneo detallado del sistema y de los puertos utilizando los comandos[-sV] intenta determinar la versión del servicio en el objetivo, [-O] informa el sistema operativo en el objetivo, entre otros. También podemos utilizar otras

Fases	Descripción	Escenario	Herramientas
	que sean eficientes al mitigar la vulnerabilidad que se presente		herramientas como footprinting y ,metasploit, para la recolección de información.
2. Análisis de vulnerabilidades	Realiza a fondo la evaluación de todos los elementos que están involucrados desde su inicio hasta su final verificando el estado dinámico y estático del sistema	Se realiza un escaneo a fondo a todos los sistemas de información de la organización, con respecto a los servicios que se están ejecutando en la red, los puertos, por lo que se encuentra una debilidad que está alojada en un equipo de cómputo.	Para esta fase se utiliza la herramienta Nmap, la cual permite realizar un escaneo de la red para identificar los dispositivos activos utilizando el comando [-iL] indica el listado de redes o equipos a escanear > nmap –iL hosts.txt, , [-p] lista los puertos que se desean escanear
3. Explotación	Evaluación de vulnerabilidades se realiza la identificación sobre las posibles debilidades a las vulnerabilidades encontradas que pueden ser detonadas por un atacante informático	Se procede a evaluar la debilidad encontrada, dentro de un equipo de cómputo de la organización, por lo que se empieza a realizar la revisión del sistema con respecto a la versión si presenta vulnerabilidades, si esta desactualizada, o presenta fallos, por lo que al realizar la explotación se encuentro la	Para esta fase se utiliza la herramienta Nmap, el cual nos permite identificar la versión del sistema, el servicio, y el puerto que está corriendo el servicio. También se puede utilizar la herramienta de metasploit, utilizando meterpreter,

Fases	Descripción	Escenario	Herramientas
		vulnerabilidad que es la fuga de Información la cual está instalada bajo el sistema operativo Windows 7. Por lo que se procede a realizar la mitigación de la vulnerabilidad encontrada.	
4. Escalar privilegios o Post Explotación	Se realiza cuando el evaluador ha identificado las vulnerabilidades a explotar predominando las siguientes tareas como son: la detección de barreras de protección, detección de módems activos, detección de servicios activos, detección de equipos activos, entre otros	Se procede a ingresar al sistema por medio de la vulnerabilidad, la cual permite la entrada a la máquina objetivo y a la escalación de privilegios, en donde se logra el ingreso como administrador con todos los permisos que se requieran para poder realizar los cambios pertinentes a la máquina objetivo y garantizar la conexión para poder logra mitigar la vulnerabilidad, sin dejar registros, ni rastros de las actividades que fueron ejecutadas durante la explotación.	Para esta fase se utiliza como herramienta Metasploit, la, cual identifica y evalúa las vulnerabilidades de los sistemas objetivo para ejecutar los exploits de las vulnerabilidades, poder tener el acceso para el escalamiento de permisos
5. Informe	En el cual entrega detalladamente los hallazgos encontrados de las vulnerabilidades	Se hace entrega un informe detallado de las debilidades encontradas en la organización,	Para esta fase se utilizan como herramientas el Nmap y Metasploit,

Fases	Descripción	Escenario	Herramientas
	que se explotaron con el fin de mitigar los riesgos de seguridad, tener en cuenta las recomendaciones para robustecer la seguridad.	iniciando con la recopilación de la información en donde se analiza y se realiza un escaneo a los sistemas informáticos, logrando identificar el equipo de cómputo en el cual se está realizando una fuga de información, porque tiene instalada una aplicación vulnerable bajo Windows 7, por los que el equipo de Red Team realiza la identificación y la explotación de la vulnerabilidad detectada y se logra por medio del escalamiento de privilegios ingresar como administrador y poder mitigar la vulnerabilidad sin dejar rastro ni huellas de las actividades realizadas en la ejecución de la debilidad encontrada.	

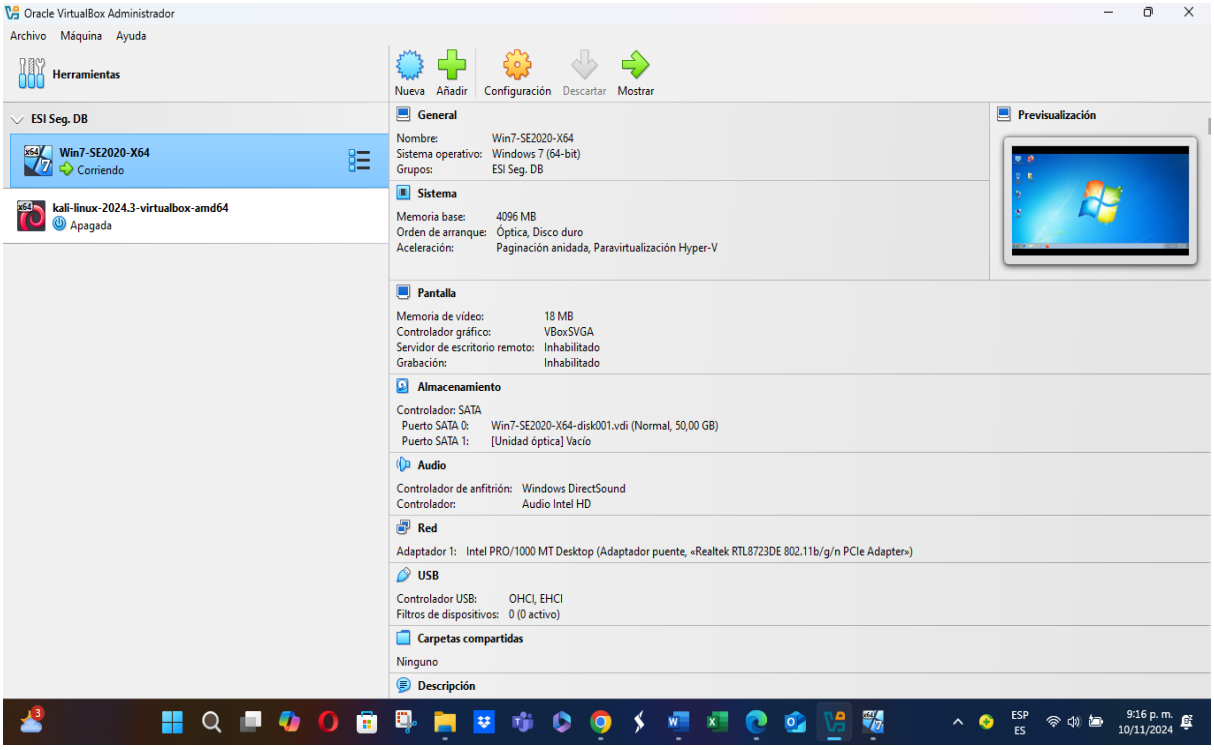
Fuente. Autoría propia

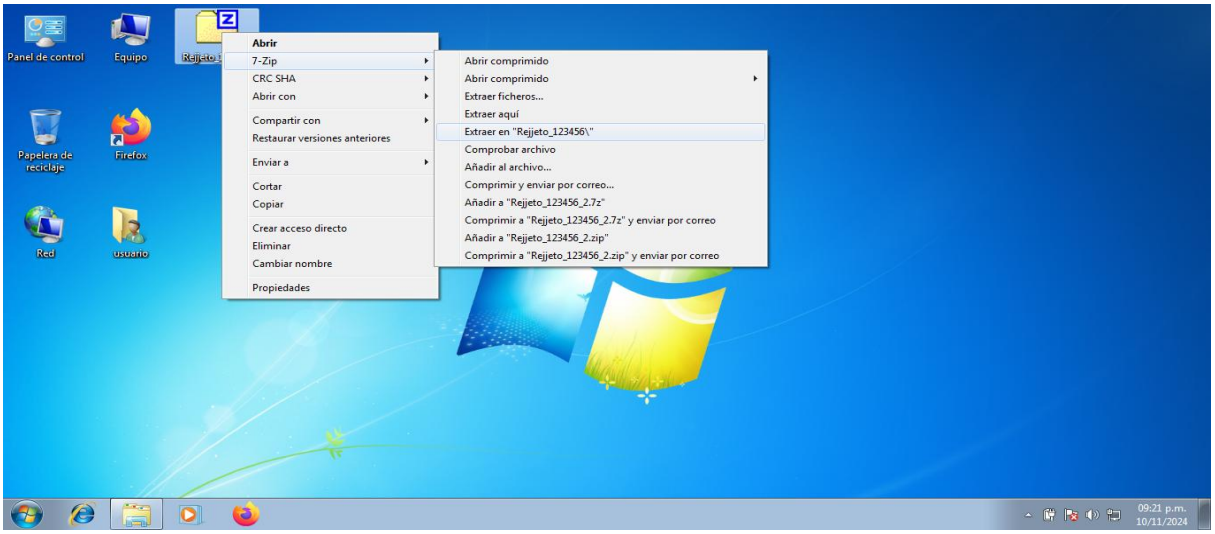
Análisis del Ataque Presentado a Cada Una de las Maquinas Identificadas

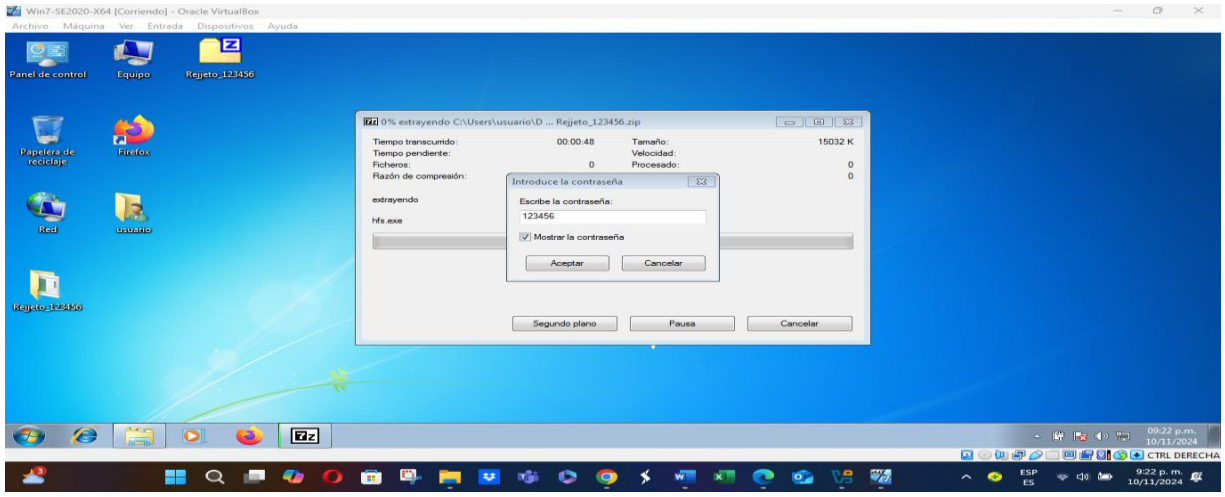
Para realizar el análisis de la vulnerabilidad, se procede a realizar la validación de la comunicación de las máquinas Windows7 con la máquina de Kali Linux, Ingreso al sistema operativo de Windows 7 en donde se procedió a desactivar el firewall, también se realizó la a cada máquina la verificación de la ip de cada una de las máquinas: Para el sistema operativo Kali Linux mediante el comando ifconfig en donde se evidencia la inet 192.168.113 con el sistema operativo Windows 7 el comando ipconfig donde se evidencia la Dirección IPv4 192.168.114

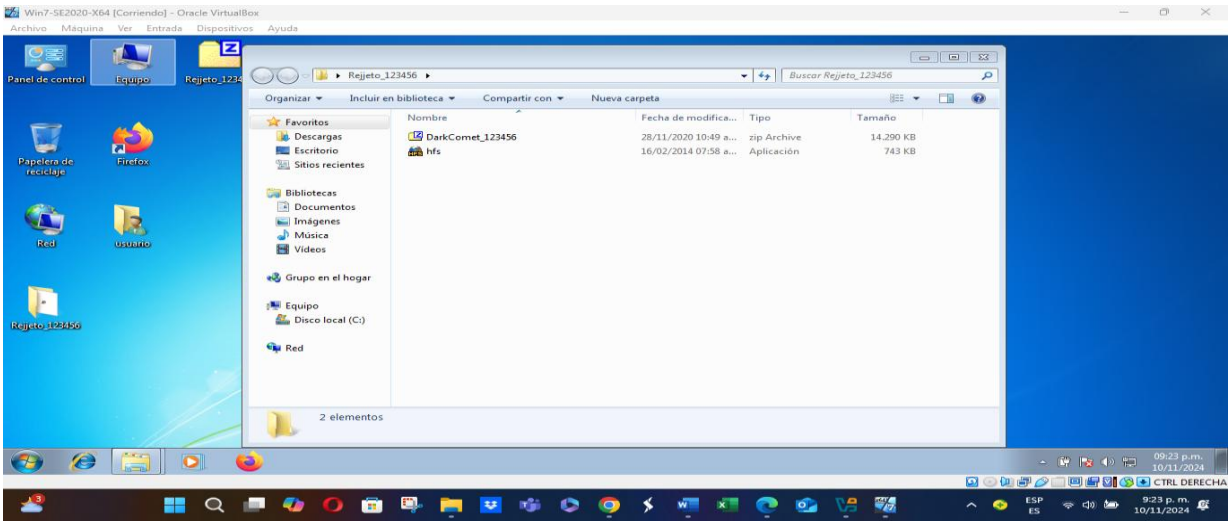
Figura 26

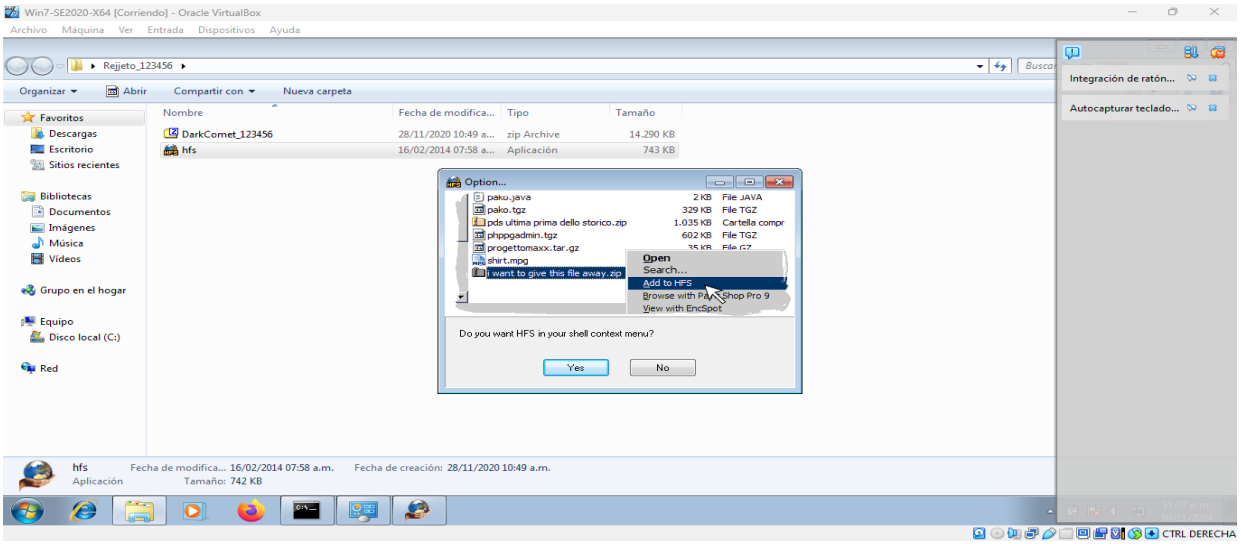
Validación de la Comunicación de las Máquinas Windows7 con la Máquina de Kali Linux

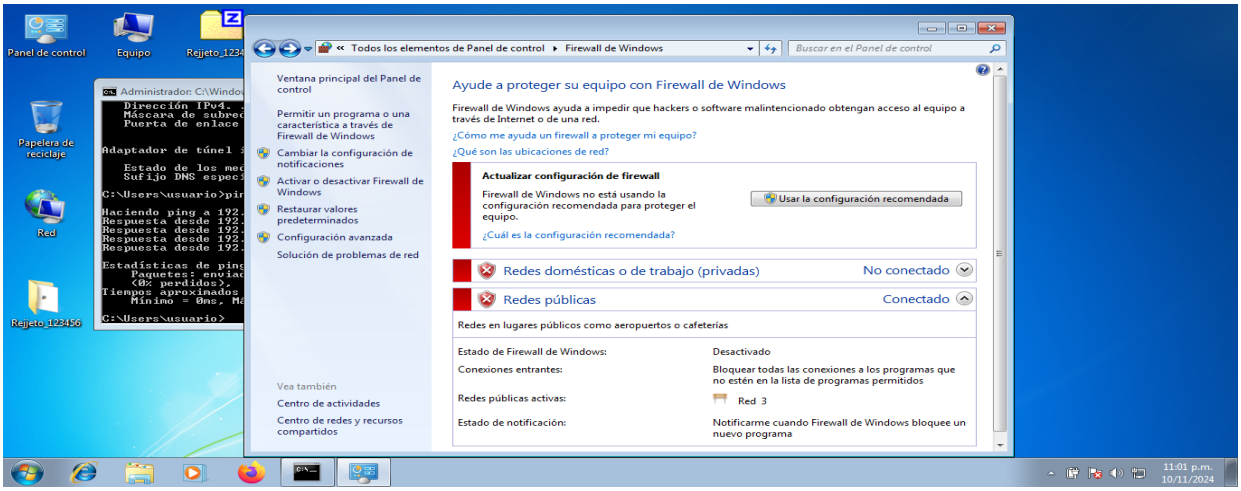


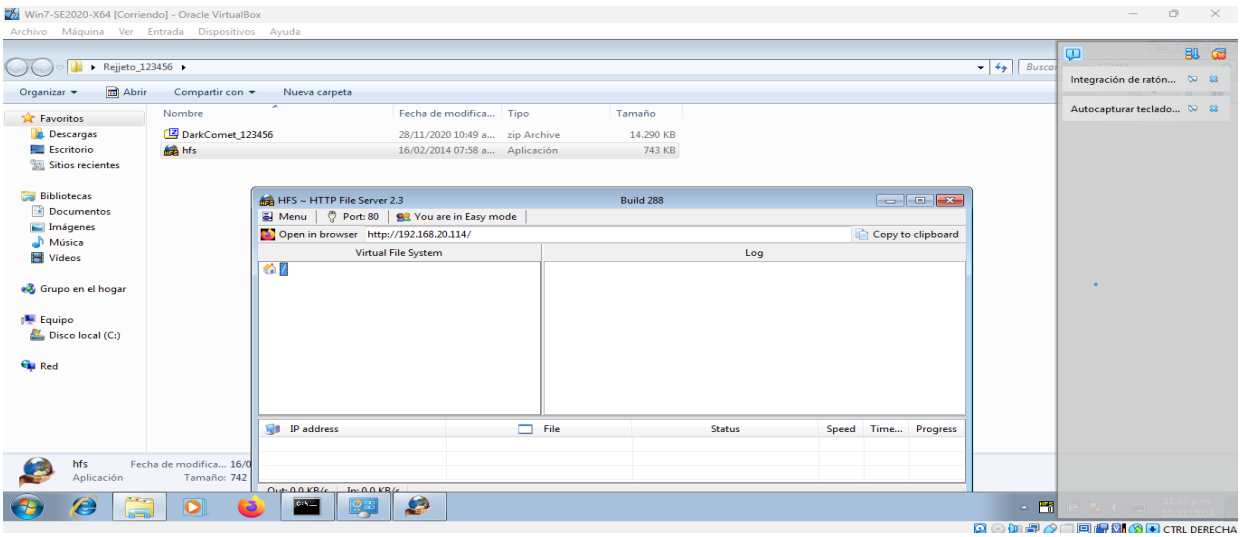

Panel de control
Equipo
Rejeto_123456
Papelera de reciclaje
Firefox
Red
usuario
Abrir
7-Zip
CRC SHA
Abrir con
Compartir con
Restaurar versiones anteriores
Enviar a
Cortar
Copiar
Crear acceso directo
Eliminar
Cambiar nombre
Propiedades
Abrir comprimido
Abrir comprimido
Extraer ficheros...
Extraer aquí
Extraer en "Rejeto_123456\"
Comprobar archivo
Añadir al archivo...
Comprimir y enviar por correo...
Añadir a "Rejeto_123456_2.7z"
Comprimir a "Rejeto_123456_2.7z" y enviar por correo
Añadir a "Rejeto_123456_2.zip"
Comprimir a "Rejeto_123456_2.zip" y enviar por correo
09:21 p.m.
10/11/2024

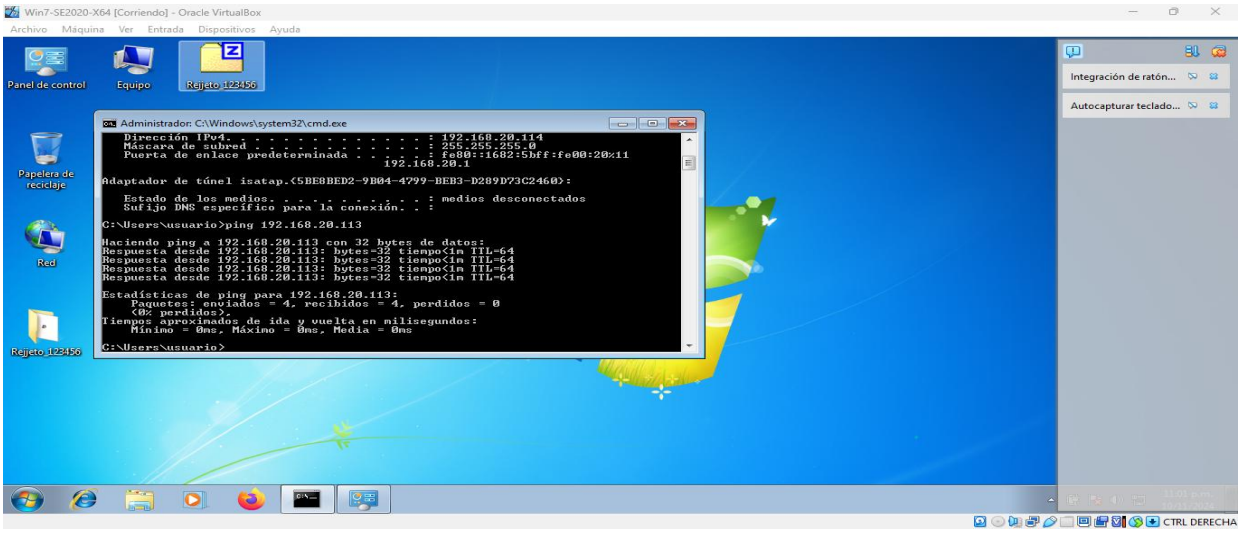

Win7-SE2020-X64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Panel de control
Equipo
Rejeto_123456
Papelera de reciclaje
Firefox
Red
usuario
0% extrayendo C:\Users\usuario\D ... Rejeto_123456.zip
Tiempo transcurrido: 00:00:48
Tiempo pendiente:
Ficheros: 0
Razón de compresión:
Tamaño: 15032 K
Velocidad:
Procesado: 0
0
extrayendo
hfs.exe
Introduce la contraseña
Escribe la contraseña:
123456
Mostrar la contraseña
Aceptar
Cancelar
Segundo plano
Pausa
Cancelar
09:22 p.m.
10/11/2024
CTRL DERECHA
ESP
ES
9:22 p. m.
10/11/2024

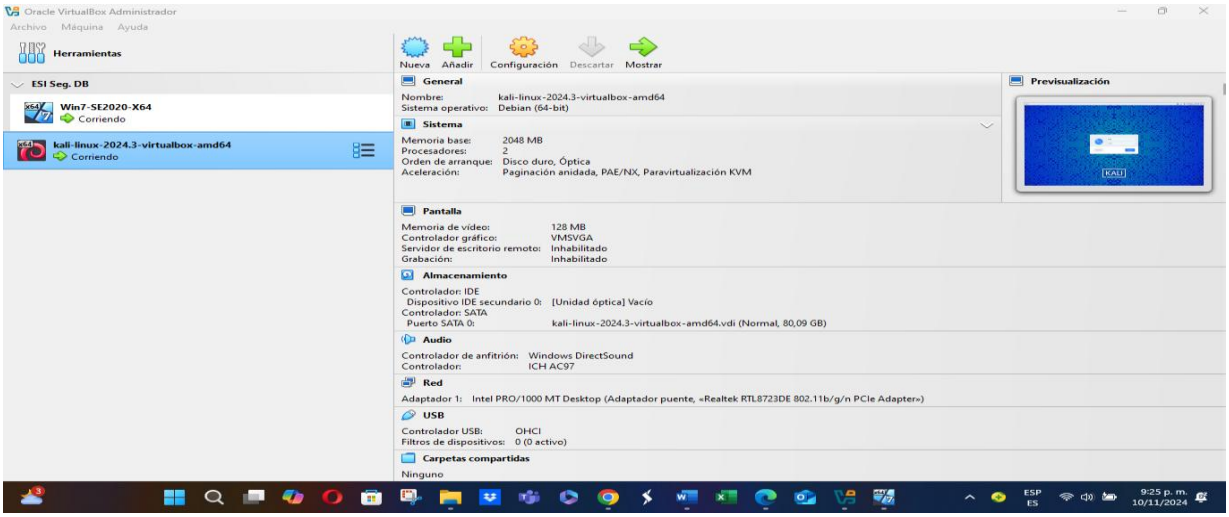

Win7-SE2020-X64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Panel de control
Equipo
Papelera de reciclaje
Firefox
Red
usuario
Rejeto_123456
Rejeto_123456
Buscar Rejeto_123456
Organizar
Incluir en biblioteca
Compartir con
Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Grupo en el hogar
Equipo
Disco local (C:)
Red
Nombre
Fecha de modifica...
Tipo
Tamaño
DarkComet_123456
28/11/2020 10:49 a...
zip Archive
14.290 KB
hfs
16/02/2014 07:58 a...
Aplicación
743 KB
2 elementos
09:23 p.m.
10/11/2024
CTRL DERECHA
ESP
ES
9:23 p. m.
10/11/2024

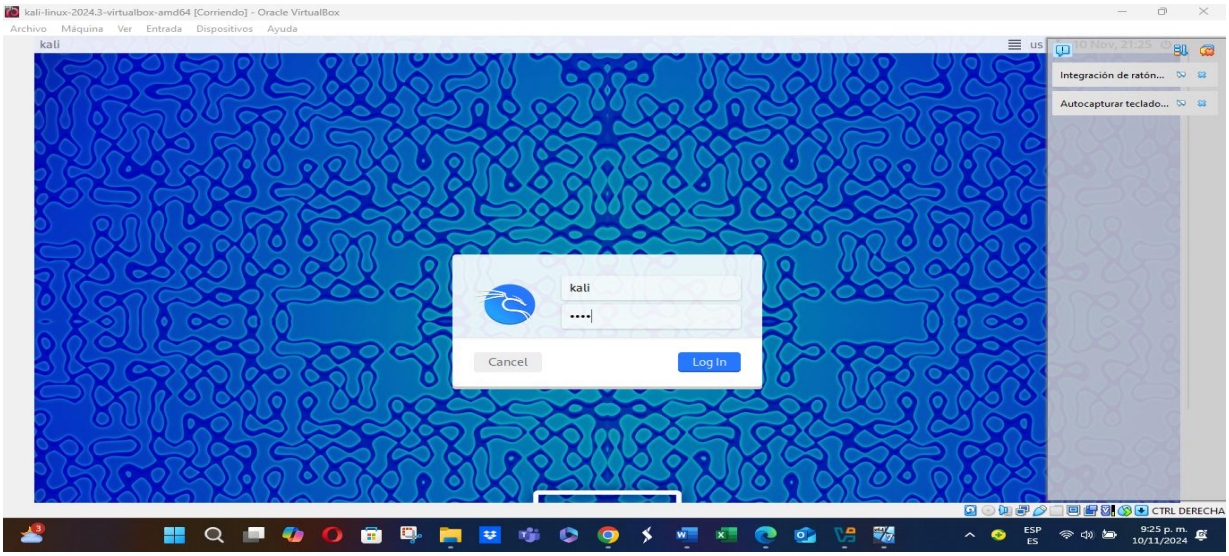

Win7-SE2020-X64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Rejeto_123456
Organizar Abrir Compartir con Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Grupo en el hogar
Equipo
Disco local (C:)
Red
Nombre Fecha de modifica... Tipo Tamaño
DarkComet_123456 28/11/2020 10:49 a... zip Archive 14.290 KB
hfs 16/02/2014 07:58 a... Aplicación 743 KB
Option...
pako.java 2 KB File JAVA
pako.tgz 329 KB File TGZ
pds ultima prima dello storico.zip 1.035 KB Cartella compr
phppgadmin.tgz 602 KB File TGZ
progettomaxx.tar.gz 35 KB File GZ
shirt.mpg
I want to give this file away.zip
Open
Search...
Add to HFS
Browse with PaintShop Pro 9
View with EncSpot
Do you want HFS in your shell context menu?
Yes
No
hfs Fecha de modifica... 16/02/2014 07:58 a.m. Fecha de creación: 28/11/2020 10:49 a.m.
Aplicación Tamaño: 742 KB
Integración de ratón...
Autocapturar teclado...
CTRL DERECHA

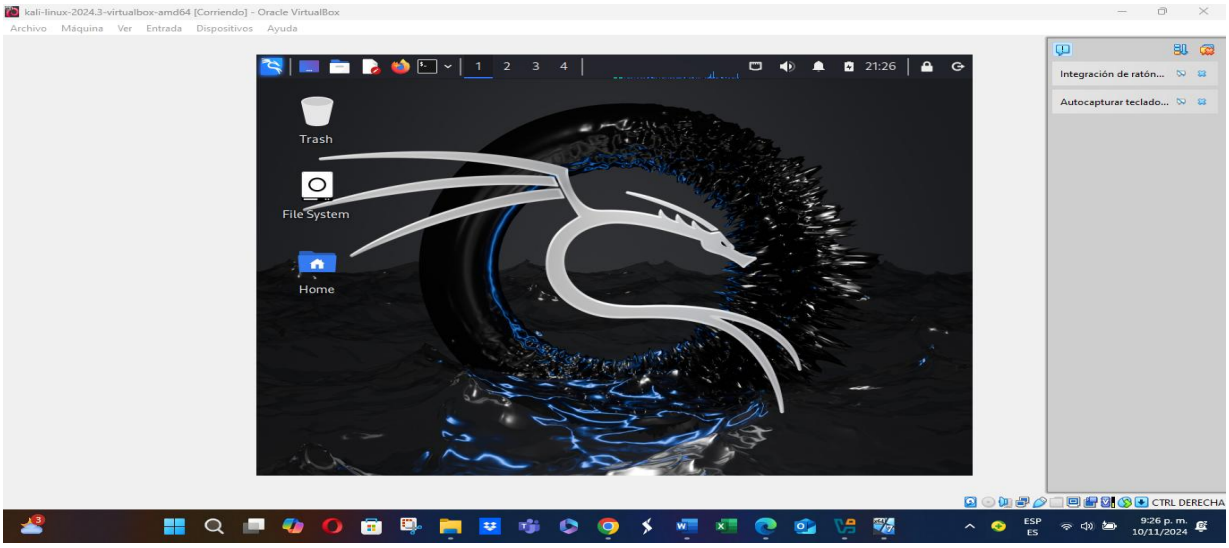

Panel de control
Equipo
Rejeto_123456
Papelera de reciclaje
Red
Rejeto_123456
Administrador: C:\Windows\system32\cmd.exe
Dirección IPv4.
Máscara de subred
Puerta de enlace
Adaptador de túnel
Estado de los medios
Sufijo DNS específico
C:\Users\usuario>pi
Haciendo ping a 192.
Respuesta desde 192.
Respuesta desde 192.
Respuesta desde 192.
Respuesta desde 192.
Estadísticas de ping
Paquetes: enviados
(0% perdidos),
Tiempos aproximados
Mínimo = 0ms, Má
C:\Users\usuario>
Todos los elementos de Panel de control ▸ Firewall de Windows
Buscar en el Panel de control
Ventana principal del Panel de control
Permitir un programa o una característica a través de Firewall de Windows
Cambiar la configuración de notificaciones
Activar o desactivar Firewall de Windows
Restaurar valores predeterminados
Configuración avanzada
Solución de problemas de red
Ayude a proteger su equipo con Firewall de Windows
Firewall de Windows ayuda a impedir que hackers o software malintencionado obtengan acceso al equipo a través de Internet o de una red.
¿Cómo me ayuda un firewall a proteger mi equipo?
¿Qué son las ubicaciones de red?
Actualizar configuración de firewall
Firewall de Windows no está usando la configuración recomendada para proteger el equipo.
Usar la configuración recomendada
¿Cuál es la configuración recomendada?
Redes domésticas o de trabajo (privadas) No conectado
Redes públicas Conectado
Redes en lugares públicos como aeropuertos o cafeterías
Estado de Firewall de Windows: Desactivado
Conexiones entrantes: Bloquear todas las conexiones a los programas que no estén en la lista de programas permitidos
Redes públicas activas: Red 3
Estado de notificación: Notificarme cuando Firewall de Windows bloquee un nuevo programa
Vea también
Centro de actividades
Centro de redes y recursos compartidos
11:01 p.m.
10/11/2024

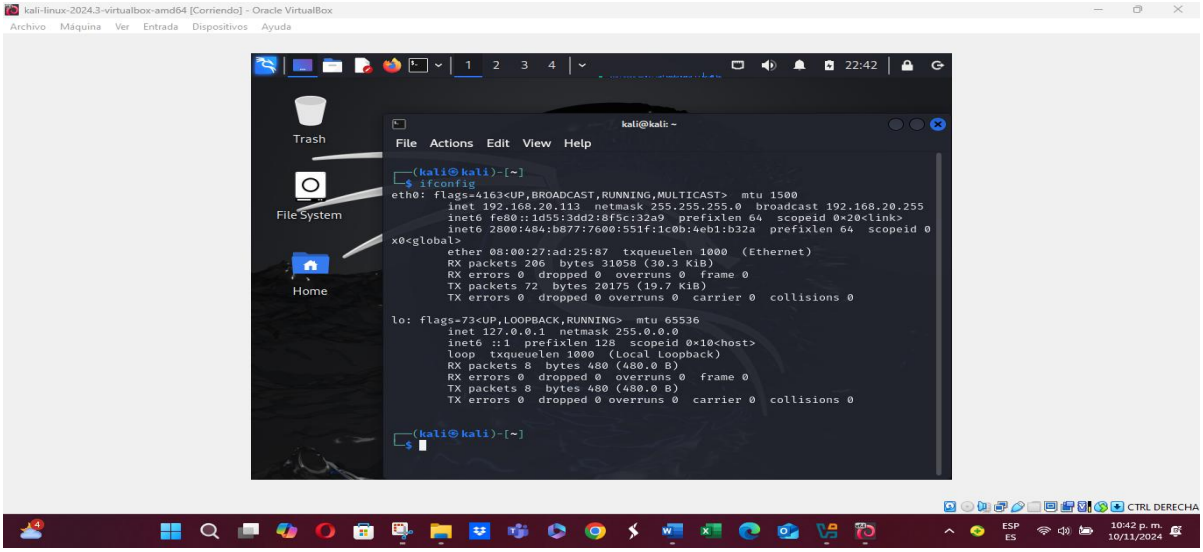

Win7-SE2020-X64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Rejeto_123456
Organizar Abrir Compartir con Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Grupo en el hogar
Equipo
Disco local (C:)
Red
Nombre Fecha de modifica... Tipo Tamaño
DarkComet_123456 28/11/2020 10:49 a... zip Archive 14.290 KB
hfs 16/02/2014 07:58 a... Aplicación 743 KB
HFS ~ HTTP File Server 2.3 Build 288
Menu Port: 80 You are in Easy mode
Open in browser http://192.168.20.114/
Copy to clipboard
Virtual File System
Log
IP address File Status Speed Time... Progress
hfs
Aplicación
Integración de ratón...
Autocapturar teclado...
CTRL DERECHA

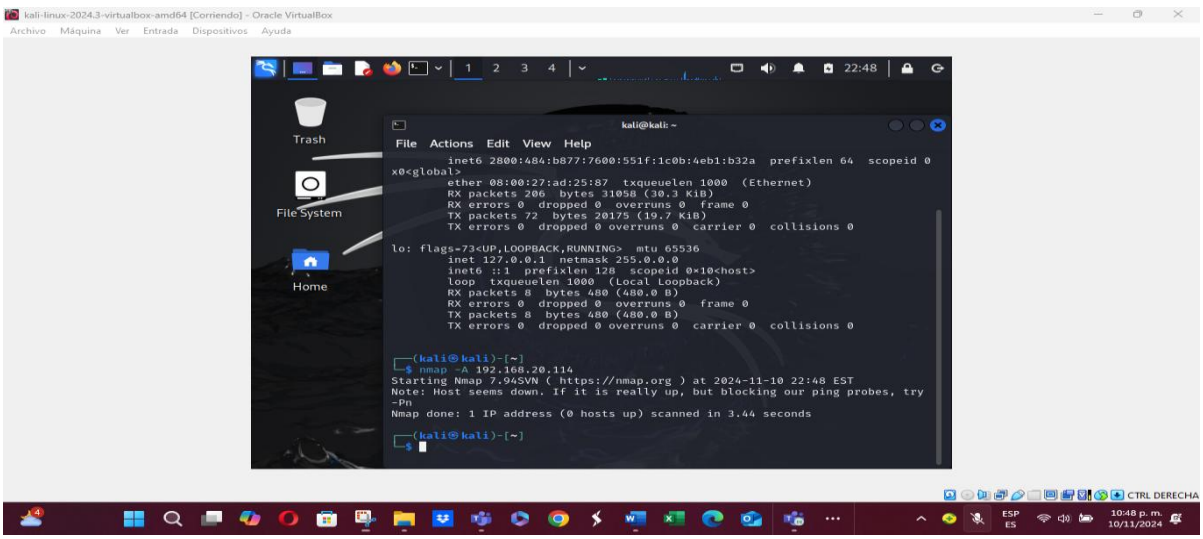

Win7-SE2020-X64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Panel de control
Equipo
Rejeto 123456
Papelera de reciclaje
Red
Rejeto 123456
Administrador: C:\Windows\system32\cmd.exe
Dirección IPv4. . . . . : 192.168.20.114
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::1682:5bff:fe00:20%11
192.168.20.1
Adaptador de túnel isatap.{5BE8BED2-9B04-4799-BEB3-D289D73C2460}:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
C:\Users\usuario>ping 192.168.20.113
Haciendo ping a 192.168.20.113 con 32 bytes de datos:
Respuesta desde 192.168.20.113: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.20.113: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.20.113: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.20.113: bytes=32 tiempo<1m TTL=64
Estadísticas de ping para 192.168.20.113:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\Users\usuario>
Integración de ratón...
Autocapturar teclado...
CTRL DERECHA

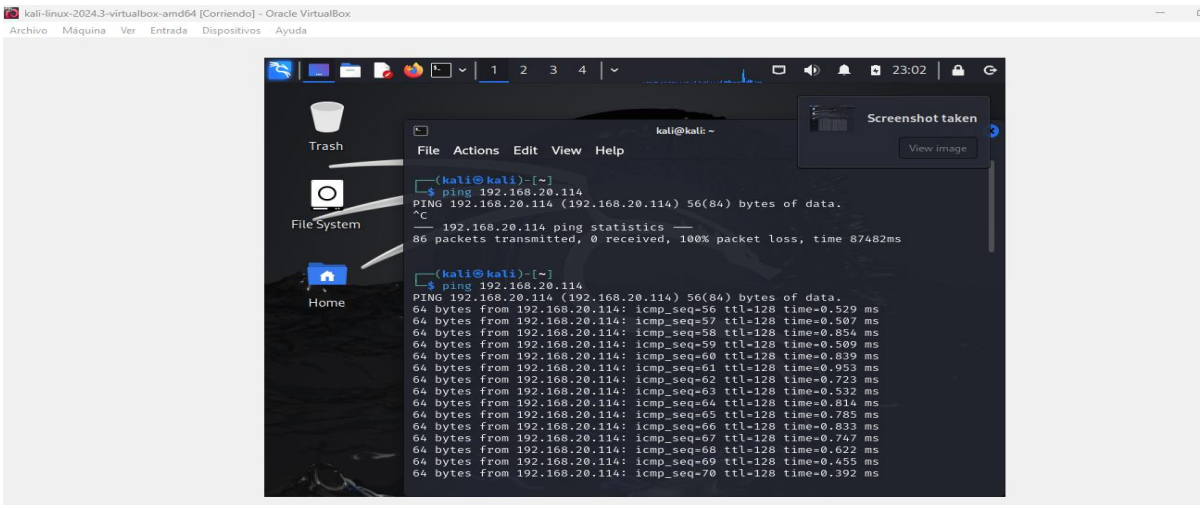

Oracle VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
ESI Seg. DB
Win7-SE2020-X64
Corriendo
kali-linux-2024.3-virtualbox-amd64
Corriendo
Nueva
Añadir
Configuración
Descartar
Mostrar
General
Nombre: kali-linux-2024.3-virtualbox-amd64
Sistema operativo: Debian (64-bit)
Sistema
Memoria base: 2048 MB
Procesadores: 2
Orden de arranque: Disco duro, Óptica
Aceleración: Paginación anidada, PAE/NX, Paravirtualización KVM
Previsualización
KALI
Pantalla
Memoria de vídeo: 128 MB
Controlador gráfico: VMSVGA
Servidor de escritorio remoto: Inhabilitado
Grabación: Inhabilitado
Almacenamiento
Controlador: IDE
Dispositivo IDE secundario 0: [Unidad óptica] Vacío
Controlador: SATA
Puerto SATA 0: kali-linux-2024.3-virtualbox-amd64.vdi (Normal, 80,09 GB)
Audio
Controlador de anfitrión: Windows DirectSound
Controlador: ICH AC97
Red
Adaptador 1: Intel PRO/1000 MT Desktop (Adaptador puente, «Realtek RTL8723DE 802.11b/g/n PCIe Adapter»)
USB
Controlador USB: OHCI
Filtros de dispositivos: 0 (0 activo)
Carpetas compartidas
Ninguno
ESP ES
9:25 p. m.
10/11/2024

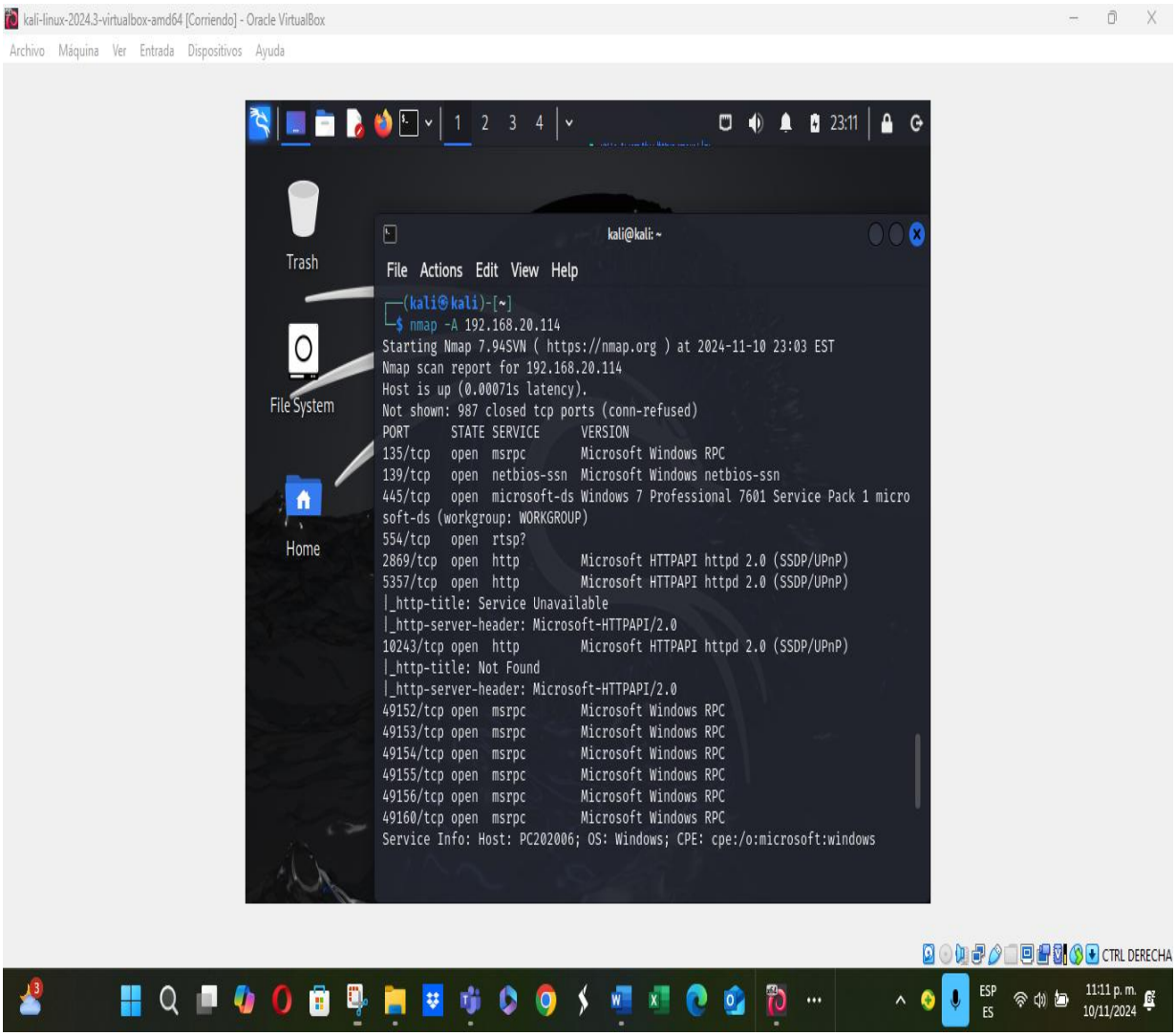

kali-linux-2024.3-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
kali
us
kali
Cancel
Log In
Integración de ratón...
Autocapturar teclado...
CTRL DERECHA
ESP ES
9:25 p. m.
10/11/2024


kali-linux-2024.3-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
21:26
Trash
File System
Home
Integración de ratón...
Autocapturar teclado...
CTRL DERECHA
ESP ES
9:26 p. m. 10/11/2024


kali-linux-2024.3-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
22:42
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.20.113 netmask 255.255.255.0 broadcast 192.168.20.255
inet6 fe80::1d55:3dd2:8f5c:32a9 prefixlen 64 scopeid 0x20<link>
inet6 2800:484:b877:7600:551f:1c0b:4eb1:b32a prefixlen 64 scopeid 0
x0<global>
ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
RX packets 206 bytes 31058 (30.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 72 bytes 20175 (19.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$
CTRL DERECHA
ESP ES
10:42 p. m. 10/11/2024


kali-linux-2024.3-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
22:48
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
inet6 2800:484:b877:7600:551f:1c0b:4eb1:b32a prefixlen 64 scopeid 0
x0<global>
ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
RX packets 206 bytes 31058 (30.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 72 bytes 20175 (19.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$ nmap -A 192.168.20.114
Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-10 22:48 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.44 seconds
(kali㉿kali)-[~]
$
CTRL DERECHA
ESP ES
10:48 p. m. 10/11/2024



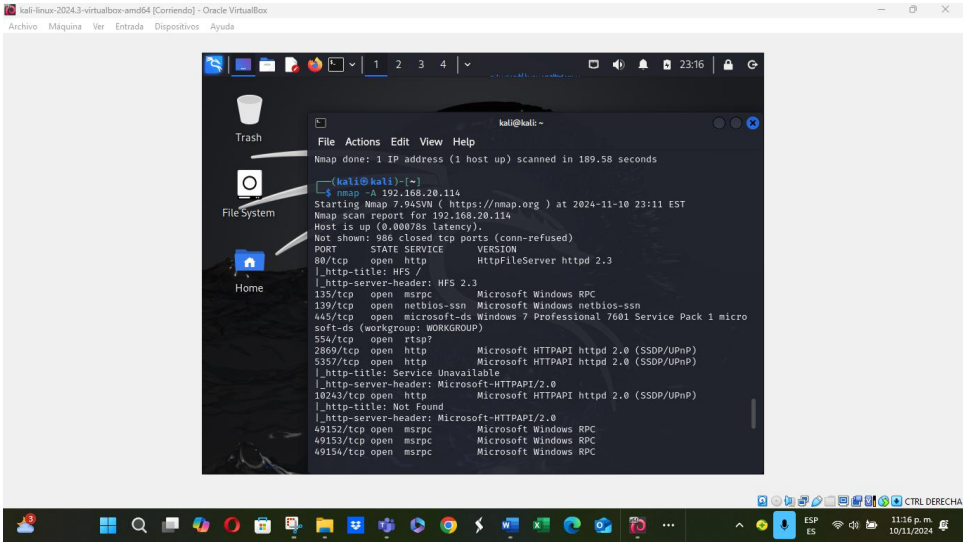


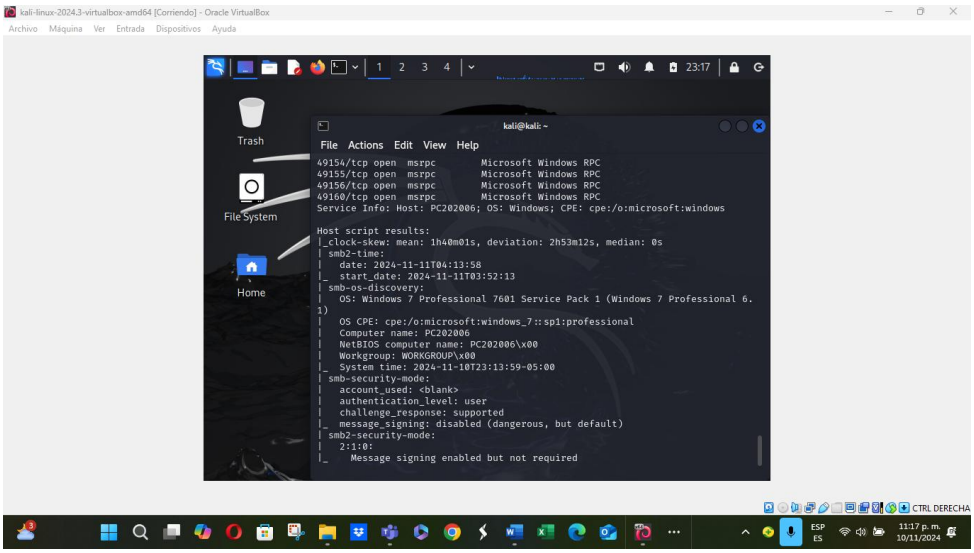
Fuente. Autoría propia

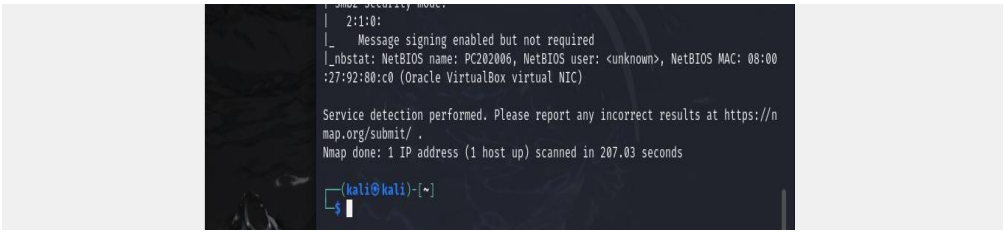
Se utiliza la terminal de Kali Linux en donde ejecuta el comando nmap -A 192.168.20.114, en donde nos permite visualizar, el sistema operativo, los servicios a través de los puertos, los cuales puedo listar para poder ver que puertos tengo abiertos de la máquina objetivo en este caso se evidencia el puerto 80 en donde se ve la vulnerabilidad que está en el servicio de la máquina de Windows 7, para poder armar el vector de ataque.

Figura 27

Comando Nmap -A 192.168.20.114





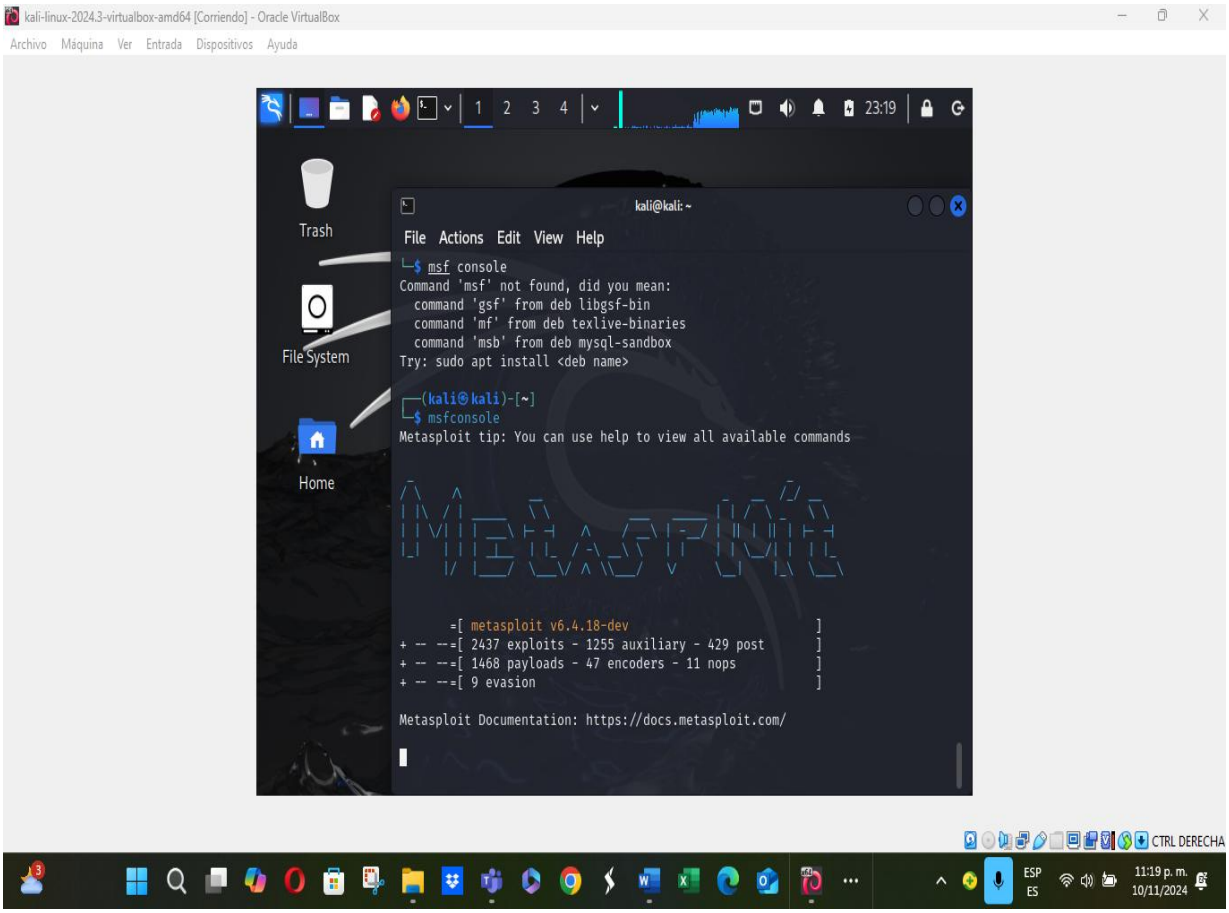


Fuente. Autoría propia

Se realiza la instalación de metasploit mediante el comando msfconsole, el cual me permite realizar la explotación de la vulnerabilidad de Windows 7.

Figura 28

Instalación de Metasploit

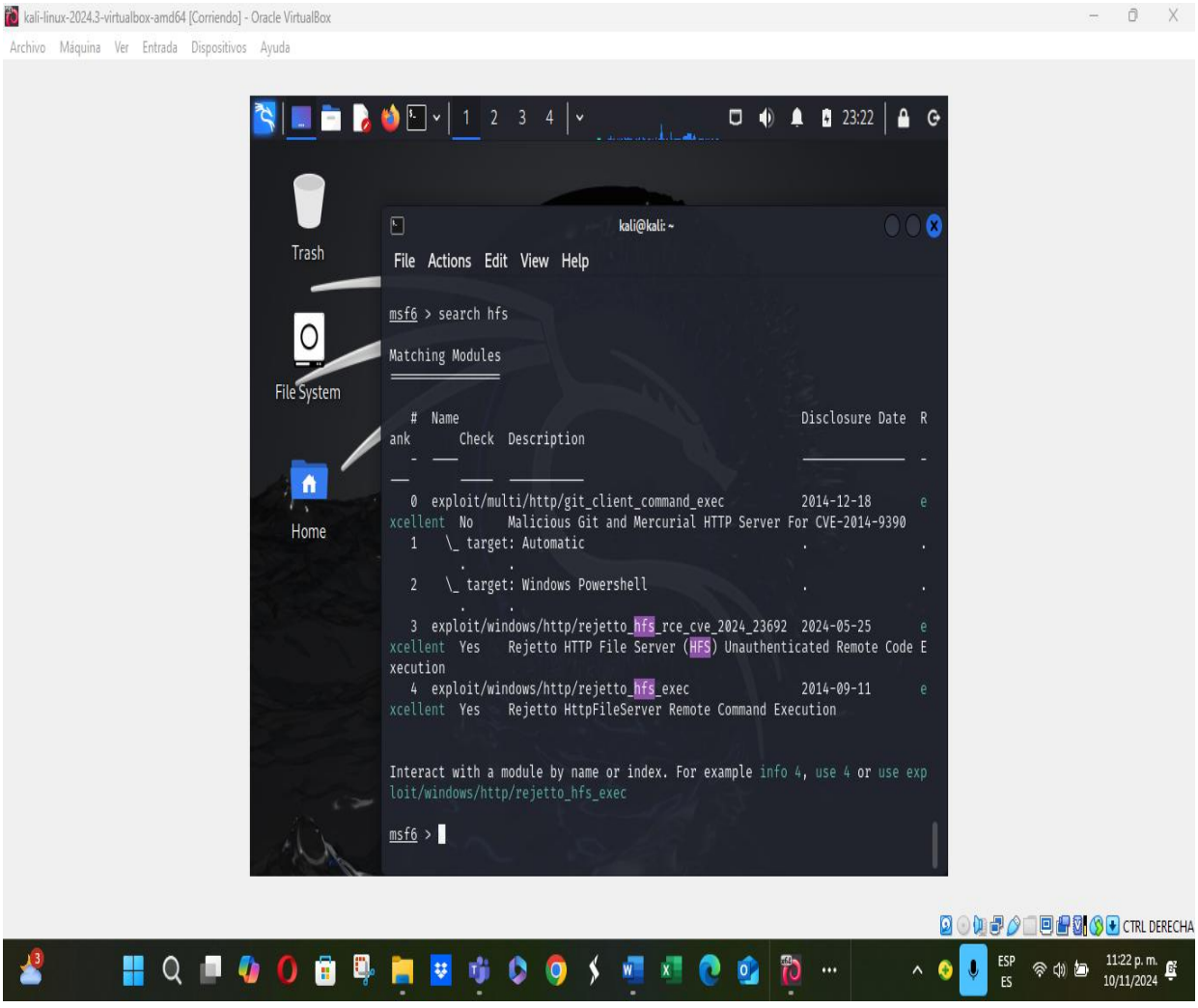


Fuente. Autoría propia

Se ejecuta el comando search hfs en donde nos visualiza los módulos de los exploit que existen que contengan la palabra hfs, el cual se encuentra el exploit para Windows, el cual se evidencia la empresa Rejetto que desarrollo el software, lo cual para la versión me permite hacer una sesión de comandos de manera remota.

Figura 29

Comando search hfs

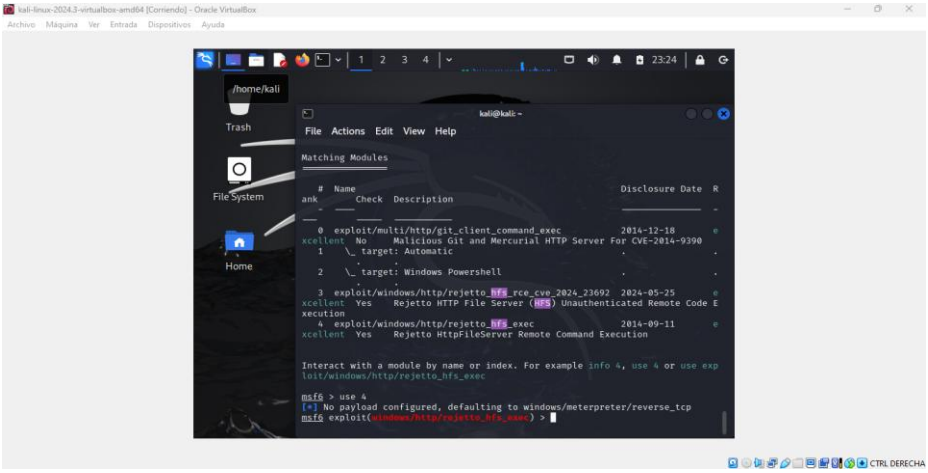


Fuente. Autoría propia

Se ejecuta el comando use 4 me selecciona el exploit donde esta la vulnerabilidad, en donde ir acompañado de un Payload para realizar la explotación, el cual en el Payload devuelve una sesión remota con la conexión de la máquina objetivo a la máquina atacante

Figura 30

Comando Payload para Realizar la Explotación

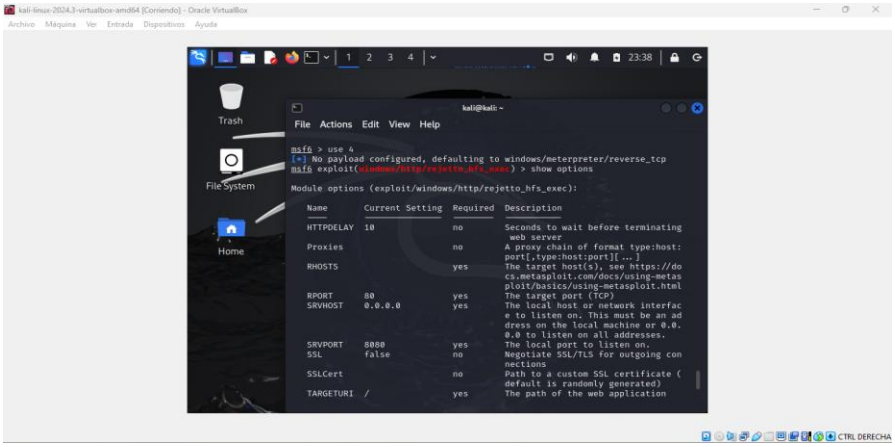


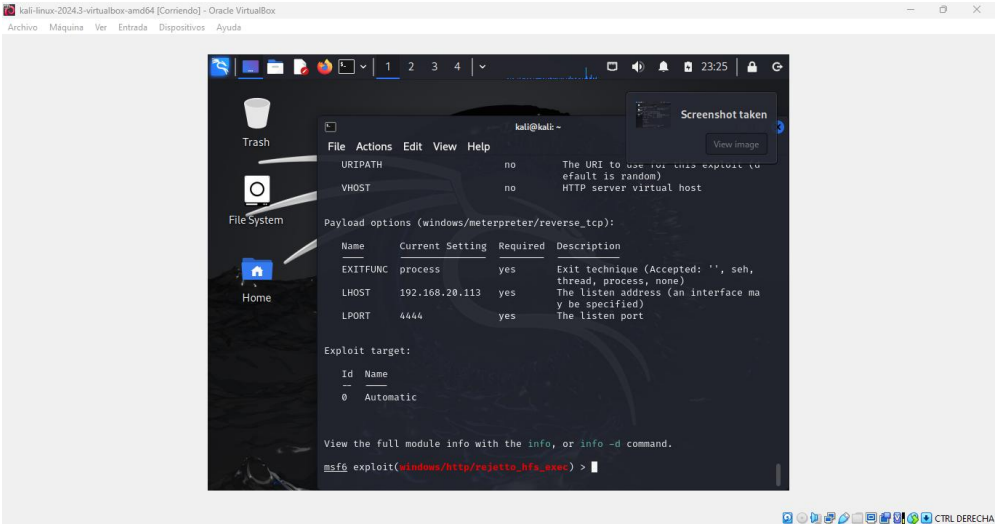
Fuente. Autoría propia

Se ejecutó el comando show options donde lista todas las opciones del exploit y en la parte inferior se evidencia todas las opciones de Payload

Figura *31*

Comando Show Options



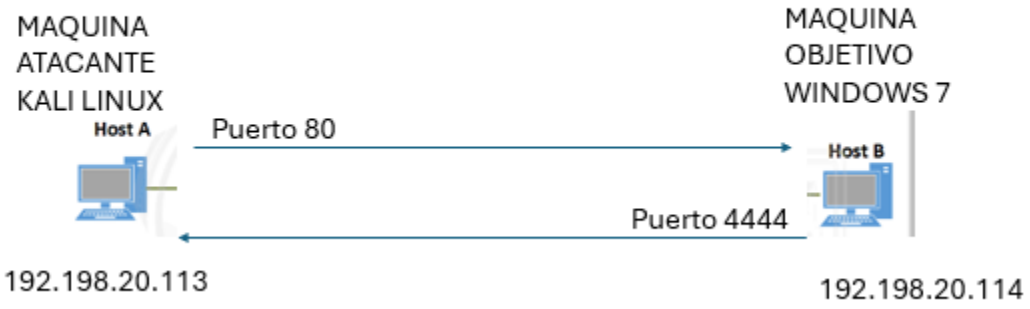


Fuente. Autoría propia

Informe de la Explotación de Vulnerabilidades en el Escenario Propuesto

Figura 32

Explotación de Vulnerabilidades

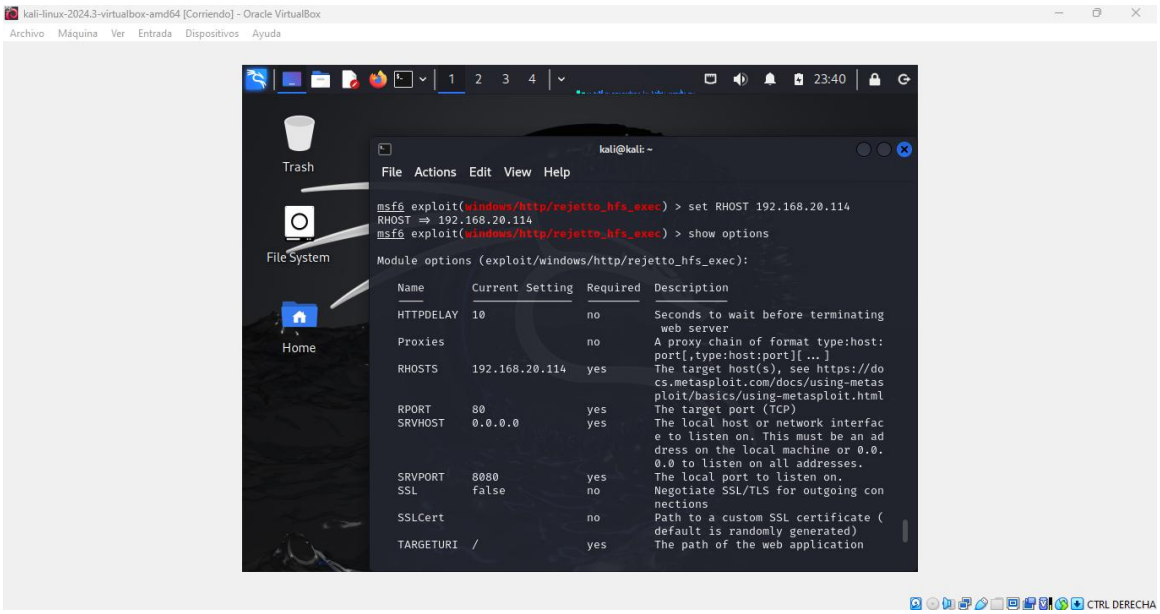


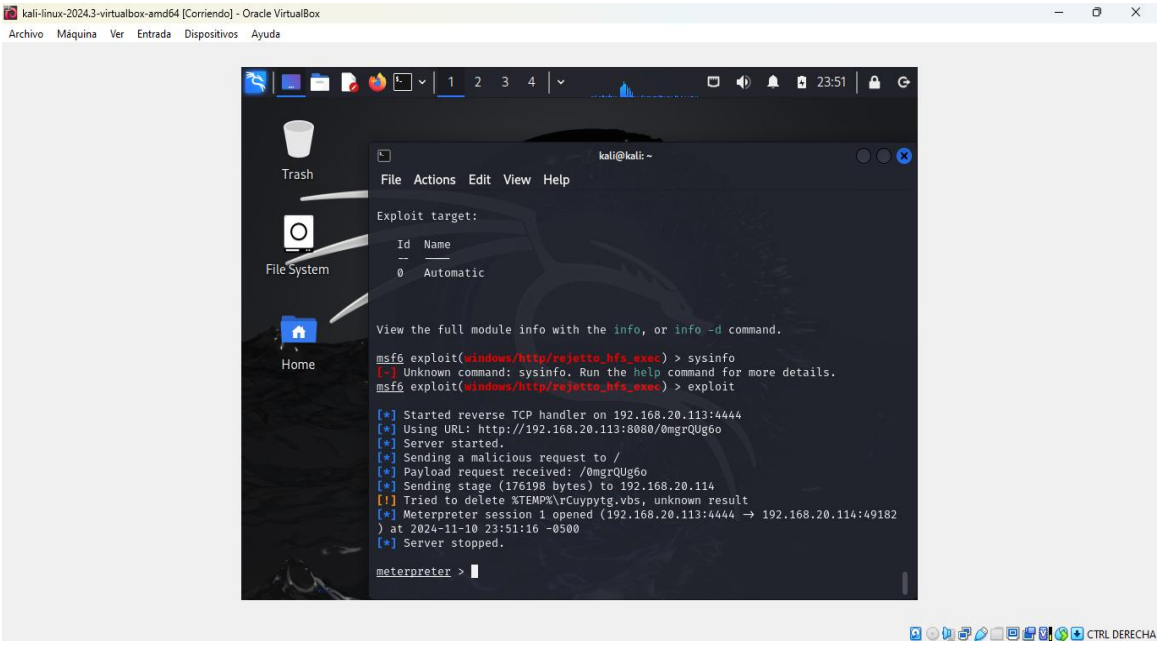
Fuente. Autoría propia

Se ejecuta set RHOST 192.168.20.114 que es la máquina objetivo remota, por lo que se evidencia el Ip de la máquina remota

Figura 33

Comando Set RHOST 192.168.20.114



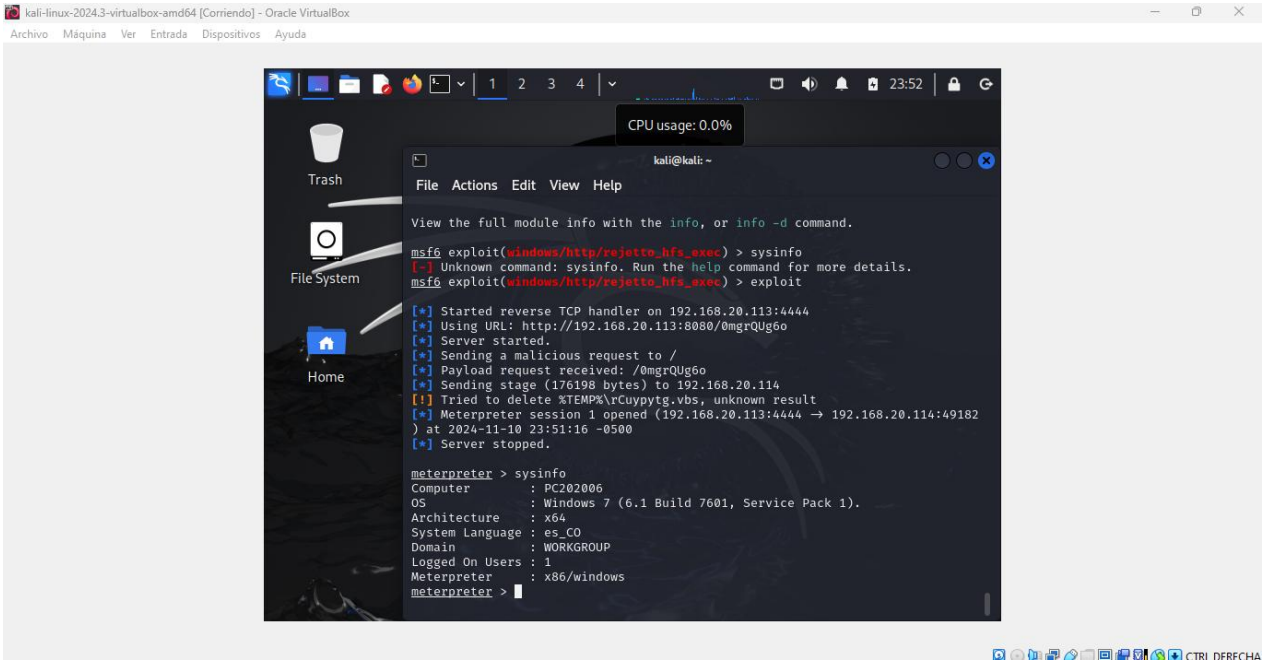


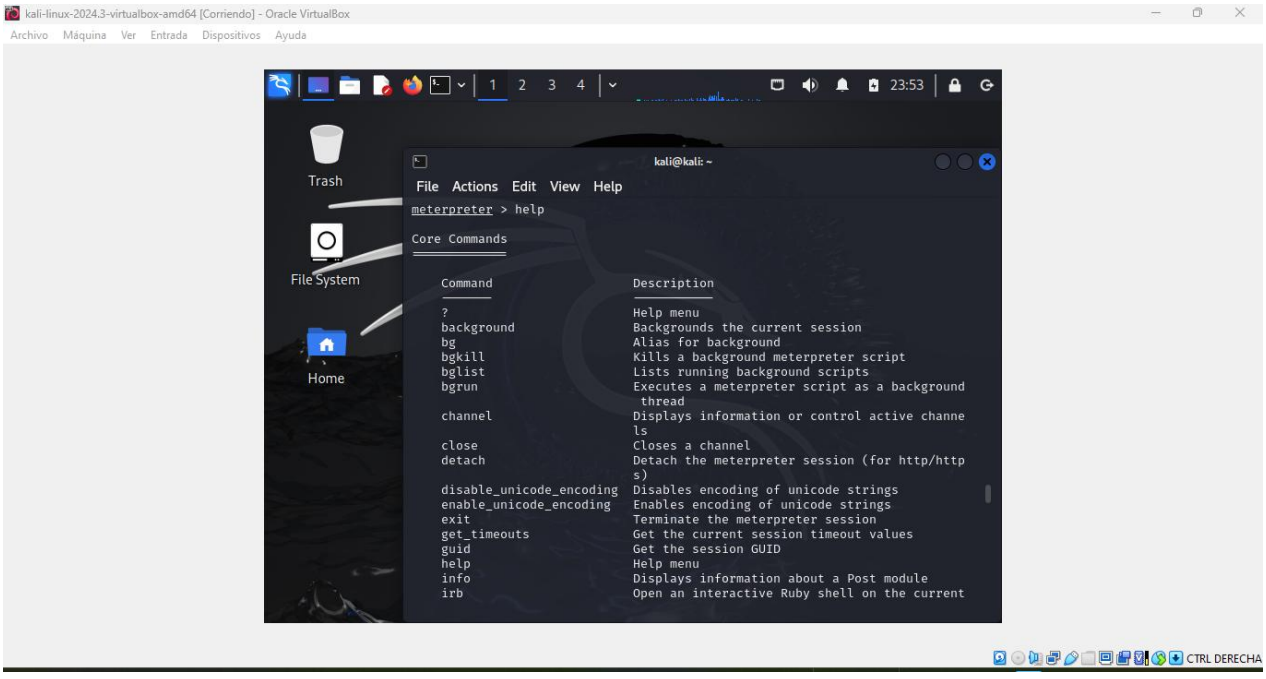
Fuente. Autoría propia

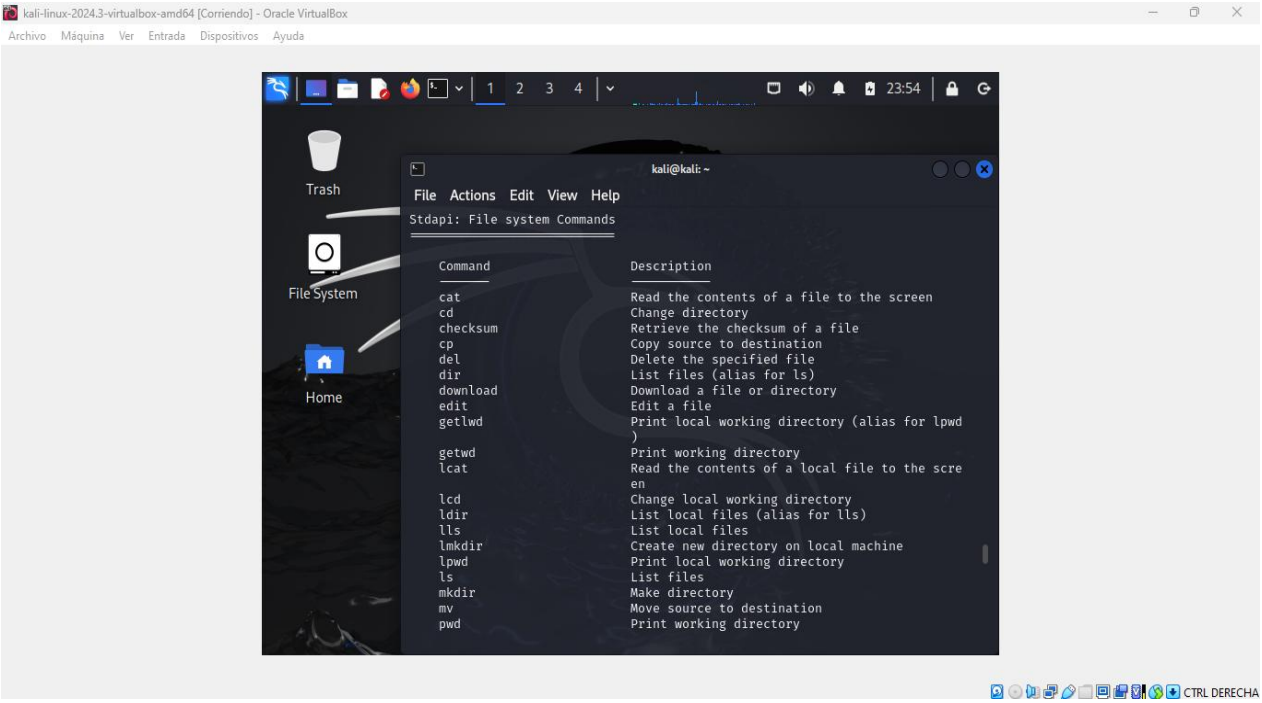
Se ejecuta el comando sysinfo en donde se visualiza la información de la máquina objetivo y sus características

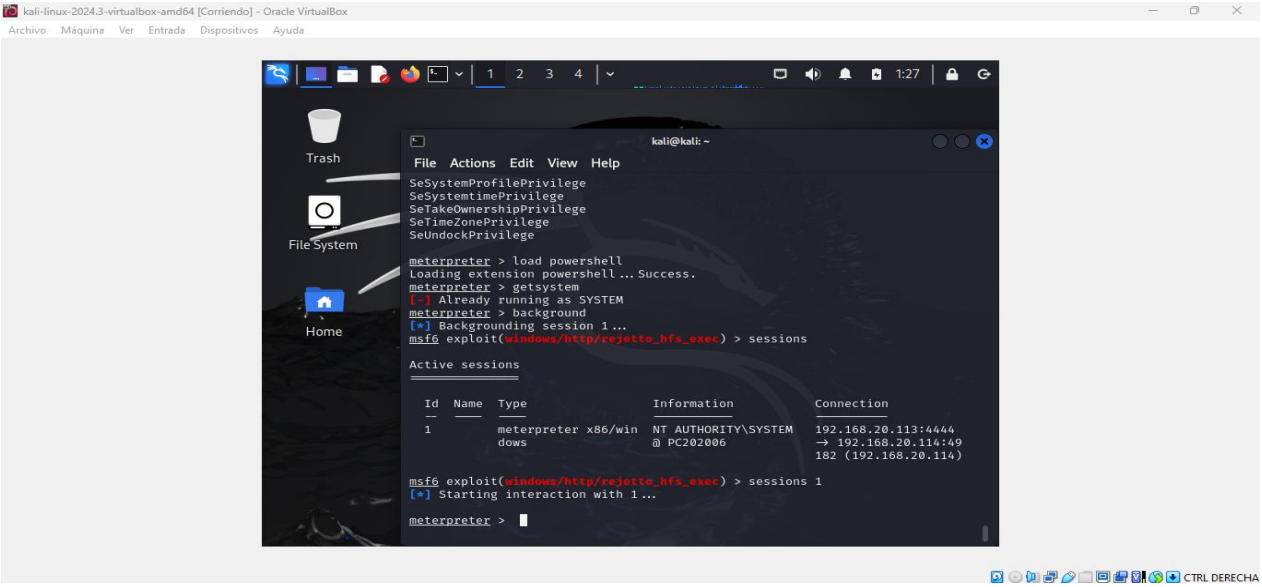
Figura 34

Comando Sysinfo







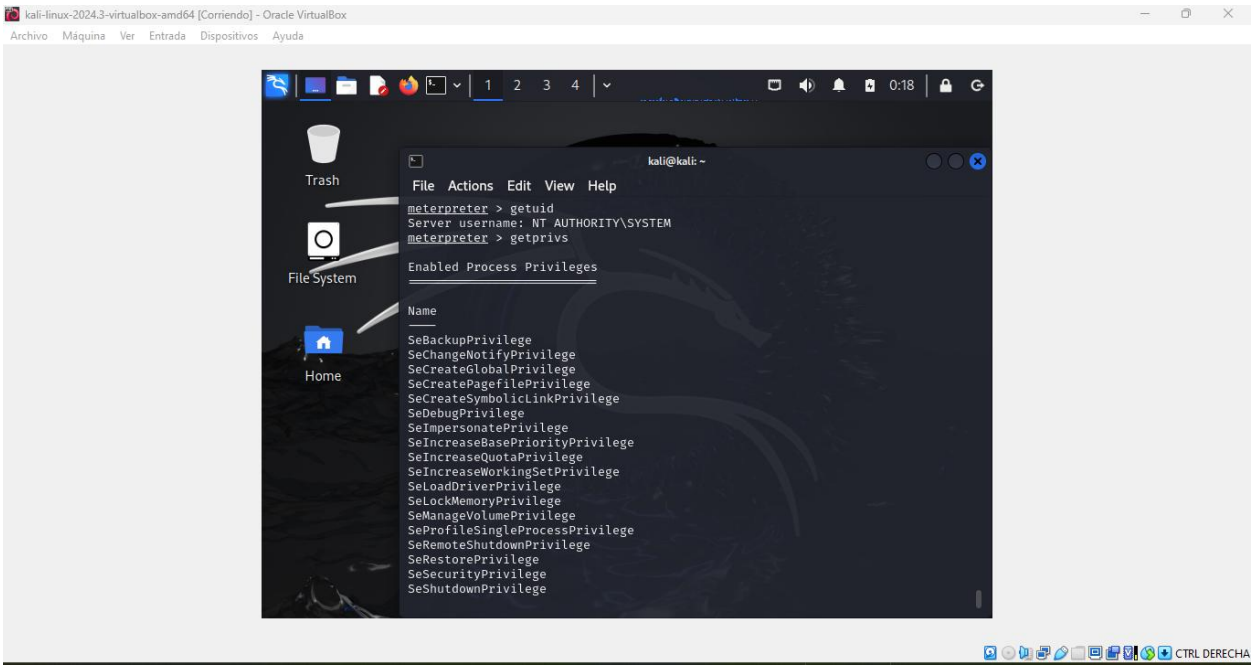


Fuente. Autoría propia

Se ejecuta el comando getvid visualiza el nombre del administrador y el comando getprivs muestra los privilegios, el cual permite ingresar como administrador y poder eliminar la vulnerabilidad sin dejar evidencias de lo ejecutado.

Figura 35

Comando getvid



Fuente. Autoría propia

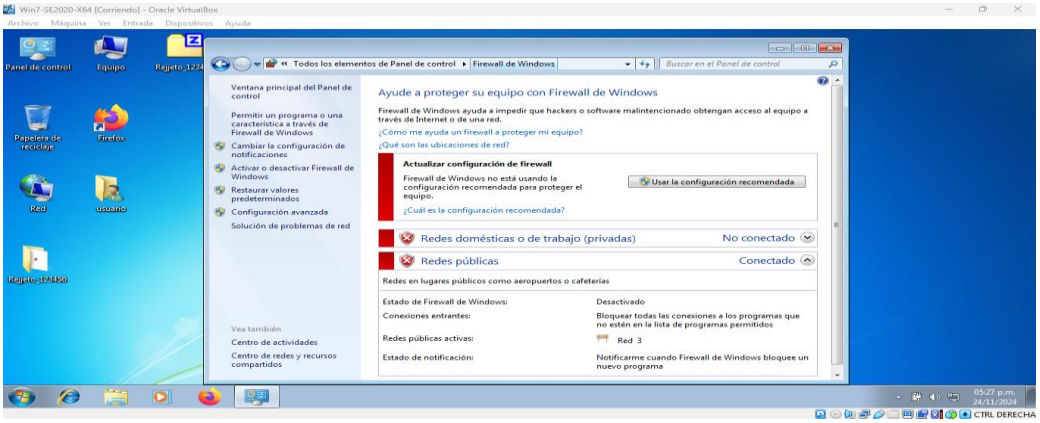
Análisis con Acciones Necesarias Para Contener un Ataque en Tiempo Real

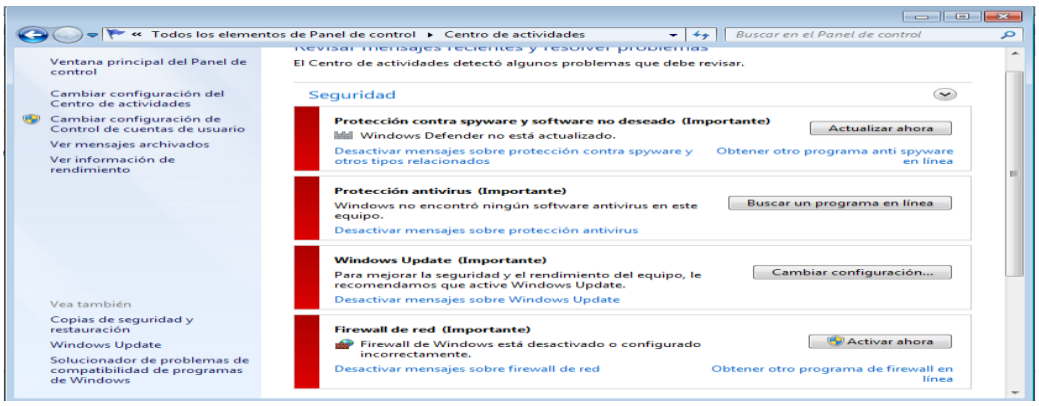
Se solicitó a los integrantes de Blue Team realicen un análisis del ataque informático que está presentando en uno de los equipos de computo y red de la organización CyberFort Technologies. Lo primero que se realizaría es un plan de contingencia, que nos permita identificar, monitorear, detectar, responder, recuperar y proteger los activos de la organización y en donde se analicé la problemática de seguridad informática que se está presentando al interior de la organización para entrar a evaluar y validar el grado de riesgo del incidente a identificar y los daños que está ocasionando, con el fin de contener su propagación a los demás los sistemas informáticos, mediante herramientas que permitan la mitigación del ataque informático, logrando salvaguardar la integridad, confidencialidad y disponibilidad de la organización.

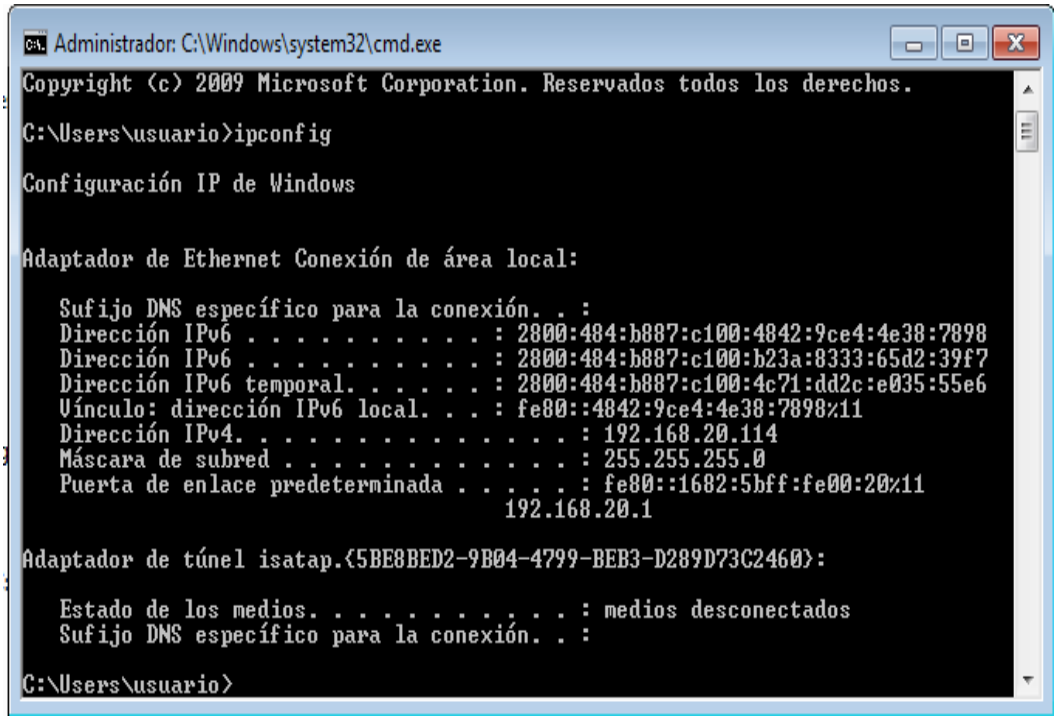
Una vez aplicado el plan de contingencia en donde se realizó un análisis exhaustivo a los activos de la organización, se logró identificar el equipo de cómputo es donde se presentó el incidente, el cual tiene instalado el sistema operativo Windows 7, al ingresar a Firewall de Windows se evidencia que se encuentra desactivado, esto quiere decir que esta sin protección el equipo, el cual le permitió al atacante ingresar fácilmente a realizar el ataque informático en tiempo real. Por lo que se evidencia en la siguiente imagen:

Figura 36

Firewall de Windows se Evidencia que se Encuentra Desactivado







Fuente. Autoría propia

Informe de Acciones de Hardenización a Implementar Para Evitar que Sucedan Ataques de Seguridad Informática

Se evidenciaron falencias encontradas en la seguridad de la información, se recomienda a la organización CyberFort tomar acciones de hardenización de manera inmediata, lo cual permite el endurecimiento a la seguridad informática dentro de la organización, con el propósito de reducir al máximo las vulnerabilidades que el atacante realice, se recomienda incluir dentro de sus políticas de seguridad y privacidad de la información los siguiente información y que sea socializada al personal de la organización, de no consultar ni descargar archivos de páginas web no oficiales, tener contraseñas robustas, tener activado el programa de antivirus en los equipos de cómputo, no abrir archivos desconocidos, tener cuidado con los correos electrónicos: (Smartekh, 2012)

Tabla 5

Acciones de Hardenización

Actividades	Descripción
Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de los equipos.	Entre otras tareas, sobresalen la actualización de firmware, la configuración de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la desactivación del inicio de sistema para cualquier unidad distinta al disco duro principal, y en situaciones de servidores, la desactivación de dispositivos ópticos, USB o equivalentes, para prevenir la infiltración de malware desde un dispositivo de almacenamiento externo.
Instalación segura del sistema operativo.	Esto conlleva, entre otros aspectos, la consideración de al menos dos particiones principales (1 para el sistema operativo en sí mismo y otra para carpetas y archivos de relevancia), la utilización de un sistema de archivos con características de seguridad, y la idea de instalación mínima, es decir, eludiendo la instalación de cualquier elemento de sistema que no sea imprescindible para el correcto funcionamiento del sistema.
Activación y/o configuración adecuada de servicios de actualizaciones automáticas	Para garantizar que el equipo cuente con todos los actualizados de seguridad que proporciona el proveedor. Si se ubica dentro de una entidad, es apropiado instalar un servidor de actualizaciones, el cual debe evaluar en un ambiente de laboratorio el efecto de la implementación de actualizaciones antes de su implementación en la producción.
Instalación, configuración y mantención de programas de seguridad	Tales como, Antispyware, Antivirus, y un filtro Antispam según las necesidades del sistema.
Configuración de la política local del sistema,	Tomando en cuenta diversos aspectos importantes: Política de contraseñas sólida, con claves válidas, almacenamiento de datos históricos (para evitar el uso de contraseñas cíclicas), bloqueos de cuentas por intentos incorrectos y requerimientos de complejidad de contraseñas. El renombre y la desactivación subsiguiente de las cuentas estándar del sistema, como la de administrador e invitado. Correcta asignación de derechos de usuario, con el objetivo de

Actividades	Descripción
	disminuir las oportunidades de incremento de privilegios, y siempre procurando reducir al mínimo los privilegios y/o derechos de los usuarios en activo.
Configuración de opciones de seguridad generales,	Tales como las vinculadas a rutas de acceso compartido, desactivación del sistema, inicio y finalización de sesión y alternativas de seguridad en la red.
Restricciones de software	Fundamentado, en la medida de lo posible, en la utilización de listas blancas de software permitido en lugar de listas negras de este.
Activación de auditorías de sistema	Esenciales para llevar un seguimiento de ciertos intentos de ataque distintivos, como la interpretación de contraseñas.
Configuración de servicios de sistema	En este momento, es imprescindible procurar siempre desactivar todos los servicios que no proporcionen la funcionalidad requerida para el correcto funcionamiento del sistema. Por ejemplo, si su dispositivo no cuenta con tarjetas de red inalámbrica, debería estar desactivado el servicio de redes inalámbricas.
Configuración de los protocolos de Red.	Es aconsejable, a la mayor capacidad, emplear sistemas de traducción de direcciones (NAT) para orientar los equipos internos de una entidad. Habilitar todos los protocolos de red superfluos en el sistema y restringir su utilización al mínimo. TCP/IP es un protocolo que no se desarrolló con el objetivo de proteger, por lo que es esencial restringir su utilización al indispensable.
Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema.	Conforme sea viable, eliminar de manera explícita cualquier autorización de archivo a las cuentas de acceso anónimos o sin contraseña. Es crucial establecer adecuadamente los permisos a nivel de carpetas y archivos para prevenir el acceso indebido al contenido de estos.
Configuración de opciones de seguridad de los distintos programas.	Tales como clientes de email, exploradores web y en general cualquier tipo de software que interactúe con la red.
Configuración de acceso remoto.	Si no es imprescindible, sería conveniente desactivar el acceso remoto. No obstante, cuando se requiere un control remoto de la máquina, es esencial configurarlo correctamente, limitando el acceso a un número muy reducido de usuarios, limitando al mínimo las

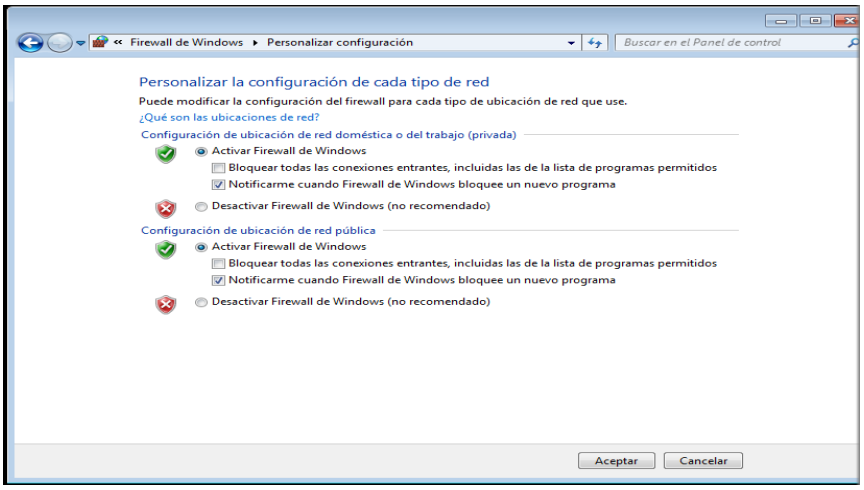
Actividades	Descripción
	conexiones simultáneas, teniendo precaución en la desconexión y cierre de sesión, y estableciendo un canal de comunicaciones cifrado para estos fines, como SSH.
Configuración adecuada de cuentas de usuario,	Intentando emplear la mayoría del tiempo en cuentas de acceso restringido y desactivando las cuentas de administrador. Se aconseja de manera absoluta utilizar la impersonificación de usuarios para llevar a cabo tareas administrativas en lugar de entrar como administradores.
Cifrado de archivos o unidades según las necesidades del sistema,	Tomando en cuenta un almacenaje externo para las claves de descodificación. Además, se debe considerar la posibilidad de emplear sistemas de cifrado para mensajería instantánea y correo electrónico.
Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema.	Como sea posible, gestionar los respaldos a través de la red o trasladar los respaldos a unidades físicas que se encuentren lejos del equipo que los produce.

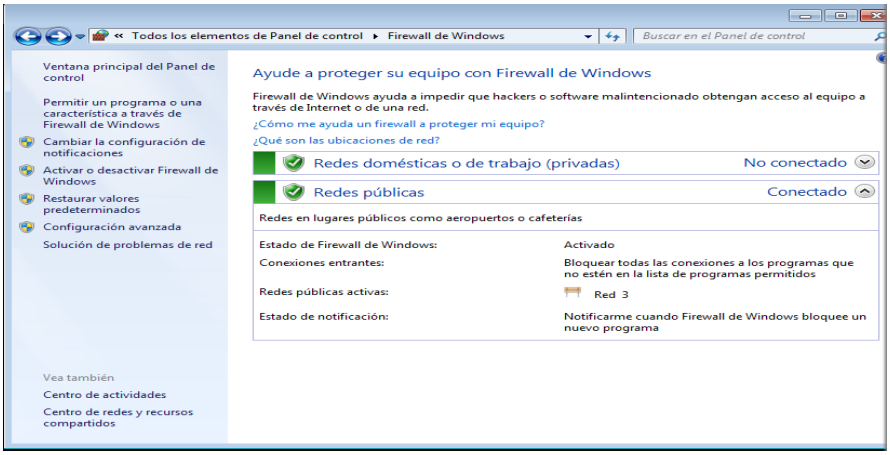
Fuente. Autoría propia

Se procedió a la activación de Firewall, con el fin de bloquear el acceso a terceros

Figura 37

Activación de Firewall



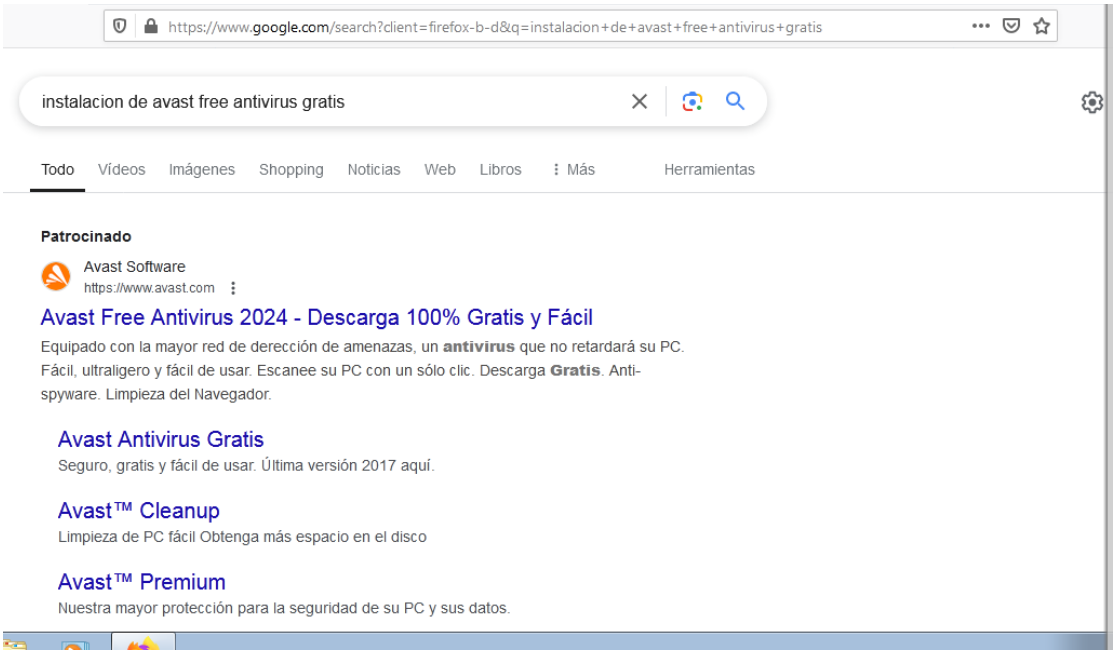


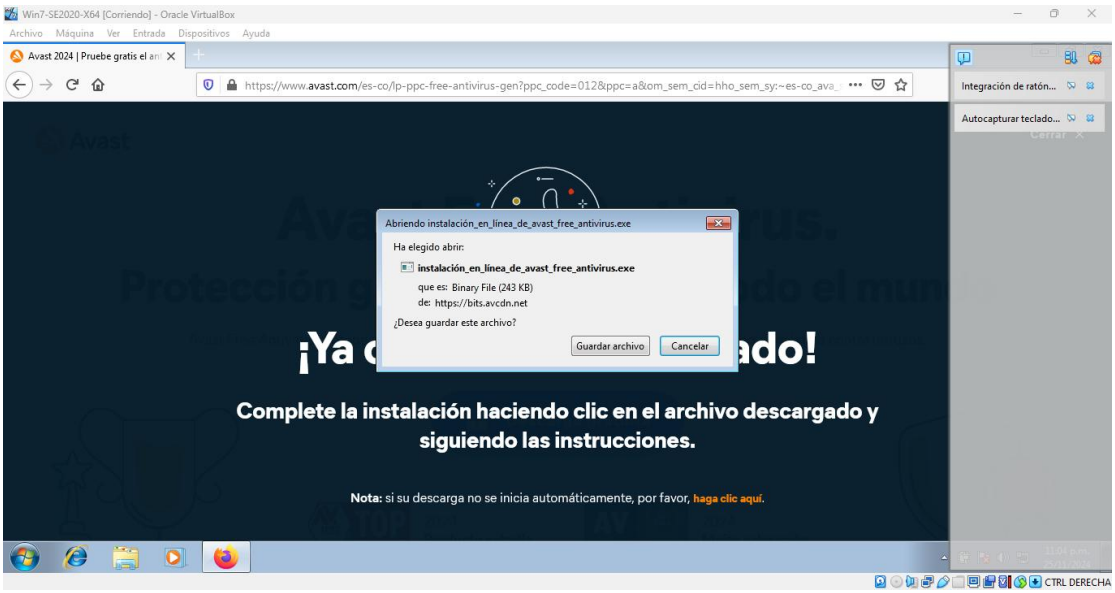
Fuente. Autoría propia

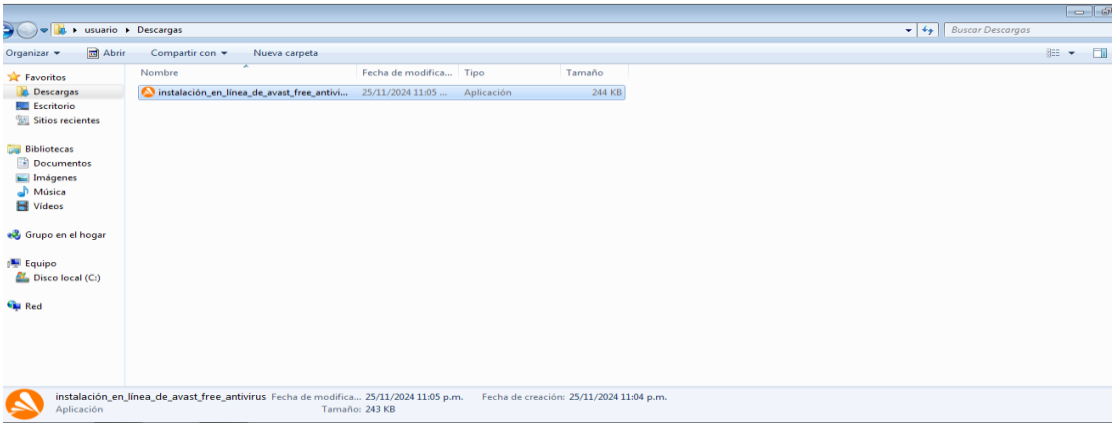
Se procedió a la descarga de Avast Free Antivirus y a su respectiva instalación, con el fin mitigar el ataque informático y de robustecer los sistemas de información que están afectando a la organización.

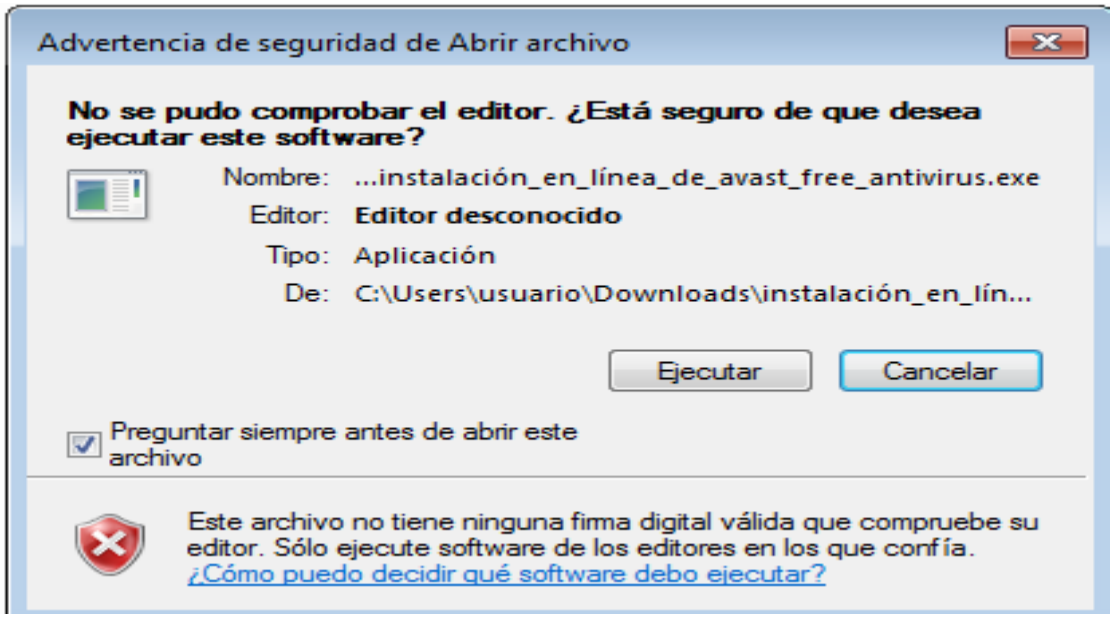
Figura 38

Descarga de Avast Free Antivirus



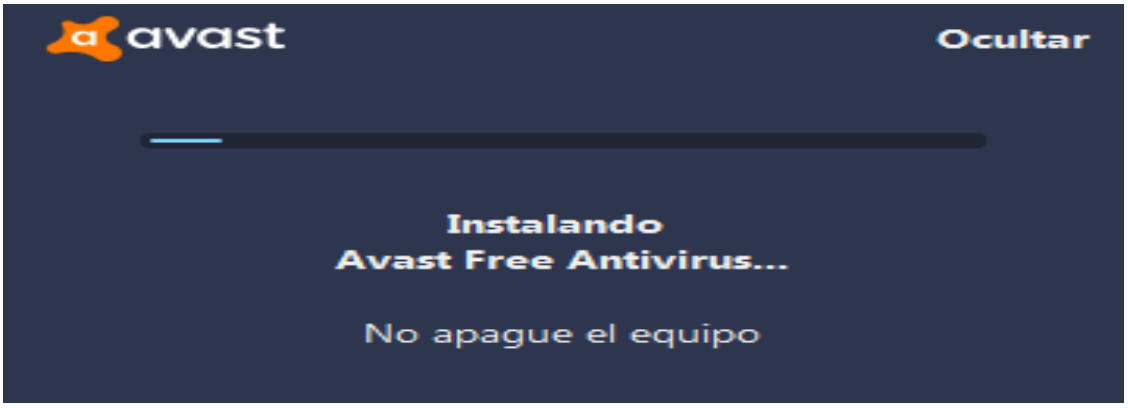

Win7-SE2020-X64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Avast 2024 | Pruebe gratis el an
https://www.avast.com/es-co/lp-ppc-free-antivirus-gen?ppc_code=012&ppc=a&om_sem_cid=hho_sem_sy:~es-co_ava
Integración de ratón...
Autocapturar teclado...
Abriendo instalación_en_línea_de_avast_free_antivirus.exe
Ha elegido abrir:
instalación_en_línea_de_avast_free_antivirus.exe
que es: Binary File (243 KB)
de: https://bits.avcdn.net
¿Desea guardar este archivo?
Guardar archivo
Cancelar
Complete la instalación haciendo clic en el archivo descargado y siguiendo las instrucciones.
Nota: si su descarga no se inicia automáticamente, por favor, haga clic aquí.
CTRL DERECHA


usuario ▸ Descargas
Buscar Descargas
Organizar
Abrir
Compartir con
Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Grupo en el hogar
Equipo
Disco local (C:)
Red
Nombre
Fecha de modifica...
Tipo
Tamaño
instalación_en_línea_de_avast_free_antivi...
25/11/2024 11:05 ...
Aplicación
244 KB
instalación_en_línea_de_avast_free_antivirus
Aplicación
Fecha de modifica... 25/11/2024 11:05 p.m.
Tamaño: 243 KB
Fecha de creación: 25/11/2024 11:04 p.m.

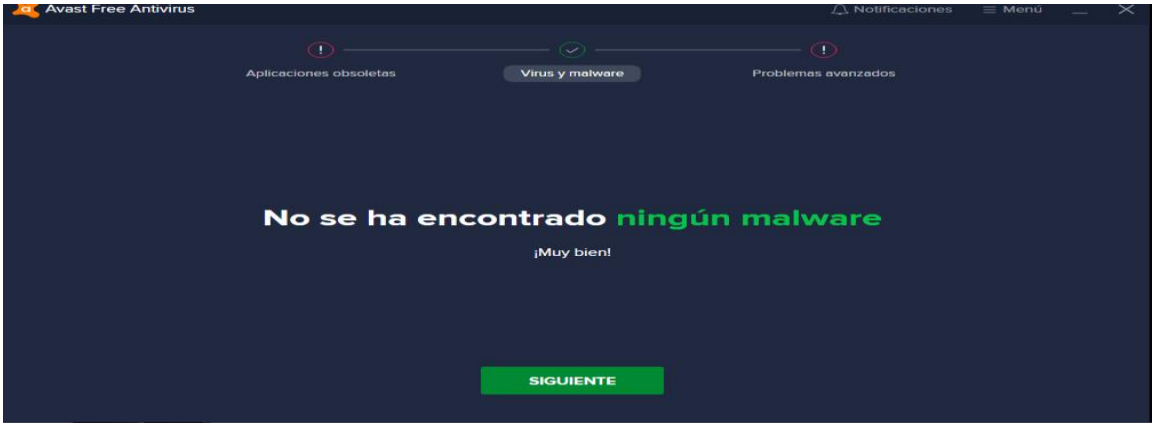

Advertencia de seguridad de Abrir archivo
No se pudo comprobar el editor. ¿Está seguro de que desea ejecutar este software?
Nombre: ...instalación_en_línea_de_avast_free_antivirus.exe
Editor: Editor desconocido
Tipo: Aplicación
De: C:\Users\usuario\Downloads\instalación_en_lín...
Ejecutar
Cancelar
Preguntar siempre antes de abrir este archivo
Este archivo no tiene ninguna firma digital válida que compruebe su editor. Sólo ejecute software de los editores en los que confía.
¿Cómo puedo decidir qué software debo ejecutar?


Avast


Instalación de Avast Free Antivirus
Español
Avast Free Antivirus
Mediante la instalación y el uso del producto, muestra su conformidad con los
Acuerdo de licencia de usuario final y Política de privacidad
INSTALAR
Personalizar


avast
Ocultar
Instalando
Avast Free Antivirus...
No apague el equipo


Avast Free Antivirus
Notificaciones
Menú
Aplicaciones obsoletas
Virus y malware
Problemas avanzados
Se ha encontrado 1 aplicación obsoleta
Estas reliquias pueden contener agujeros de seguridad que amenazan su seguridad. Es mejor actualizarlas.
Nombre de la aplicación
Versión
7-Zip Filemanager (64 Bit)
24.4.0.0 > Nueva 24.4 ¿Qué ha cambiado?
Actualizada
Mozilla Firefox (64 Bit)
77.0.1 > Nueva 115.0.3 ¿Qué ha cambiado?
1 aplicación obsoleta seleccionada
ACTUALIZAR TODO
Omitir por ahora



Fuente. Autoría propia

Análisis Sobre las Diferencias Entre el Equipo de Blue Team y el Equipo de Respuesta a Incidentes Informáticos

El siguiente cuadro nos permite ver las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos

Tabla 6

Cuadro Comparativo Equipo de Blue Team y Equipo de Respuesta a Incidentes Informáticos

Equipo de Blue Team	Equipo de respuesta a incidentes informáticos
Se encargan recolectar información para registrar todo lo que necesita ser protegido, y realiza una evaluación de riesgos. Se encarga de fortalecer el acceso al sistema de diferentes maneras, por ejemplo, implementando políticas de seguridad más rigurosas y desempeñando un papel educativo con los empleados de la organización para que comprendan y se adapten a los procedimientos de seguridad de la misma.	Se encargan recibir y dar respuesta a los incidentes de los sistemas informáticos que reporta una organización, empresa o entidad. Se encargan de recopilar información de los incidentes de los sistemas, con el fin de identificar, analizar y mitigar los incidentes.

Equipo de Blue Team	Equipo de respuesta a incidentes informáticos
Se encarga de documentar la información relacionada con el acceso a los sistemas y verificar si hay algún tipo de actividad atípica.	Se encargan de vigilar constantemente las vulnerabilidades a las que la organización puede verse expuesta.
Se encarga de realizar revisiones regulares del sistema, tales como auditorías del sistema de nombres de dominio (DNS), de la vulnerabilidad de la red interna o externa, entre otros.	Se encarga de proporcionar instrucciones sobre cómo minimizar una amenaza, e incluso proporcionar directrices para la configuración de las herramientas destinadas al servicio de la organización.
Se encargan de llevar a cabo evaluaciones de riesgo para detectar las amenazas a cada activo y las vulnerabilidades que pueden aprovechar. Así, el equipo tiene la oportunidad de elaborar un plan de acción anticipado	Se encargan de administrar las diversas vulnerabilidades que surgen en la compañía.

Fuente. Autoría propia

Análisis Sobre la Pertinencia de Trabajar con CIS "Center For Internet Security" Como Propuesta de Aseguramiento por Parte de un Equipo de Blue Team

Teniendo en cuenta la labor que realiza el Centro de Seguridad de Internet -CIS su conformación de comunidad de profesionales de ciberseguridad que inició en el año 2000, cuyo objetivo es dar recomendaciones de forma segura a los sistemas de información, redes, software, entre otros, con respecto a la identificación, desarrollo, validación, promoción, la autenticación de usuarios y dar soluciones mejoradas para la defensa cibernética, es interesante hacer parte de su comunidad con el fin de aprovechar las herramientas y poder potencializar la habilidad del equipo Blue Team en la identificación y prevención de amenazas tecnológicas, lo que contribuye a reforzar la seguridad de la organización.

Análisis Sobre las Funciones y Características Principales de un SIEM

SIEM (siem, s.f.)es la Gestión de Eventos e Información de Seguridad (Security Information and Event Management). Es una solución de seguridad que asiste a las entidades en la identificación, análisis y reacción ante amenazas. Emplean la inteligencia artificial (IA) para automatizar numerosos procedimientos manuales vinculados a la identificación de amenazas y la reacción ante incidentes. Las soluciones SIEM llevan a cabo un grado de funciones de agregación, consolidación y categorización de datos con el fin de detectar amenazas, a continuación se relacionan las funciones más utilizadas:

Gestión de Registros y Bases de Datos. Recolecta información de sucesos provenientes de diferentes fuentes en la red de la entidad. Los datos y registros de usuarios, aplicaciones, redes son procesados, activos y ambientes en la nube, guardados y examinados en tiempo real.

Correlación y análisis de eventos. Mediante el uso de análisis sofisticados para identificar y entender los patrones complejos de información, la correlación de eventos ofrece datos para identificar y minimizar rápidamente las potenciales amenazas a la seguridad.

Supervisión de Incidentes y Alertas de Seguridad. Capaz de reconocer y controlar todas las entidades del ambiente de informática. Estos sistemas emiten advertencias al identificar acciones sospechosas o malintencionadas que podrían señalar un ataque o una infracción. Las alertas pueden contener datos acerca del tipo, el origen, la severidad, y el propósito del incidente, además de recomendaciones para su solución. Para lograrlo, pueden hacer uso de programas como IDS (Sistema de Detección de Intrusión o Sistema de Prevención de Intrusión) e IPS

Cumplimiento Normativo. También asisten a las organizaciones en el cumplimiento de las regulaciones y estándares que requieren mantener un registro completo y comprobable de sus actividades e incidentes de seguridad. Es posible producir informes preestablecidos que

evidencien el acatamiento de marcos como GDPR ,PCI, SOX, DSS, HIPPA, y otros estándares de conformidad.

Las características para dar contestación rápida y eficaz a los incidentes son (Linkedin, 2024):

Monitoreo en Tiempo Real. Permite realizar la identificación a accesos no autorizados, monitorear comportamientos inusuales o sospechosos, detectar malware, lo que permite la mitigación inmediata ante incidentes.

Analítica avanzada. Puede detectar anomalías que indican amenazas para la seguridad, también proporciona técnicas, tácticas y procedimientos de los atacantes, lo que ayuda a desarrollar estrategias de defensa más eficientes.

Inteligencia de Amenazas. Permite la identificación de direcciones IP maliciosas, nombre de dominios e indicadores de compromiso que se pueden utilizar para mejorar las capacidades de detección de su sistema SIEM. También le permite avanzar ante las amenazas emergentes valiéndose de los datos de inteligencia global, lo que facilita la identificación y la respuesta a los ataques que se han visto en otros sitios antes de que perturben la organización

Gestión de Incidencias. Permite realizar un rastreo y tratar el ciclo de vida de un incidente desde su descubrimiento hasta su resolución, lo que incluye el registro de toda la información, la retribución de tareas a los integrantes del grupo y la documentación del proceso de respuesta para el análisis posterior al suceso.

Informes de Cumplimiento. `Proporcionan informes que demuestran el cumplimiento de normas como el Reglamento General de Protección de Datos (RGPD), la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA) y el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)

Análisis del Comportamiento de Usuarios y Entidades. Es una función que mejora la detección de cuentas comprometidas y amenazas internas. También ayuda a identificar rápidamente las acciones potencialmente malicioso realizadas por entidades o usuarios dentro de su red, lo que podría significar el uso indebido de las credenciales.

Informe de Elección de 3 Herramientas que Permitan Contener Ataques Informáticos

Las herramientas que permiten la contención de ataques informáticos en los activos de una organización, empresa o entidad son (Gómez, 2024):

Firewall. También conocido como cortafuegos es una herramienta que nos permite escanear los datos o paquetes de red que pueden ingresar a la red privada en donde se puede restringir el acceso de acuerdo con la autorización por parte del administrador. De igual manera tiene la capacidad de inspeccionar el tráfico web, clasificar archivos, bloquear el acceso a terceros, identificar usuarios, denegar el acceso a direcciones IP, denegar el acceso a protocolos, puertos.

Servidor Proxy. es una herramienta permite establecer un sistema de autenticación que restringe el acceso a la red externa, de igual manera analiza el tráfico de red para no permitir las solicitudes no deseadas, realizar el filtro de los paquetes de conexión entre el Internet y el navegador, también pueden bloquear el acceso a sitios no permitidos al interior de la empresa o sitios web peligrosos.

OSSEC. (Cilleruelo, 2024): es un HIDS (Host-based Intrusion Detection System) de código abierto, permite monitorear uno o más servidores, genera alertas sobre las posibles amenazas que detecta, permite utilizar los dispositivos de una red con la finalidad de procesar toda la información recopilada durante el monitoreo del sistema, puede ejecutar con este programa la detección de rootkits, respuesta activa ante brechas e incidentes, detección de

intrusos basada en logs, monitorización de la integridad de los archivos y el inventario del sistema.

Conclusiones

La normatividad colombiana sobre los delitos informáticos y la protección de los datos personales establece la penalidad a los delincuentes informáticos y en acabar con este flagelo.

El Código de Ética profesional para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, establece los derechos, deberes, prohibiciones y faltas gravísimas, que deben de acatar y cumplir en el ejercicio de sus funciones.

Las herramientas de ciberseguridad como el pentestig, los equipos Red Team & Blue Team, entre otros, logran la identificación de las vulnerabilidades, el ciberespionaje a la que están expuestas las aplicaciones, los sistemas de redes y servidores en una organización, empresa o entidad, con el fin de mejorar la disponibilidad, confidencialidad e integridad, seguridad, protección de la información y datos personales.

Las estrategias de contención de ataques de ciberseguridad, permiten la mitigación de: riesgos, ataques, amenazas y vulnerabilidades que una organización, empresa o entidades puede tener en sus activos los cuales puedan afectar la integridad, disponibilidad y confidencialidad de la información y la protección de los datos personales, por tal motivo es importante la protección de los activos de la organización, con herramientas que nos permitan robustecer los sistemas informáticos contra los ataques maliciosos y estar actualizados como profesionales de ciberseguridad logrando un buen desempeño laboral en la protección de la información.

Recomendaciones

Implementar herramientas que permitan la protección de la información como sistemas de detección de intrusiones, antivirus, firewalls, pruebas de penetración pentesting, entre otros

Fomentar estrategias en el buen manejo herramientas tecnológicas, la seguridad y protección de la información, con el fin de promover la cultura de la seguridad de los sistemas de información y poder mitigar los incidentes que se presentan al interior o exterior de una organización.

Implementar políticas de seguridad y protección de la información y de los datos personales que permitan la mitigación a incidentes o eventos, con el fin de robustecer los sistemas de información, mejorar el control por parte del administrador de la seguridad de la información y aplicar los aspectos éticos y legales.

Proteger los activos de información de los riesgos cibernéticos que diariamente se viven en el mundo, con el fin de que no sean vulnerados.

Implementar auditorias de seguridad en los sistemas de información que permitan identificar las falencias que se puedan presentar al interior o exterior de la organización, con respecto a incidentes de ciberseguridad.

Bibliografía

1989, D. 1. (s.f.). Decreto 1360 de 1989. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=10575

2000, L. 5. (2000). Ley 599 de 2000.

2001, L. 6. (2001). Ley 679 de 2001. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=18309

2003, L. 8. (2003). Ley 842 de 2003. http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html

Alvarez, V. (2018). Propuesta de una Metodología de Pruebas de Penetración. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Chindrus, C. &. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information. https://doi.org/10.3390/info14110587

Ciberseguridad. (s.f.). Ciberseguridad Noticias de ciberseguridad, Ciberataques, Vulnerabilidades Informáticas. https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Cilleruelo, C. (2024). KEEPCODING. ¿Qué es OSSEC?. https://keepcoding.io/blog/que-es-ossec/

CIS, C. f. (2020). Center for Internet Security CIS. https://www.cisecurity.org/cis-benchmarks

Colombia, C. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Contabilidad, C. d. (2010). SCIELO. Delitos Informáticos y Entorno Jurídico Vigente en Colombia. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Copnia. (2015). Código de Ética para el Ejercicio de la Ingeniería en General. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

FORTINET. (2023). ¿Qué es una CVE? Vulnerabilidades y exposiciones comunes definidas https://www.fortinet.com/lat/resources/cyberglossary/cve#:~:text=Vulnerabilidades%20y%20exposiciones%20comunes%20explicadas,describe%20los%20riesgos%20conocidos%20p%C3%BAblicamente.

Gómez, J. A. (2024). APOLO. Las 12 Mejores Herramientas de Seguridad Informática para Empresas. https://www.deltaprotect.com/blog/herramientas-seguridad-informatica

INCIBE. (2019). ¿Qué es el Pentesting? Auditando la Seguridad de tus Sistemas. https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tus-sistemas

Jurado, P. J. (2015). Técnicas de Detección de Ataques en un Sistema SIEM (Security Information and Event Management). https://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

KEEPCONDING. (s.f.). ¿Qué es ExploitDB? https://keepcoding.io/blog/que-es-exploitdb/#:~:text=ExploitDB%20es%20una%20aplicaci%C3%B3n%20web,lo%20que%20contribuyen%20los%20usuarios.

Kotwani, B. (2023). Red Teaming vs. Blue Teaming: Un análisis comparativo de las estrategias de ciberseguridad en el campo de batalla digital. https://ijsrem.com/download/red-teaming-vs-blue-teaming-a-comparative-analysis-of-cybersecurity-strategies-in-the-digital-battlefield/

Lazaro, R. G. (2020). Hack By Security. https://www.hackbysecurity.com/blog/metasploit-cheat-sheet-1

Linkedin. (2024). Linkedin. https://es.linkedin.com/advice/1/what-key-features-look-siem-system-effective-jkpbe?lang=es

Luis Fernando Zambrano Hernández, L. C. (2024). Guía para la Gestión y Clasificación de Incidentes de Ciberseguridad. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Mateus, Z. (2017). Hacking Ético Basado en la Metodología Abierta de Testeo de Seguridad – OSSTMM, Aplicado A La Rama Judicial. https://repository.unad.edu.co/handle/10596/17410

MINTIC. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

Nacional, C. C. (2016). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file?format=html

pandasecurity. (2023). Grandes retos de las pymes en ciberseguridad. https://www.pandasecurity.com/es/mediacenter/retos-pymes-ciberseguridad/

Policía. (2009). Ley 1273 [LEY_1273_2009]. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Qué son los puntos de referencia de CIS? (2000). https://www.ibm.com/mx-es/topics/cis-benchmarks

Quintero, J. (2020). RedTeam y BlueTeam, Equipos Estratégicos al Interior de una Organización. [Objeto_virtual_de_Informacion_OVI]. https://repository.unad.edu.co/handle/10596/35497

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. https://ieeexplore.ieee.org/document/6081410

Rapid7. (2012). Metasploitable 2. https://docs.rapid7.com/metasploit/metasploitable-2/

REDES ZONE. (s.f.). Realiza Escaneos de Puertos con Nmap a Cualquier Servidor o Sistema https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

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

SIEM. (s.f.). ¿Qué es la Gestión de Eventos e Información de Seguridad (SIEM)? https://www.ibm.com/es-es/topics/siem

Smartekh, G. (2012). Tips Tecnológicos, de Configuración y Negocio que Complementan tu Seguridad. https://blog.smartekh.com/que-es-hardening

Vera, R. A. (2020). OpenWebinars. https://openwebinars.net/blog/que-es-openvas/

Apéndice

Apéndice A

Sustentación del Informe Técnico

- Link video: https://www.youtube.com/watch?v=rNOcoWonink