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

HAYR ALEXIS MARTINEZ PEÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACION SEGURIDAD INFORMATICA
DUITAMA
2023

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

HAYR ALEXIS MARTINEZ PEÑA

JOHN FREDDY QUINTERO TAMAYO
DIRECTOR CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACION SEGURIDAD INFORMATICA
DUITAMA
2023

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Duitama, septiembre 2023

DEDICATORIA

Con amor dedico este trabajo a toda mi familia, la cual me impulsa a la mejora continua de mis capacidades como profesional y persona. Logrando ser integral en todo aspecto. Agradezco el apoyo de ellos por colaborarme en ciertas tareas de la vida diaria, para que por mi parte me pueda enfocar de lleno en este trabajo para lograr un producto de calidad.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, por permitirme ser parte de tan prestigiosa institución. La cual por medio de sus docentes y calidad de educación me ha permitido progresar en el ámbito educativo y profesional, proporcionando todo lo que está a su alcance para que pueda estudiar y logar mis sueños.

RESUMEN

Debido a la problemática planteada en cada uno de los anexos suministrados dentro del seminario, por medio de personal experto se busca verificar y analizar ciertos tipos de comportamientos relacionados con este tema. Por otro lado, el uso de herramientas de penetración y detección de vulnerabilidades por parte de Red Team y Blue Team se podría afectar servicios y procesos en organización.

Se toma una metodología mixta la cual permite abarcar distintos puntos de vista y permite recolectar información orientada al tema en cuestión, se hace uso del modelo metodológico el cual está muy enfocado en pruebas de penetración, teniendo como referente este. Permite identificar distintas herramientas para realizar este tipo de pruebas de igual forma se tiene en cuenta las ventajas y desventajas que tiene el uso de estas herramientas dentro de las organizaciones tecnológicas. Se logra inferir que por este tipo de prácticas y técnicas se puede verificar el estado de seguridad de los servicios mencionados con anterioridad, pero de igual manera en algunas ocasiones se puede estar afectando alguno de estos procesos y servicios en las organizaciones debido al uso de estas herramientas ya que se está haciendo una intrusión al sistema, se plantea ciertas pautas y recomendaciones para que al momento de realizar estas pruebas no se vea afectada la organización.

Teniendo en cuenta los anteriores aspectos, se realiza la construcción del diseño para la implementación de pruebas de intrusión, este tipo de pruebas están enfocadas primero que todo para la detección de vulnerabilidades por medio del uso de herramientas de tipo software, estas permitirán al Red Team diseñar estrategias para no afectar ningún servicio, proceso o fuga de información de la organización la cual se encuentra involucrada. Por otro lado, al momento de tener la estrategia de intrusión y la metodología de ejecución clara se dispondrá a realizar por medio de un ambiente controlado pruebas de intrusión para así poder detectar las falencias que puede tener el sistema a intervenir. Teniendo en cuenta lo anterior por parte del Blue Team suministrara controles y recomendaciones de como asegurar la infraestructura, servicios y procesos de la organización, esto con el fin de mitigar o eliminar ataques.

Palabras claves: Blue Team, Herramientas de penetración y detección de vulnerabilidades, Intrusión, Metodología, Red Team.

ABSTRACT

Due to the problems raised in each of the annexes provided within the seminar, expert personnel seek to verify and analyze certain types of behaviors related to this topic. On the other hand, the use of penetration and vulnerability detection tools by Red Team and Blue Team could affect services and processes in the organization.

A mixed methodology is taken which allows covering different points of view and allows collecting information oriented to the topic in question, using the methodological model which is highly focused on penetration testing, having this as a reference. It allows different tools to be identified to carry out this type of tests, and the advantages and disadvantages of using these tools within technological organizations are also taken into account. It can be inferred that through this type of practices and techniques, the security status of the services mentioned above can be verified, but in the same way, on some occasions some of these processes and services in organizations may be affected due to the use of these tools since an intrusion is being made to the system, certain guidelines and recommendations are proposed so that when these tests are carried out the organization is not affected.

Taking into account the previous aspects, the construction of the design for the implementation of intrusion tests is carried out, this type of tests are focused first of all on the detection of vulnerabilities through the use of software type tools, these will allow the Red Team design strategies to not affect any service, process or information leak of the organization which is involved. On the other hand, once you have the intrusion strategy and the clear execution methodology, you will be prepared to carry out intrusion tests through a controlled environment in order to detect any flaws that the system to intervene may have. Taking the above into account, the Blue Team will provide controls and recommendations on how to secure the organization's infrastructure, services and processes, in order to mitigate or eliminate attacks.

Keywords: Blue Team, Penetration and vulnerability detection tools, Intrusion, Methodology, Red Team.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

CIBERSEGURIDAD: Practica que se encarga de la protección de información, infraestructura tecnológica y aplicativos de ciberdelincuentes.

DETECCIÓN: Proceso el cual permite analizar y monitorear eventos poco inusuales dentro de los sistemas de la organización.

ESTÁNDAR: Guía o modelo que se toma como referencia para realizar una implementación o actividad especifica, en el área de la ciberseguridad se utiliza como guía de buenas prácticas y diseño de sistemas de gestión de la seguridad de la información.

HERRAMIENTAS DE PENETRACIÓN O PENTESTING: Herramientas de tipo software las cuales permiten ingresar o captar información de un sistema especifico, herramienta utilizada por el Red Team o Ciberdelincuentes.

INFORMACIÓN: Conjunto de datos lo cuales contienen un mensaje especifico el cual puede ser de alto valor, en temas de ciberseguridad la mayoría de las veces es de mucha criticidad.

RED TEAM: Grupo de hackers éticos los cuales implementan técnicas de penetración para la detección de vulnerabilidades en organizaciones.

RIESGO: Es un elemento o factor el cual genere un tipo de desconfianza o probabilidad de fuga de información, daño a la infraestructura tecnológica y operaciones y servicios de la organización.

TÉCNICAS: Práctica la cual tiene como objetivo llegar a un resultado final con los parámetros y requisitos que tenía el objetivo inicial.

VULNERABILIDAD: Se conoce como una falencia dentro de un sistema informático, la cual puede provocar un peligro o riesgo a la organización, esto lo puede aprovechar un ciberdelincuente para hacer daño a esta.

INTRODUCCIÓN

En el presente documento se puede apreciar lo fundamental que es para las organizaciones contar con un Red Team y Blue Team. Por medio de prácticas, técnicas y con la ayuda de herramientas de penetración y detección de vulnerabilidades. El uso de estándares y metodologías, se identificaron herramientas de penetración, las cuales permiten saber si cumplen con los requerimientos de seguridad para la operabilidad. Debido al crecimiento de amenazas y ataques por parte de ciberdelincuentes, las organizaciones cada vez están haciendo más uso del Red Team y Blue Team para realizar este tipo de pruebas. Teniendo en cuenta lo anterior se realiza recomendaciones a las organizaciones para mitigar el riesgo al momento de realizar pruebas de penetración debido a que algunas ocasiones pueden afectar algunos procesos y servicios al momento de hacer uso de las herramientas de penetración de detección de vulnerabilidades.

OBJETIVOS

Objetivo General.

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

Objetivos Específicos.

- Establecer estrategias o técnicas de intrusión con el fin de emular lo hecho por el atacante.
- Diseñar políticas de seguridad para mitigar o eliminar amenazas relacionadas con ciberseguridad.

DESARROLLO DEL INFORME

CONCEPTOS EQUIPOS DE SEGURIDAD

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

Ley 1273 de 2009: Esta ley está enfocada en la protección de la información y datos, esto con el fin de proteger a personas u organizaciones de algún tipo de fraude o ataque relacionado con la información y protección de la datos. Teniendo en cuenta lo anterior se puede comprender mejor esta ley sus respectivos artículos los cuales serán mencionados a continuación.

Artículo 269A: Acceso abusivo a un sistema informático. Este articulo quiere decir que todo acceso sin autorización puede tener una pena de prisión entre 48 a 96 meses y una multa 100 a 1000 SMLV.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Por medio de este que, si alguien que no tenga las facultades, obstruye o interrumpe algún sistema informático o de telecomunicaciones, puede tener una pena de prisión entre 48 a 96 meses y una multa 100 a 1000 SMLV.

Artículo 269C: Interceptación de datos informáticos. Esta terminante prohibido el intercepción de datos sin previa autorización judicial, si se incurre en esto puede tener una pena de prisión entre 36 a 72 meses.

Artículo 269D: Daño Informático. El daño, modificaciones, eliminación de información de algún sistema informático , puede tener una pena de prisión entre 48 a 96 meses y una multa 100 a 1000 SMLV.

Artículo 269E: Uso de software malicioso. Es prohibido el uso, venta, circulación de cualquier tipo de software malicioso, puede tener una pena de prisión entre 48 a 96 meses y una multa 100 a 1000 SMLV.

Artículo 269F: Violación de datos personales. Sin tener las facultades o su respectiva autorización, no se puede hacer uso de datos de ninguna índole para

realizar venta, intercambios, modificaciones, entre otros, puede tener una pena de prisión entre 48 a 96 meses y una multa 100 a 1000 SMLV.

Artículo 269G: Suplantación de sitios web para capturar datos personales. No se podrá realizar ningún diseño, programa, publicidad, ejecutables con el fin de capturar datos, puede tener una pena de prisión entre 48 a 96 meses y una multa 100 a 1000 SMLV.

Artículo 269H: Circunstancias de agravación punitiva, en este articulo las penas pueden variar respecto a los siguientes ítems:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.

Teniendo en cuenta lo anterior, se puede aumentar la pena de la mitad a tres cuartas partes.

Artículo 269I: Hurto por medios informáticos y semejantes, por medio de este aquel que incurra en la penetración de cualquier sistema informático que manipule o modifique información tendrá como pena la mencionada en el artículo 240 de este código.

Artículo 269J: Transferencia no consentida de activos, todo aquel que se lucre por medio de la información o datos o haga afectaciones por medio de esta tendrá como pena entre 48 a 120 meses de prisión y una multa de 200 a 1500 SMLV.

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

Antes de responder las preguntas se debe de dar claridad en que consiste footprinting, lo podríamos ver como un pre antes de un ciberataque. La información

recolectada se puede encontrar de manera pública y gratuita, mucha de esta información está disponible en sitios web, redes sociales y motores de búsqueda.

¿Qué aplicaciones (Opensource y pagas) podría utilizar para este proceso?

- Google Dorks.
- WHOIS.
- Netcraft.
- DNS Recon.

¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?

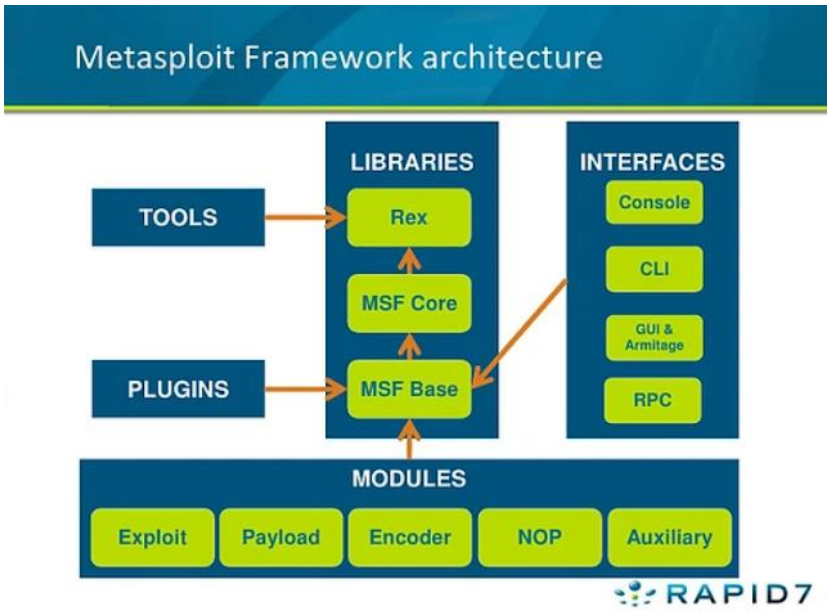
Teniendo en cuenta lo anterior este procedimiento es muy importante debido a que por medio de este se recolecta información de gran importancia para realizar el proceso de pentesting, la información recolectada usando uso de las distintas herramientas footprinting nos podrá suministra por medio del dominio, IPs de servidores, puertos, servicios, protocolos, entre otros.

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

Metasploit: Es un framework y software de código abierto el cual se encuentra disponible en la paquetería de herramientas de Kali Linux, esta herramienta es una de la más utilizadas en la ejecución de exploits. Metasploit ahora incluye más de 1677 exploits.

Teniendo en cuenta lo anterior los exploits que contienen esta herramienta pueden ser utilizados en: Escaneos y recopilación de información, detección y explotación de vulnerabilidades, escalamiento de privilegios, ataques relacionados con puertas traseras, fuzzing, evasión de software de seguridad, acceso remoto, eliminación de rastros de actividades maliciosas, entre otros.

Figura 1. Arquitectura Metasploit.



Fuente: https://mostrandomishobbies.blogspot.com/

- ¿Qué es un CVE y su estructura?

  CVE (Common Vulnerabilities and Exposures) es conocido como un programa encargado de identificar, definir y catalogar las vulnerabilidades de seguridad cibernética divulgadas públicamente, este proyecto fue formado principalmente por el gobierno de los estados unidos, por medio de este se busca tener una colaboración internacional con el fin de estructurar y definir las distintas amenazas y ataques cibernéticos.

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

  CVE cuenta con un proceso de articulación para definir si es necesario incluir dentro del programa una vulnerabilidad, para esto se debe de tener los siguientes aspectos:

Presentación inicial y tratamiento: En este fase lo que se busca es analizar, investigar las solicitudes de los registros correspondientes a las vulnerabilidades presentadas.

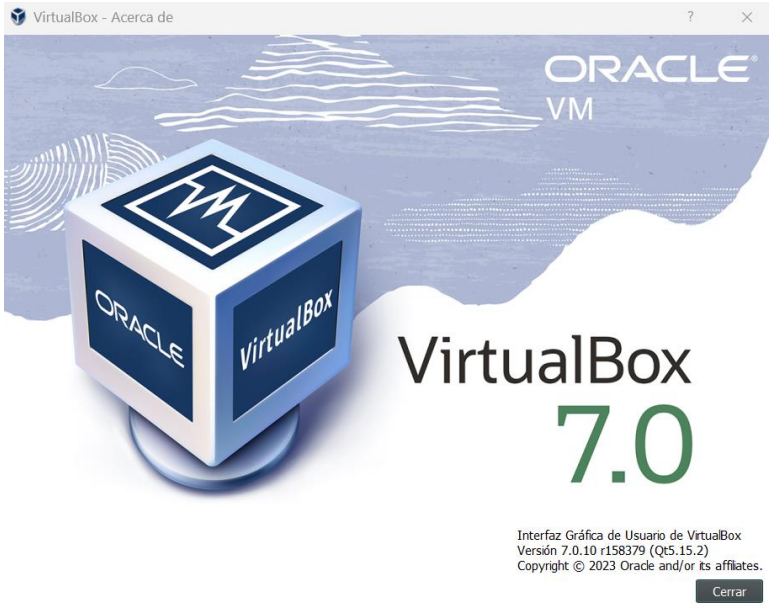
Candidatura: Esta fase tiene en cuenta 3 ítems, las cuales pueden ser por medio de la asignación directa de CVE Content Team, teniendo en cuenta el estudio previo de la propuesta de la vulnerabilidad. Por otro lado, CVE Editor puede realizar una asignación directa si la vulnerabilidad se considera critica. Después se realiza una reserva o identificador CVE-ID esto lo realiza una organización o personal calificado.

Publicación: El tema de la publicación puede tardar un tema indefinido, este proceso puede cambiar ya que puede cambiar algunos factores en la revisiones y aprobaciones previas.

4. Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad.

Paso A: Descargar la herramienta virtualizadora “VirtualBox”

Figura 2. VirtualBox 7.0.10

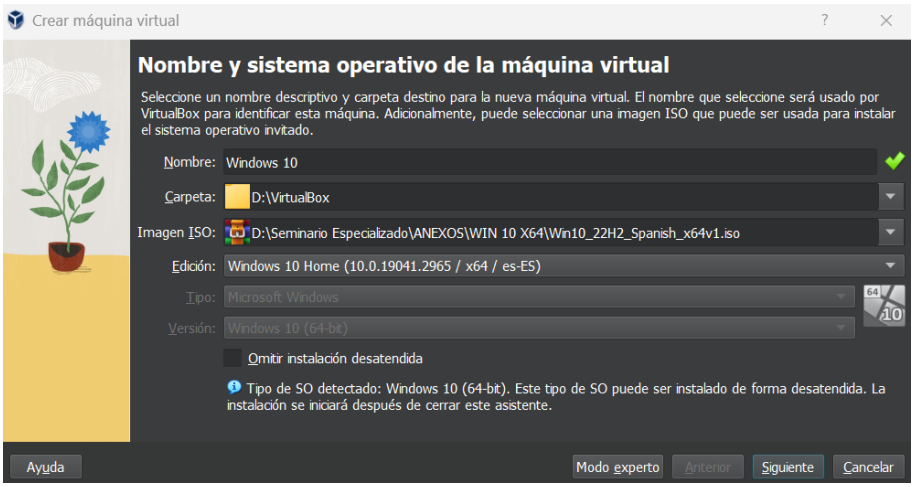


Fuente: Propia.

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

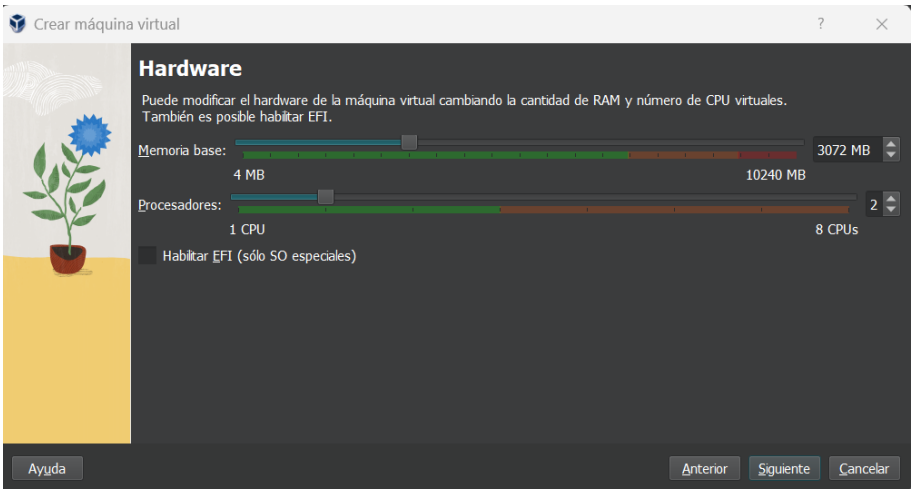
Instalación máquina virtual Windows 10.

Figura 3. Creación Máquina Virtual.



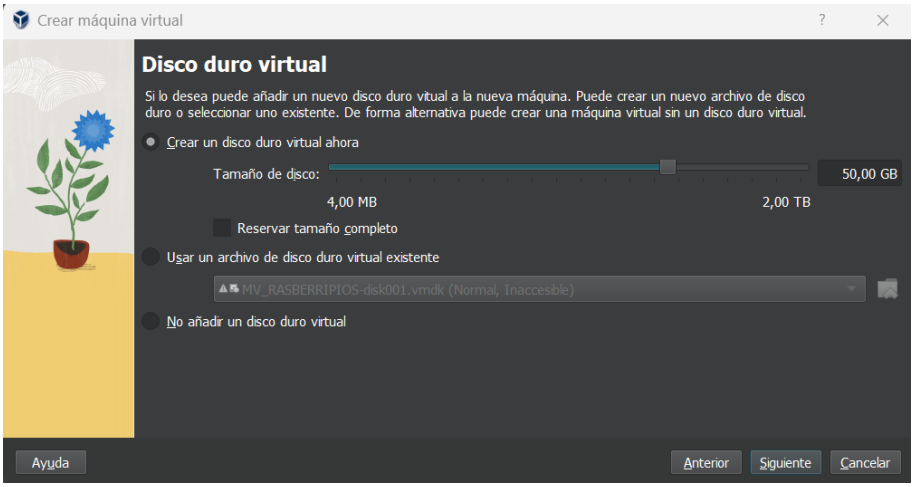
Fuente: Propia.

Figura 4. RAM - Procesador.



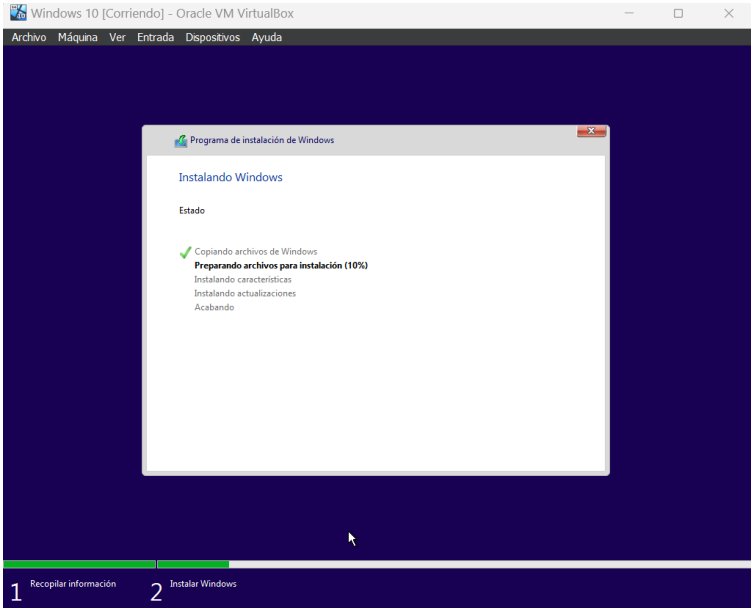
Fuente: Propia.

Figura 5. Disco Duro.



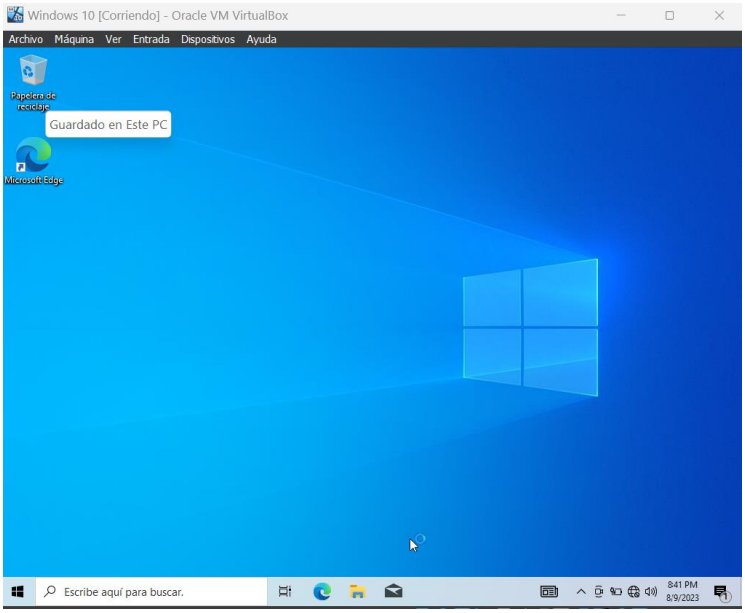
Fuente: Propia.

Figura 6. Instalación SO.



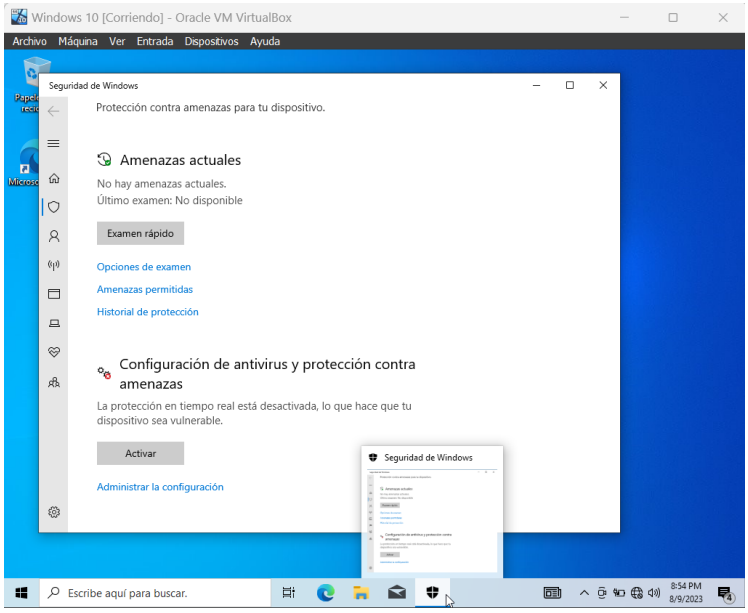
Fuente: Propia.

Figura 7. Escritorio Windows 10.



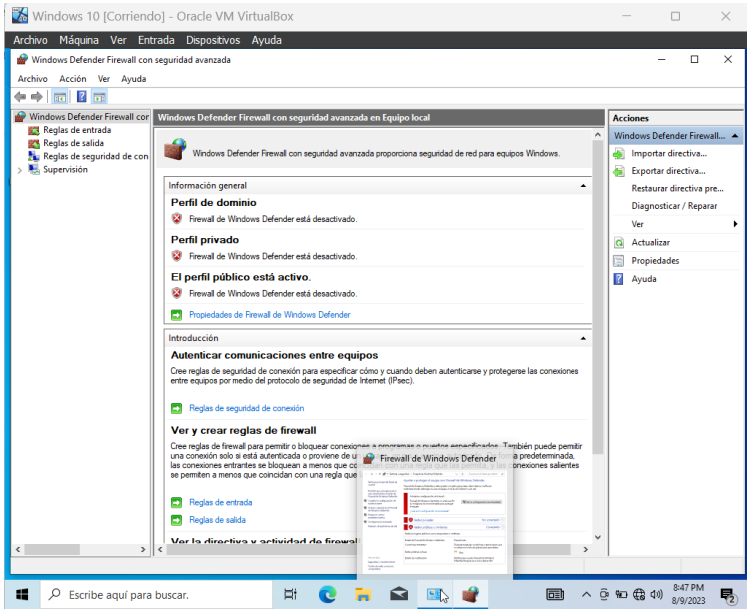
Fuente: Propia.

Figura 8.Desactivación antivirus.



Fuente: Propia.

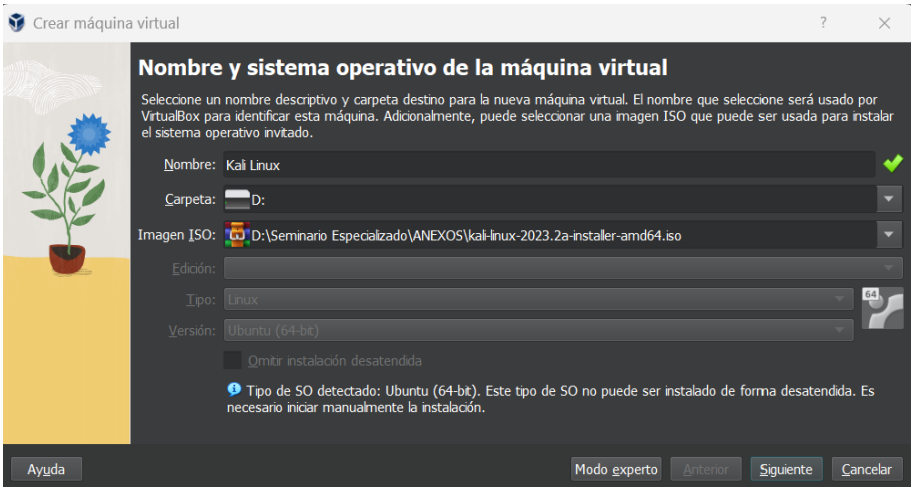
Figura 9. Firewall desactivado.



Fuente: Propia.

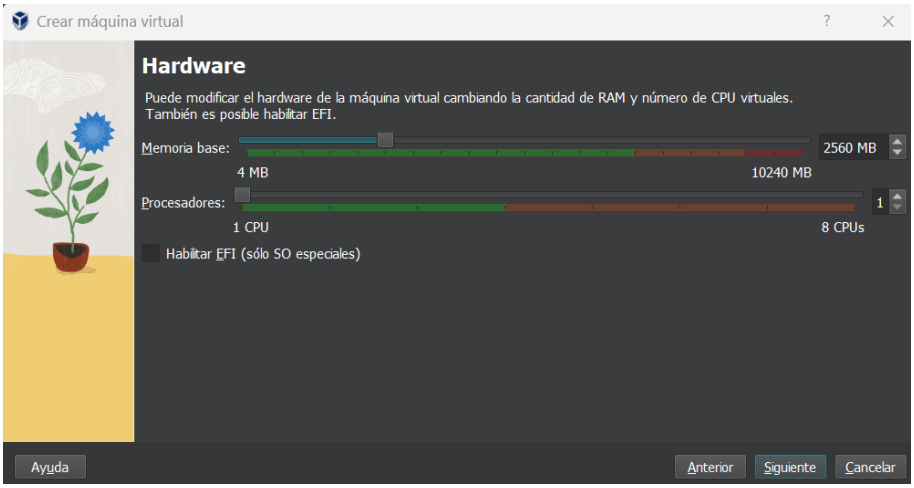
Instalación máquina virtual Kali Linux.

Figura 10. Creación Máquina Virtual.



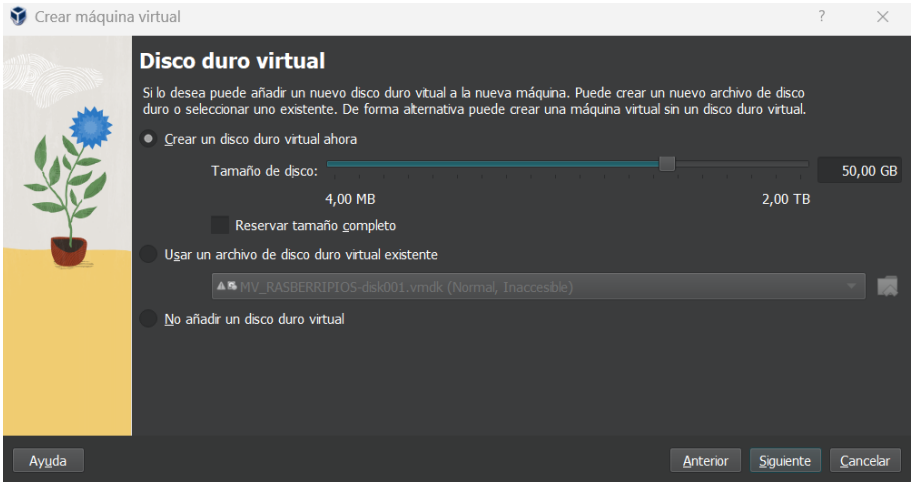
Fuente: Propia.

Figura 11. RAM y Procesador.



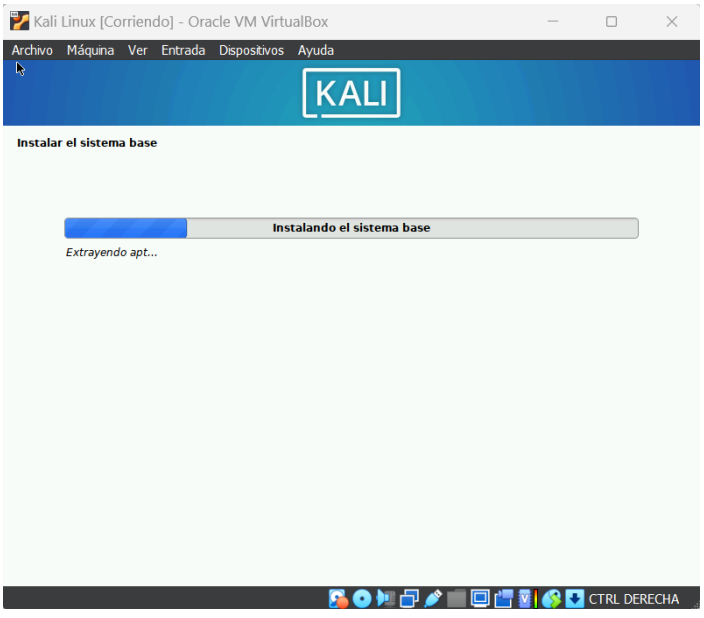
Fuente: Propia.

Figura 12. Disco Duro.



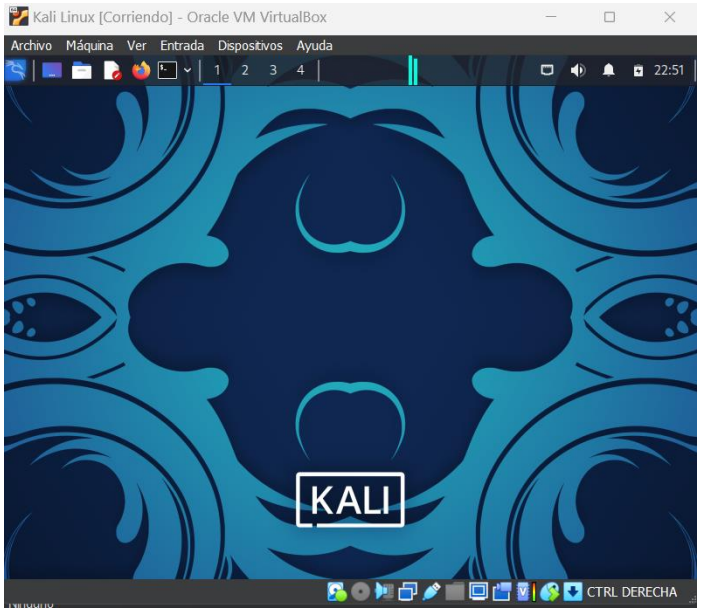
Fuente: Propia.

Figura 13. Instalación Kali Linux.



Fuente: Propia.

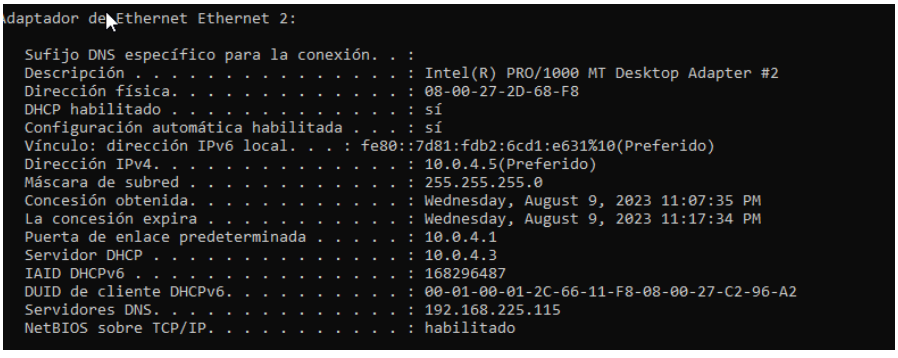
Figura 14. Kali Linux.



Fuente: Propia.

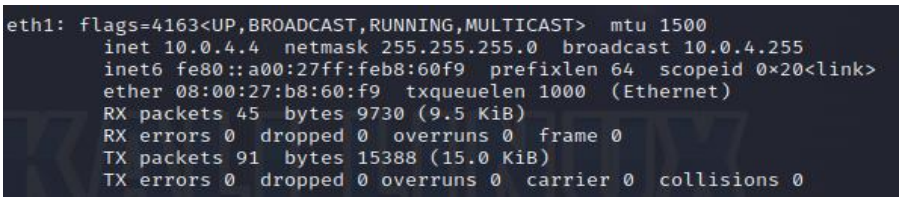
Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows y Kali Linux, recuerde por favor no exceder la asignación de recursos entre las dos máquinas ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda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

Figura 15. IP Maquina Windows 10.



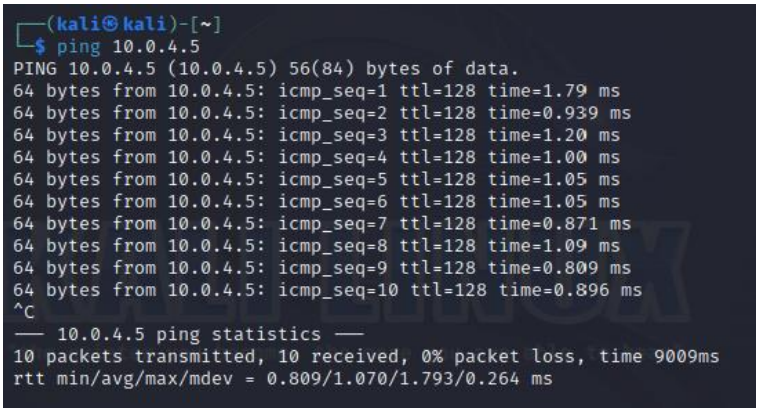
Fuente: Propia.

Figura 16. IP Maquina Kali Linux.



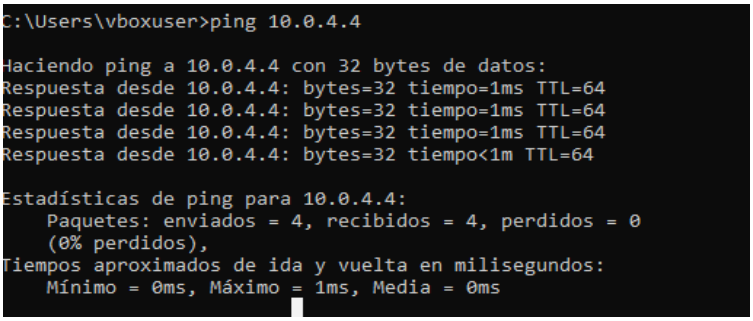
Fuente: Propia.

Figura 17. Ping de Kali Linux a Windows.



Fuente: Propia.

Figura 18. Ping Windows a Kali Linux.



Fuente: Propia.

ACTUACIÓN ÉTICA Y LEGAL

Teniendo en cuenta el anexo 2 y anexo 3 se da con el desarrollo de la presente actividad.

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

Teniendo en cuenta el análisis realizado de los anexos suministrados previamente se logra encontrar distintas falencias en el acuerdo de confidencialidad, para ello se indicará las partes y párrafos que se consideran ilegales o que podrían afectar a la parte receptora y a su ver a la organización.

Cláusulas.

Primera: En esta cláusula se indica que no se puede divulgar ningún tipo de proceso Ilegal dentro de la organización.

Segunda: En el ítem 2 indica temas relacionados con datos secretos, chuzadas, Intercepción ilegal de información, accesos intrusivos a sistemas informáticos.

Cuarta: En el ítem 3 indica que la parte receptora no realizara denuncias de Actividades sospechosas, las cuales tengan que ver con espionaje y temas relacionados con la apropiación de datos de terceros. En el ítem 6 indica que la parte receptora no trasmitirá ningún tipo de información confidencial o ilegal sin consentimiento de la organización.

Octava: Según la solución de controversias, indica que teniendo en cuenta la información ilegal o confidencial que se encuentre en el poder de la parte receptora, esta deberá acudir a un abogado privado y deberá dejar exenta de cualquier responsabilidad legal y penal a la organización.

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

Teniendo en cuenta el anexo 3, se encontraron ciertas inconsistencias las cuales incurren en aspectos ilegales, para ello se logra sustentar dicha información en los artículos relacionados con la ley 1273 del 2009.

- En la primera clausula, puede estar incurriendo en el artículo 269F el cual habla de la violación de datos personales, donde se habla de la divulgación de datos y esto puede incurrir en penas de prisión de 48 a 96 meses y una multa de 100 a 1.000 SMLV.

- En la segunda clausula en el ítem 2 se puede estar incurriendo en Acceso abusivo a un sistema informático del artículo 269A, Interceptación de datos informáticos del artículo 269C. Estas infracciones pueden incurrir en sanciones económicas y penas carcelarias, el primer artículo indica que estas pueden ser de 48 a 96 meses de prisión y multas de 100 a 1.000 SMLV. Por otro lado, el segundo artículo mencionado habla de 36 a 72 meses de prisión.

- En la cuarta clausula en el ítem 3 puede estar incurriendo en el artículo 269F el cual habla de la violación de datos personales, donde se habla de la obtención de datos y esto puede incurrir en penas de prisión de 48 a 96 meses y una multa de 100 a 1.000 SMLV. En el ítem 6 de la presente clausula también se encuentra relacionada con el articulo mencionado con anterioridad.

- En la octava clausula, puede estar incurriendo en el artículo 269F el cual habla de la violación de datos personales, donde se habla del aprovechamiento propio o de un tercero de datos y esto puede incurrir en penas de prisión de 48 a 96 meses y una multa de 100 a 1.000 SMLV.

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

Analizando la pregunta y teniendo en cuenta el código de ética profesional, no aceptaría trabajar con la organización HackerHouse, debido a que si encuentro procesos ilegales en el acuerdo confidencial estaría infringiendo en distintos artículos los cuales se encuentran enfocados en deberes y prohibiciones como profesional. Por lado, estaría arriesgando mi tarjeta profesional, siendo esta suspendida o en un peor caso la cancelación de esta.

Teniendo en cuenta lo anteriormente mencionado también estaría incurriendo en distintas faltas relacionadas con la ley 1273 del 2009, por este tipo de situaciones no aceptaría ningún tipo de acto ilegal relacionado con el acuerdo de confidencialidad. El monto económico es muy atractivo, pero teniendo en cuenta todos estos aspectos no sería ético y profesional aceptar los términos planteados.

4. Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.

Realizando un breve resumen de la noticia la cual fue publicada en diciembre del 2022, la cual tiene como título o encabezado: EMP, Sanitas y Afina continúan en jaque por ataque cibernético contra sus sistemas.

Estas organizaciones las cuales pertenecen al mismo grupo empresarial fueron atacadas de manera simultánea donde logran expresar que sufrieron ataques a sus sistemas por más de 27 días, los datos más relevantes dentro de los inconvenientes y falencias encontradas por el personal forense y legal el cual fue contratado para solventar esta situación, se encontró lo siguiente:

- Control de las operaciones por parte de los ciberdelincuentes.
- Afectaciones a sus infraestructura (Data center).
- Afectaciones de sus distintos aplicativos(pagos, citas, entre otros).
- Robo y divulgación de información, esto tanto de usuarios, colaboradores, proveedores, entre otros.
- Afectación a servicios y aplicativos web
- Ataques de Ransoware BlackCat.
- Posible atacante fue el grupo conocido como RansomHouse.

Teniendo en cuenta lo mencionado con anterioridad se logra ver que estas organizaciones fueron expuestas y atacadas de distintas formas. Por otro lado, los ciberdelincuentes incurrieron en distintos delitos los cuales pueden incurrir en distintas penas o multas a continuación, se mencionará algunos de los artículos que se pueden considerar para dictaminar las sanciones.

- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269E: Uso de software malicioso.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

A continuación, se presenta la construcción del informe con el cual se busca entregar pautas y recomendaciones para garantizar la seguridad de la información, procesos y servicios de organizaciones tecnológicas frente a distintos ataques intrusivos. Esto se hace con fin de poder generar conciencia en estas organizaciones ya que son unas de las más expuestas hoy en día respecto al tema de ataques intrusivos.

EJECUCIÓN PRUEBAS DE INTRUSIÓN

Metodología.

El diseño metodológico se basa en un enfoque mixto el cual permite trabajar con datos cuantitativos y cualitativos, por medio de ello nos permite analizar de mejor manera cada uno de los objetivos propuestos para detectar, y saber qué fue lo que causo la intrusión que fue relatada en cada uno de los anexos suministrados y a su vez eliminar o mitigar este tipo de amenazas. Esto con ayuda del Red Team y Blue Team.

Alcance.

Se busca por medio de esta metodología tener un enfoque seguro y de calidad al momento de realizarlas pruebas de intrusión relacionadas por el Red Team, teniendo este enfoque se garantizará la normal operación de los servicios y procesos de la organización en cuestión.

Aspectos para tener en cuenta:

- Permite realizar análisis de seguridad en los sistemas a intervenir.
- Establece parámetros para realizar evaluación y monitoreo.
- Define proceso detallado para realizar pruebas de penetración.
- Considera áreas de alcance.
- Se dará de forma detallada las técnicas utilizadas para cada prueba.
- Presenta análisis y evaluación de riesgos.

- Establece valores y niveles de evaluación de riesgos.
- Clasifica vulnerabilidades encontradas.
- Realiza estimado de impacto.

Diseño de ataques y pruebas de intrusión por parte del Red Team.

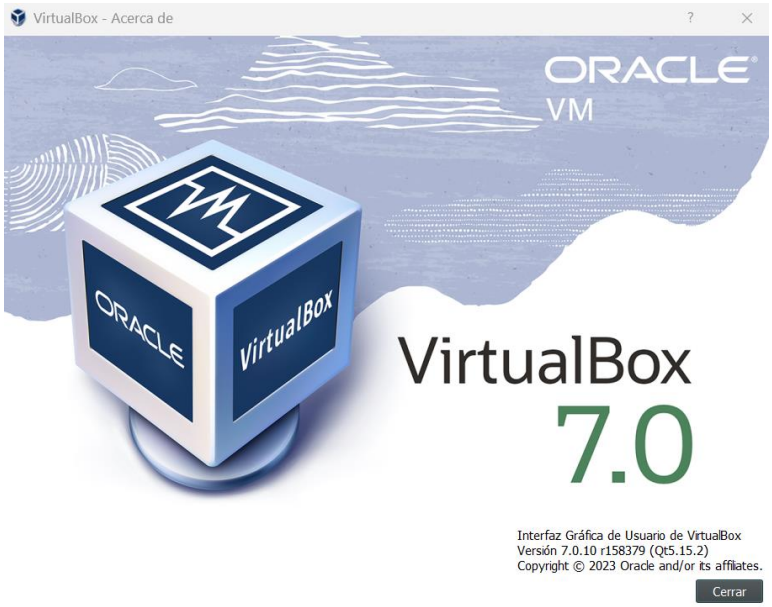
Es importante establecer para el diseño de los ataques y pruebas de intrusión el paso a paso para su respectiva implementación, esto garantizará la efectividad de las pruebas, ataques. Esto con el fin de no afectar servicios, procesos de la organización a la cual se le está realizando la intervención.

Ambiente controlado.

Antes de realizar cualquier tipo de prueba de intrusión de debe de tener en cuenta para que se va a realizar y cuál es su fin, es importante contar con un ambiente controlado para realizar este tipo de pruebas las cuales son intrusivas y pueden causar daños a la organización a la cual se está realzando este tipo de prácticas. Por otro lado, siembre será importante garantizar la operatividad de los servicios de la organización en todo momento.

VirtualBox: Este tipo de software permite virtualizar cualquier sistema operativo, por medio de imágenes ISO, por medio de este podemos contar con distintas maquinas corriendo al mismo tiempo solo utilizando un equipo físico.

Figura 19. VirtualBox 7.0.10.



Fuente: Propia.

Teniendo en funcionamiento el ambiente controlado o virtualizador, es importante saber qué tipo de pruebas de intrusión se van a realizar esto debido a que existen varias opciones, en este caso específico se realizara el uso de la siguiente:

Caja blanca: Este tipo auditoria es aquella donde el auditor conoce todos los aspectos de la organización: infraestructura, contraseñas, IPs, entre otros. Se realiza un análisis de forma integral. Teniendo en cuenta esta información el auditor puede realizar pruebas enfocadas y de forma certera donde podrá encontrar de forma directa la vulnerabilidad. Este tipo de intrusión es utilizado ya que lo realiza el personal del Red Team de la organización.

Procedimiento pruebas de intrusión.

Este procedimiento consiste en la práctica de vulnerar cualquier sistema, en este caso específico la afectación, acceso o sustracción de información a la máquina de la víctima. Se dispone de las siguientes fases las cuales permitirán realizar la ejecución de estas pruebas de la mejor manera por parte del Red Team.

Fase 1 Recolección de información: Esta fase inicial consiste en la recolección de la información relacionada con la organización, esto puedo incluir cualquier tipo de información relacionada con cualquier departamento de la organización, esta

información se puede encontrar tanto en buscadores de internet o aplicando cualquier tipo de practica relacionada con ingeniería social como una de las más efectivas.

Fase 2 Modelos de amenazas: Teniendo en cuenta la información recolectada anteriormente, nos depondremos a pensar como un atacante, métodos y estrategias que pueda utilizar para realizar pruebas de intrusión.

Fase 3 Análisis y explotación de vulnerabilidades: En esta fase se hace uso de herramientas de detección de vulnerabilidades enfocadas en toda la información recolectada con anterioridad por otro lado tomando en cuenta las estrategias y métodos planteados con anterioridad, esta fase permite contar con la creatividad del pentester. Por otro lado, se busca tener acceso a los sistemas, equipos, servidores. Para ello se ejecutan los exploit contra las vulnerabilidades encontradas con anterioridad, obteniendo acceso al sistema se buscará por medio de credenciales ganar acceso a aplicativos, equipos y servidores.

Fase 4 Post-Explotación: Teniendo el acceso como tal al sistema, lo que se va a realizar ahora es buscar el mayor acceso posible dentro del sistema, permitiéndonos llegar a información crítica y servicios, procesos de la organización los cuales sean de gran importancia para esta.

Fase 5 Presentación informes: Por último, se le entregará a la organización y a los entes involucrados un informe donde se verá consignando las pruebas que se realizaron, vulnerabilidades encontradas y recomendaciones donde se busca mitigar y eliminar estas vulnerabilidades. Por otro lado, se entregará un informe técnico respecto al pentesting.[1]

Caso de estudio.

Teniendo en cuenta el anexo 4 – escenario 3. En resumen, en la organización HackerHouse encontró que un equipo de su propiedad fue vulnerado de alguna manera, esto es confirmado con el personal que hace uso de este equipo, donde expresa que en el escritorio del dispositivo tenía un archivo con extensión txt el cual contenía datos relevantes como lo son: nombre del estudian, código, fecha y actividad. De igual forma este trabajador expresa que también había recibo un archivo por medio de WhatsApp con la extensión exe, el descarga el archivo y procese a ejecutarlo.

[1] GUÍA DE ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web [Anónimo]. Redalyc.org [página web]. (2022). [Consultado el 1, diciembre, 2022]. Disponible en Internet: <https://www.redalyc.org/articulo.oa?id=512251501005>.

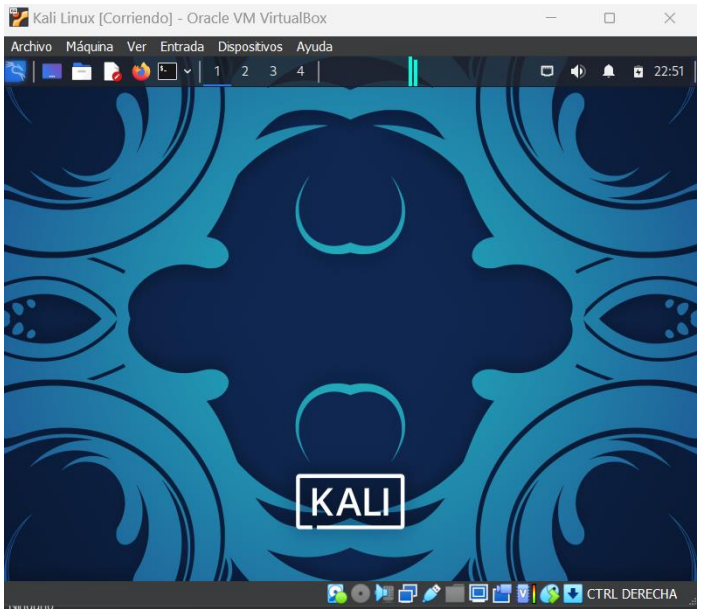
Paso 1: Acondicionamiento del escenario.

En este paso en el software de virtualización VirtualBox, se realiza la instalación de la maquina víctima de SO Windows 10, la máquina del Red Team será Kali Linux.

Teniendo en cuenta las herramientas de tipo software utilizas por el Red Team para realizar pruebas de intrusión dentro de un sistema a continuación, se presenta una de las herramientas más eficientes al momento de realizar este tipo de pruebas:

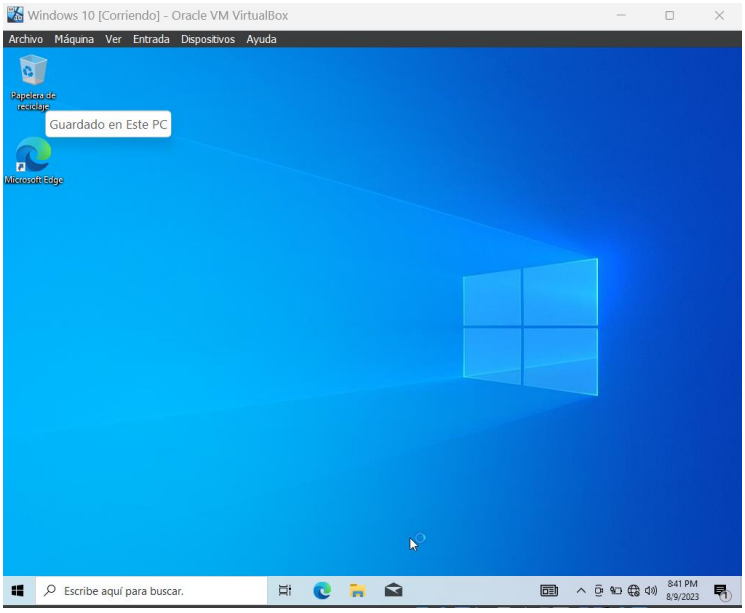
Para las pruebas de intrusión se hace uso de Kali Linux es un sistema operativo de código abierto utilizando para realizar pruebas de intrusión, en este podrá encontrar distintos exploits y herramientas las cuales permitirán al Red Team realizar todo tipo de tarea relacionado con pruebas de intrusión. Por otro lado, permite recolectar información, analizar vulnerabilidades, analizar aplicaciones web, valoración de datos, ataques de contraseñas, análisis forense, ingeniería social, entre otros.

Figura 20. Kali Linux.



Fuente: Propia.

Figura 21. Windows 10.

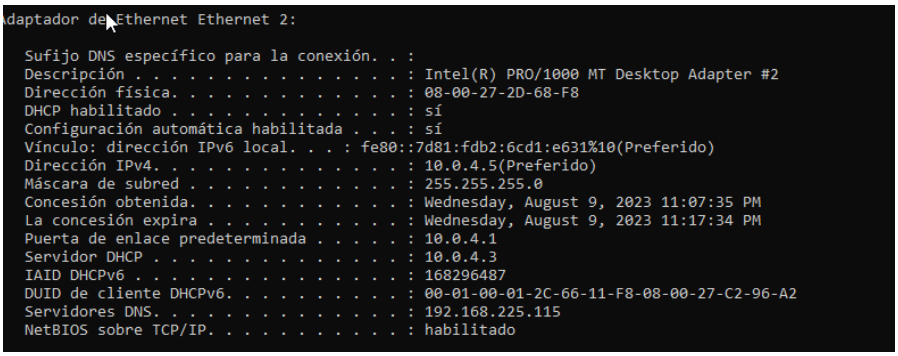


Fuente: Propia.

Paso 2: Verificación de comunicación.

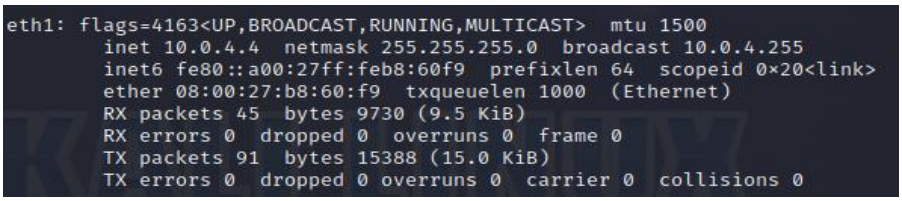
Ya teniendo el escenario organizado, se dispone a verificar la comunicación entre las dos máquinas, ya que por medio de lo descrito en el anexo anteriormente comentado se indica que el Payload o archivo que descarga la víctima fue enviado por un compañero. Esto es un indicador que la conexión entre las dos máquinas fue en la misma red.

Figura 22. IP Windows 10.



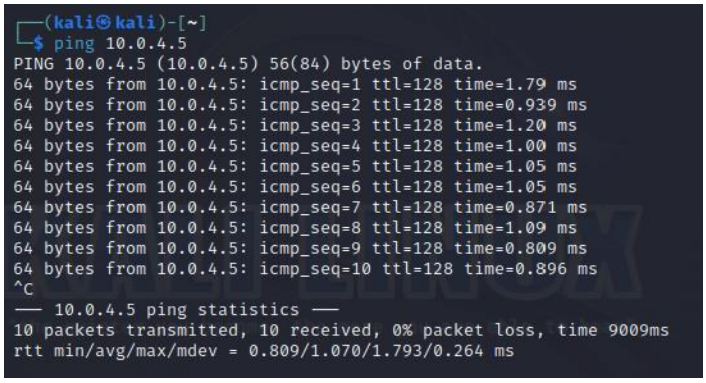
Fuente: Propia.

Figura 23. IP Kali Linux.



Fuente: Propia.

Figura 24. Ping desde Kali Linux a Windows 10.



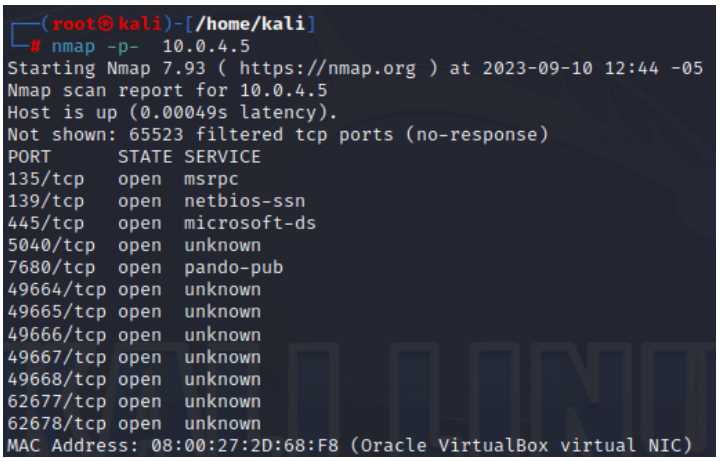
Fuente: Propia.

Con el comando ping más la dirección IP de la máquina de la víctima se está verificado que allá comunicación hacia esta.

Paso 3: Análisis de puertos con nmap.

El uso de nmap este tipo de herramienta permitió analizar que puertos y que tipo de servicios están corriendo dentro de la maquina víctima. Con el comando nmap -p- 10.0.4.5 lo que se quiere es que haga un escaneo de todos los puertos abiertos.

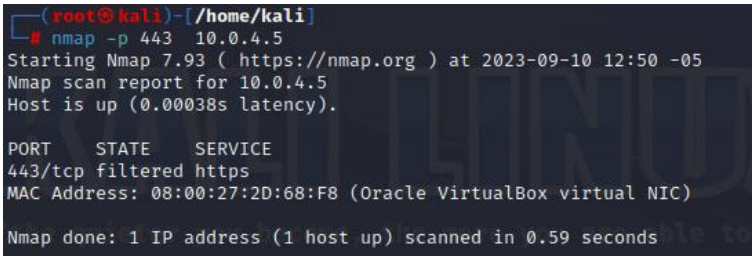
Figura 25. Escaneo puertos maquina víctima.



Fuente: Propia.

Con el siguiente comando nmap -p 443 10.0.4.5 lo que se quiere hacer es que haga un escaneo especifico en el puerto 443, el cual es que se va a utilizar para ingresar a la máquina de la víctima.

Figura 26. Escaneo puerto 443 maquina víctima.

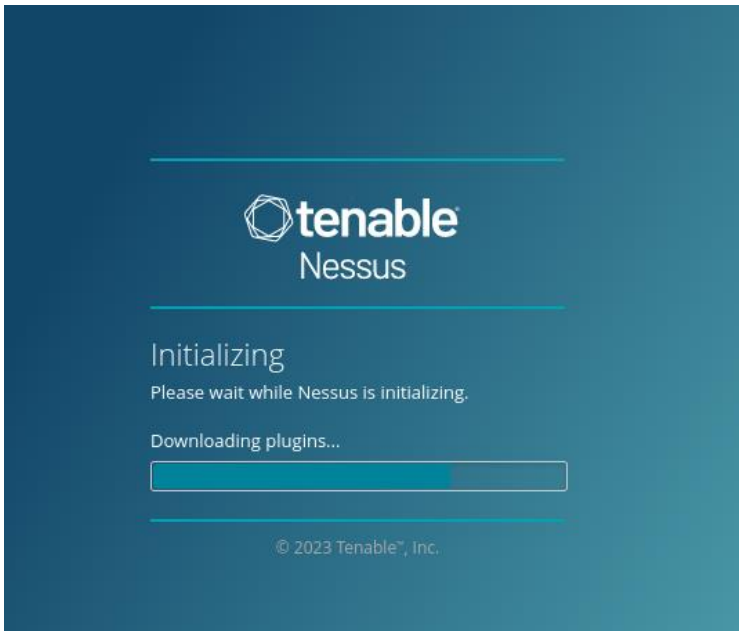


Fuente: Propia.

Paso 4: Análisis de vulnerabilidades con Nessus.

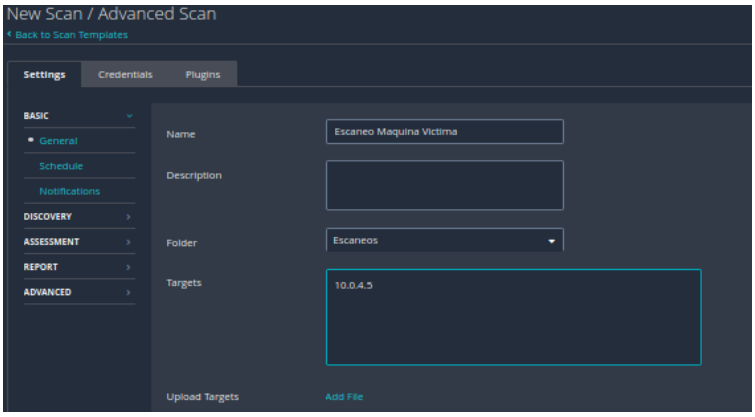
Por otro lado, con ayuda de una herramienta de escaneo del vulnerabilidades se validará que tipo de vulnerabilidades puede tener la máquina de la víctima, en este caso se hará uso de Nessus.

Figura 27. Nessus.



Fuente: Propia.

Figura 28. Creación Escaneo.

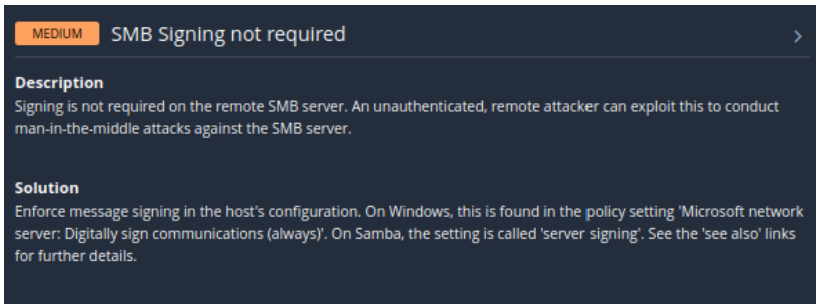


Fuente: Propia.

Ya teniendo Nessus instalado en nuestra maquina Kali Linux, se dispone a crear un escaneo esto con el fin de verificar que vulnerabilidades pueden estar afectando a la maquina víctima.

Al termina el escaneo se logra evidenciar que hay un inconveniente con el servidor SMB de forma remota, este indica que hay la probabilidad que un atacante se pueda conectar de forma remota y realice ataques al mismo.

Figura 29. Vulnerabilidad más relevante.



Fuente: Propia.

Fuente: Propia.

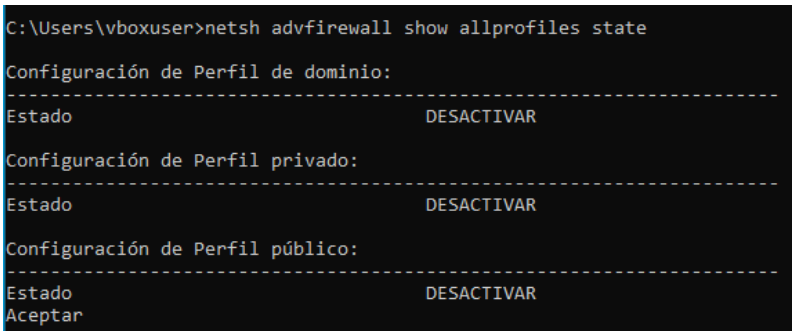
Otros hallazgos:

- El dispositivo admite conexiones remotas.
- Por medio del puerto tcp 135 está permitiendo realizar conexiones remotas.
- Se logro obtener datos del sistema operativo por medio de los puertos 139,443,445.
- Se evidencia falencia en las firma de SMB para conexiones remotas.

Paso 5: Creación Payload.

Se debe de tener en cuenta que en la máquina de la víctima el estado del firewall debe estar inactivo para el desarrollo del ataque que se va a llevar a cabo.

Figura 30. Estado firewall maquina víctima.

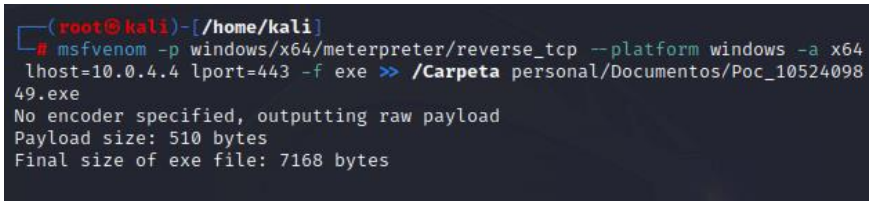


Fuente: Propia.

Después de validar la información anterior, se procede a crear el Payload por medio de la herramienta Msfvenom, esto se realiza desde la máquina del atacante en este

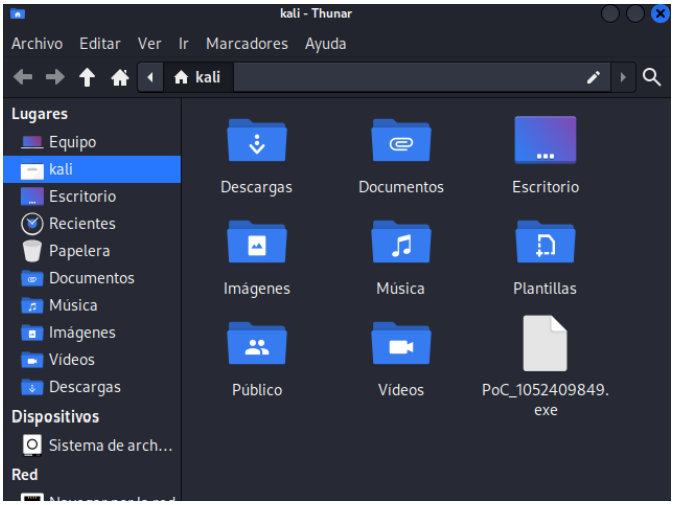
caso utilizando Kali Linux, importante activar el super usuario esto se hace haciendo uso del comando sudo su.

Figura 31. Creación Payload.



Fuente: Propia.

Figura 32. Ubicación Payload.

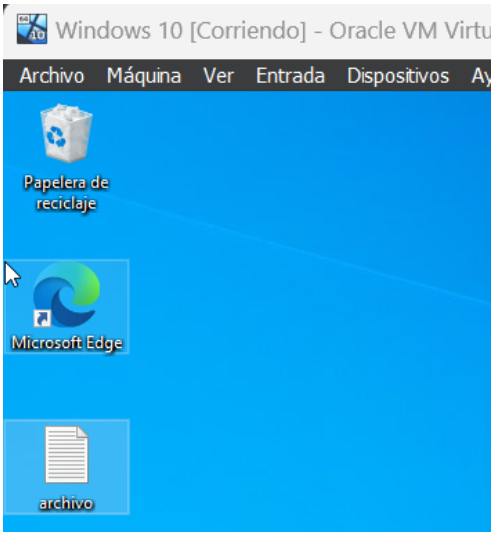


Fuente: Propia.

Paso 6: Interacción usuario con el Payload.

A continuación, se observa cómo fue la interacción de la víctima con el archivo .exe o el llamado Payload.

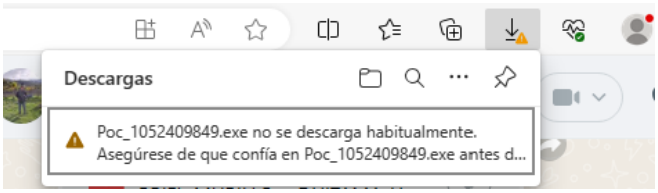
Figura 33. Escritorio maquina víctima, antes del ataque.



Fuente: Propia.

En la siguiente figura, se puede evidencia como se realiza el proceso de descarga del archivo PoC_1052409849.exe.

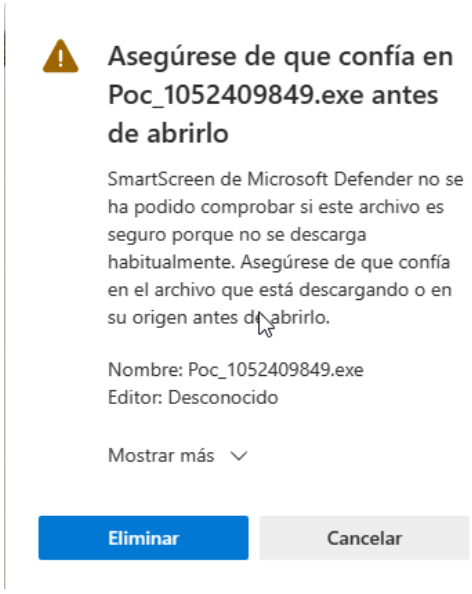
Figura 34. Descarga del archivo exe.



Fuente: Propia.

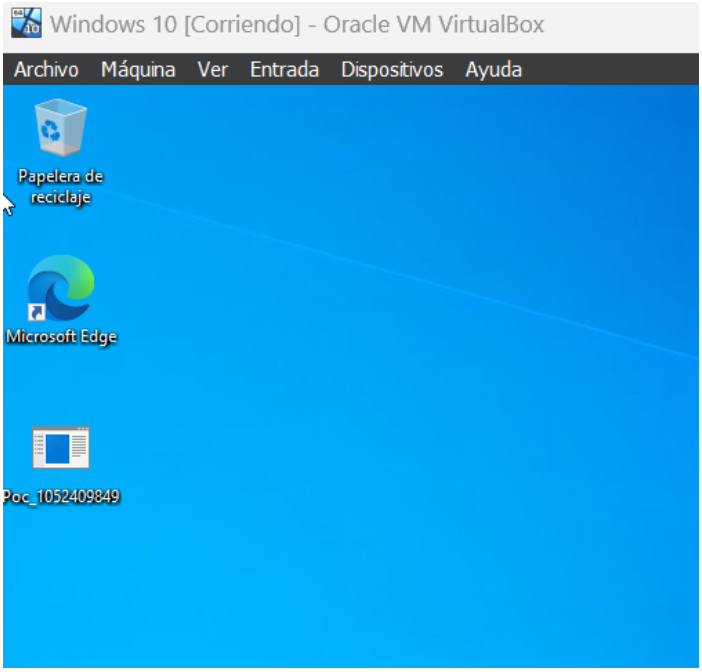
Al momento de realizar la descarga, Windows pregunta que, si desea realizar La descarga, el trabajador hace caso omiso a esta advertencia debido a que el archivo que le suministraron procede de un compañero de labor.

Figura 35.Advertencia de descarga.



Fuente: Propia.

Figura 36. Archivo .exe en la maquina víctima.



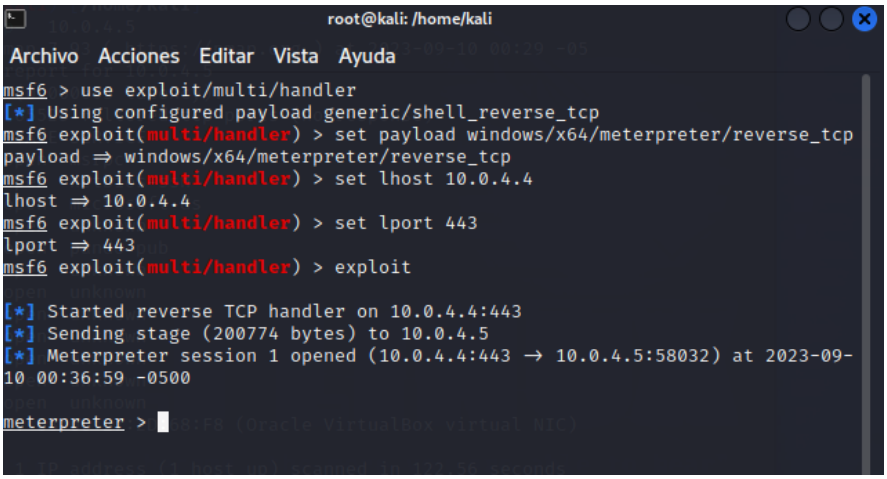
Fuente: Propia.

Paso 7: Ejecución del Payload.

A continuación, se procede a realizar la ejecución del Payload que se creó previamente, lo primero que se realiza es ingresar a la consola de Msfvenom, esto haciendo uso del comando msfconsole.

Ya adentro de la consola, se indica el tipo de payload que se quiere utilizar que en este caso es el de meterpreter/reverse_tcp este exploit se utiliza para tener acceso remoto a la máquina de la víctima, esto con el fin de sustraer, modificar o eliminar información. Con el comando set lhost y lport le estamos indicando que nos deje conectar por el puerto 443 y que la comunicación sea a la IP del atacante.

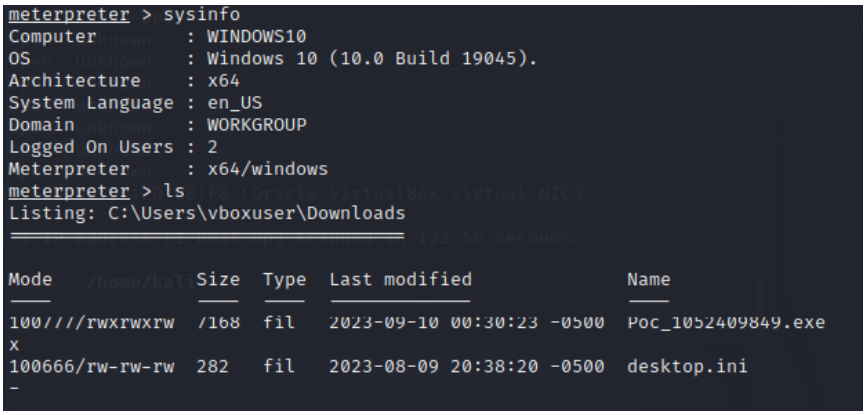
Figura 37. Ejecución Payload.



Fuente: Propia.

Con el comando sysinfo, lo que se logra ver es toda la información que tiene el sistema operativo como lo es: arquitectura, nombre del equipo, SO y su respectivo dominio.

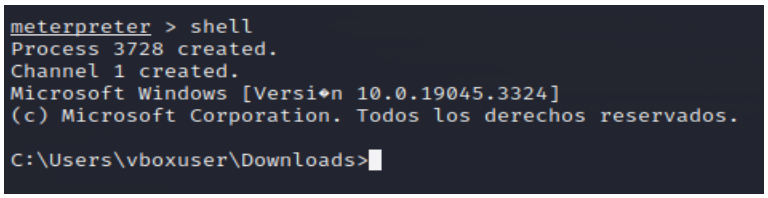
Figura 38. Comando sysinfo.



Fuente: Propia.

Ya teniendo acceso a la máquina de la víctima, lo que se dispone a realizar es ingresar y borrar la información en este caso el archivo.txt que se encuentra en el escritorio, esto se realizará haciendo uso del siguiente comando Shell este comando permite ingresar a la terminal de comandos de la máquina que se está atacando.

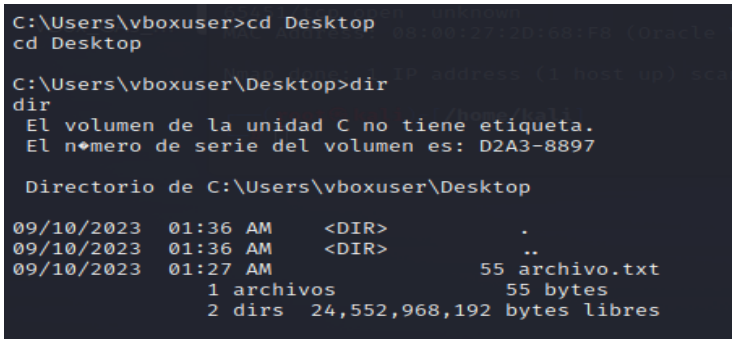
Figura 39. Comando Shell.



Fuente: Propia.

En este paso se ingresó al escritorio y se ubicó el archivo.txt el cual se quiere eliminar, esto se realiza haciendo uso del comando del y el nombre del archivo.

Figura 40. Ubicación archivo .txt



Fuente: Propia.

Figura 41. Comando del.

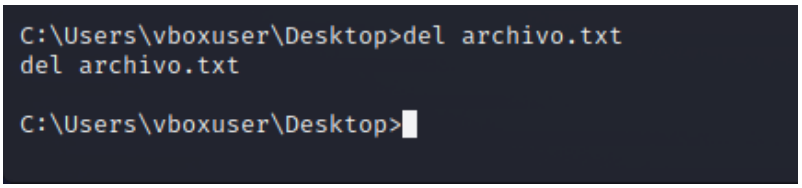
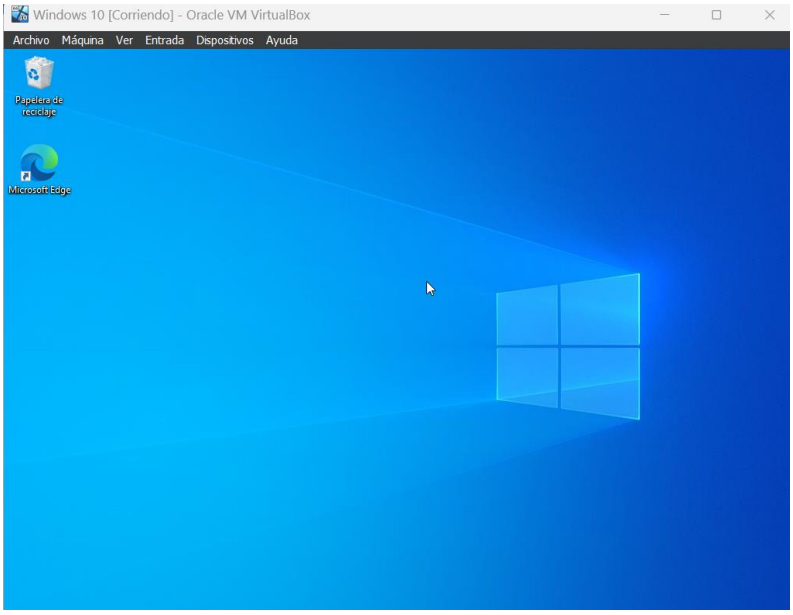


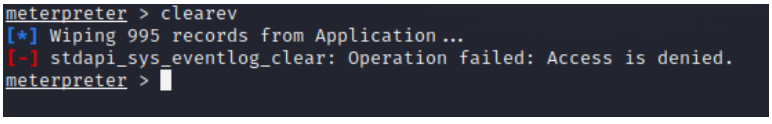
Figura 42. Escritorio maquina víctima, después del ataque.



Fuente: Propia.

Después con el comando clearev, se busca eliminar los log de eventos de Windows, esto con el fin de no dejar huella del ataque.

Figura 43. Comando Clearev.



Fuente: Propia.

CONTENCIÓN DE ATAQUES INFORMÁTICOS

Aseguramiento, recomendaciones para la mejora de la seguridad de la información.

A continuación, se presenta la construcción del informe con el cual se busca entregar pautas y recomendaciones para garantizar la seguridad de la información, procesos y servicios de organizaciones tecnológicas frente a distintos ataques intrusivos. Esto se hace con fin de poder generar conciencia en estas organizaciones ya que son unas de las más expuestas hoy en día respecto al tema de ataques intrusivos.

Visión general.

La visión general seria nuestro primer paso para realizar la entrega del informe, esto nos permite ver en que postura se encuentra la organización en el aspecto de ciberseguridad. Teniendo esto en claro, se analizará cada componente, proceso o plan que esté relacionado con este tema, a continuación, se indicara que aspectos son relevantes para tener un análisis concreto y efectivo:

- Activos de la organización.
- Vulnerabilidades.
- Amenazas.
- Procedimientos.

Esto nos ayuda a diligenciar el siguiente formato el cual permitirá realizar un checklist y así poder evaluar la situación de la organización.

Figura 44. Checklist.

LOGOTIPO	**GESTIÓN TI, SEGURIDAD DE LA INFROMACIÓN.** Check List para actividades.

1. GENERALIDADES										
Fecha:			Hora Inicio:			Hora Terminación:				
Centro de Trabajo:								N° OT/Aviso:		
Área de Trabajo / Equipo a Intervenir:										
Herramienta / Equipo a Usar:										
Personal Autorizado para Trabajar en el Área:										
Descripción Trabajo a Realizar:										
Evaluación Matriz de riesgos:		MA		A		M		B		MB
Existen otros permisos de trabajo abiertos?								SÍ		NO
Cuáles?										

2. VERIFICACIÓN ACTIVOS							
	ESTADO				**ESTADO**		
VERIFICACIÓN	**B**	**M**	**N/A**	**VERIFICACIÓN**	**B**	**M**	**N/A**
Servidor Web				Planta IP			
Servidor DNS				Teléfono			
Servidor de Correo				Computador			
Directorio Activo				CCTV			
Firewall				Office 365			
Router Principal				Antivirus			
Router Inalámbrico				Otros:			

	VALORACIÓN RIESGO						**VALORACIÓN RIESGO**				
AMENAZAS	**MA**	**A**	**M**	**B**	**MB**	**VULNERABILIDADES**	**MA**	**A**	**M**	**B**	**MB**

CONTESTE LAS SIGUIENTES PREGUNTAS	**SI**	**NO**	**N/A**
Se debe de pedir ventana de mantenimiento para intervenir algún equipo ?			
Se debe de realizar copias de seguridad al equipo a intervenir ?			
Se realiza actualización de software en el equipo a intervenir ?			
Se realiza algún tipo de cambio físico respecto a los equipos ?			

En caso que se requiera diligencie los siguientes recuadros:	
RECOMENDACIONES:	
OBSERVACIONES ESPECIALES:	

FUNCIONARIO RESPONSABLE DEL TRABAJO	
NOMBRE Y APELLIDOS:	FIRMA:

Fuente: Propia.

Evaluación de riesgos.

Con la evaluación de riesgos se busca identificar el nivel de impacto y criticidad que pueda afectar a cualquier proceso, activo, información. Esto con el fin de garantizar la integridad, disponibilidad de estos. Por otro lado, la evaluación de riesgos nos permite tener en claridad en que se podría estar fallando y así mismo poder entregar pautas y recomendaciones para mitigar o eliminar estos riesgos.

Identificación de activos.

Para determinar la evaluación de riesgos es necesario saber con qué activos cuenta la organización y a partir de ahí identificar riegos, amenazas y vulnerabilidades las cuales puedan comprometer la seguridad de la información de la organización. En la siguiente tabla se presenta algunos de los activos más comunes.

En la siguiente tabla se podrá establecer algunas de las amenazas y vulnerabilidades a las cuales se encuentran expuestos cada uno de los activos de la organización, estos activos pueden variar debido a que todas las organizaciones no cuentan con los mismos activos, esta tabla es algo generalizada.

Tabla 1. Identificación de activos.

Activo	Tipo	Encargado	Amenazas	Vulnerabilidades
Servidor Web	Software	Especialista en ciberseguridad	Ataques de inyección SQL. Programación Cross-Site (o XSS). Ataques de fuerza bruta. Ataques DoS/DDoS.	Puede ser vulnerable debido a muchas veces la administración por terceros. Fuga de información. Desconexiones frecuentes. Problemas en aplicativos.
Office 365	Software	Técnico segundo nivel	Código abierto. Suplantación de identidad. Acceso no autorizado.	Vulnerabilidades XSS. Problemas de autenticación. Fuga de la información.
Firewall	Hardware	Especialista en ciberseguridad	Acceso no autorizado. Suplantación de identidad.	No puede proteger a la red de ataques cuyo tráfico no pase por este.

			Ataques de fuerza bruta.	No puede proteger de ataques internos.
Servidores físicos	Hardware	Especialista en ciberseguridad	Rodo de los equipos. Acceso no autorizado.	Fuga de la información. Modificación de información. Daños físicos.
Antivirus	Software	Técnico de primer nivel	Malware. Acceso no autorizado.	Inestabilidad. Problemas de software.
Control de acceso	Hardware y Software	Técnico de primer nivel	Acceso no autorizado. Ataques relacionados con ingeniería social.	Falla en el sistema de control del CCTV. Fuga de la información. Daños físicos.
Especialista en ciberseguridad	Personal	Director TI	Ataques relacionados con ingeniería social. Acceso no autorizado. Suplantación de identidad.	Fuga de la información. Personal no disponible.
Técnico de segundo nivel	Personal	Director TI	Ataques relacionados con ingeniería social.	Fuga de la información. Personal no disponible.

			Suplantación de identidad.	
Técnico de primer nivel	Personal	Director TI	Ataques relacionados con ingeniería social. Suplantación de identidad.	Fuga de la información. Personal no disponible.
Data Center	Locativo	Técnico de segundo nivel	Acceso no autorizado. Desastres locativos. Robo de equipos.	Fuga de la información. Daños físicos.

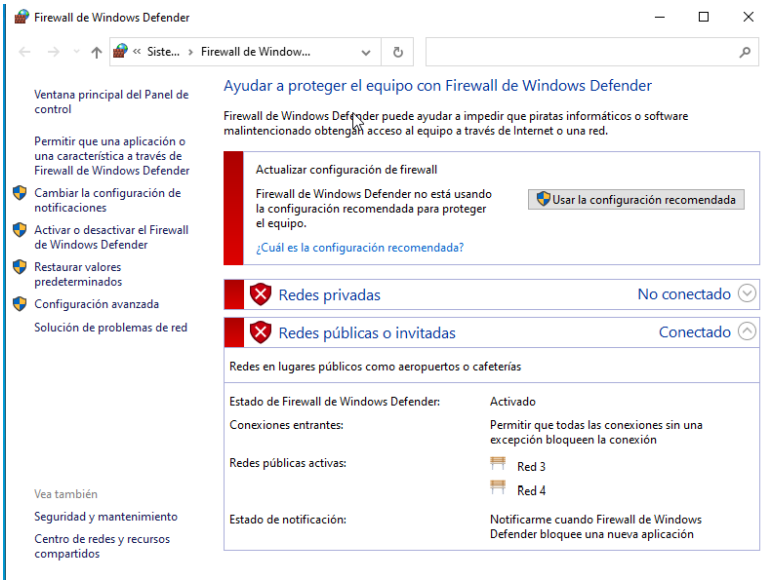
Fuente: Propia.

Aseguramiento maquina víctima.

Teniendo en cuenta las pruebas de intrusión realizadas por el Red Team y los hallazgos encontrados, se plantean estrategias para el aseguramiento de la red, infraestructura, activos, información, entre otros. Para lograr esto el Blue Team hará uso de una guía hardening.

Paso 1: Activar firewall de Windows.

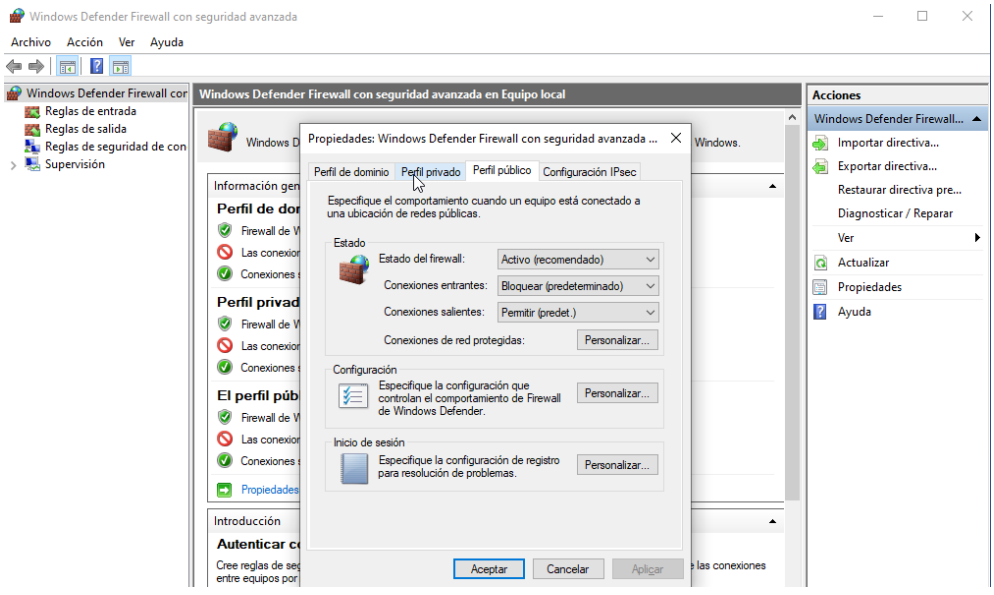
Figura 45. Firewall desactivado.



Fuente: Propia.

Se bloquea las conexiones entrantes en cada uno de los perfiles, esto con el fin de evitar conexiones no autorizadas al host.

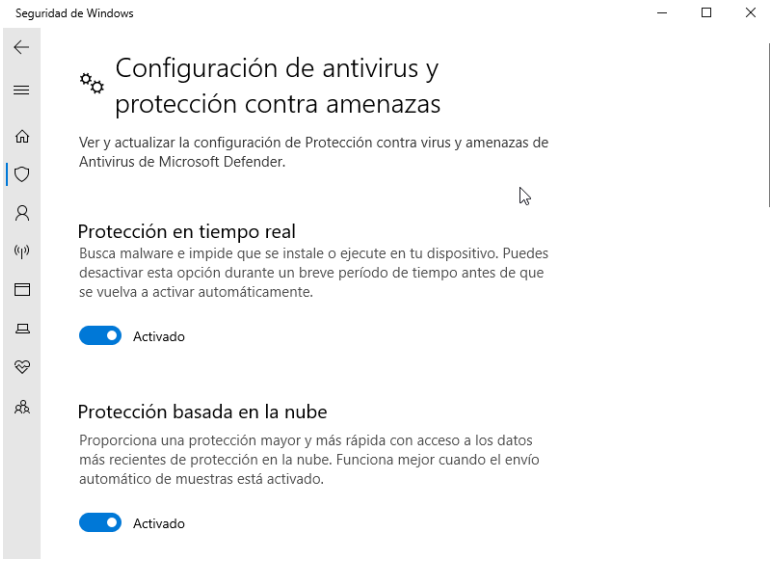
Figura 46. Configuración de perfiles firewall.



Fuente: Propia.

Paso 2: Activar antivirus de Windows o instalar uno con licencia.

Figura 47. Antivirus activado.

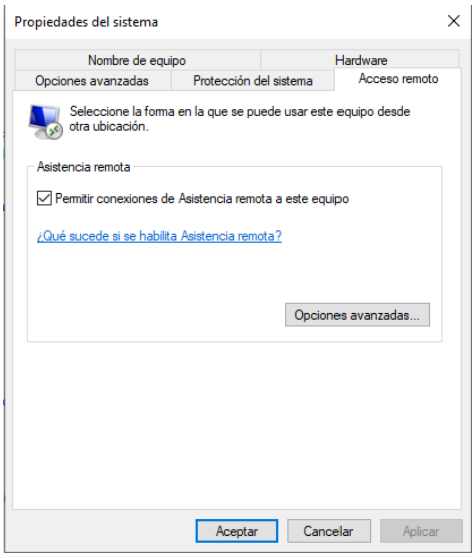


Fuente: Propia.

En este caso el antivirus de Windows permite dar avisos de software malicioso que se instala o es descargado dentro del sistema operativo, esto con el fin de dar aviso de esta actividad sospechosa.

Paso 3: Restringir el acceso remoto.

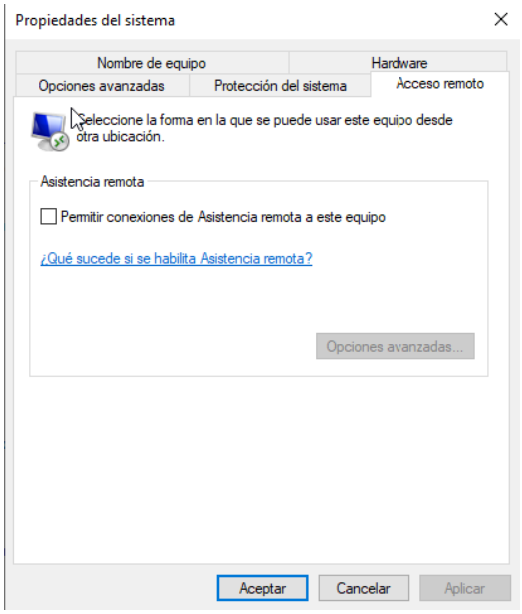
Figura 48. Acceso remoto activo.



Fuente: Propia.

Como se puede observar en la figura anterior la asistencia remota se encuentra activa, ahora lo que se procede es a deshabilitar.

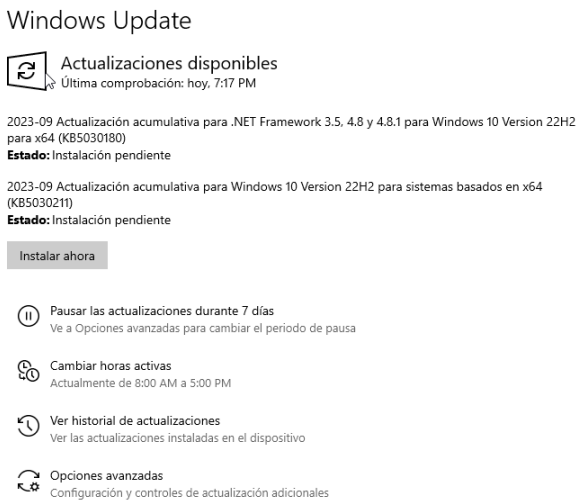
Figura 49. Acceso remoto desactivado.



Fuente: Propia.

Paso 4: Tener activas las actualizaciones de Windows.

Figura 50. Windows Update.

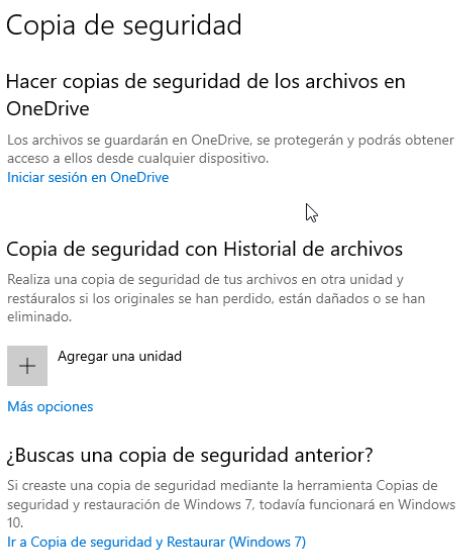


Fuente: Propia.

Es importante siempre tener actualizado el sistema operativo ya que en muchas de estas actualizaciones traen parches de seguridad los cuales permitirán proteger al equipo.

Paso 5: Generar copias de seguridad.

Figura 51. Copia de seguridad.

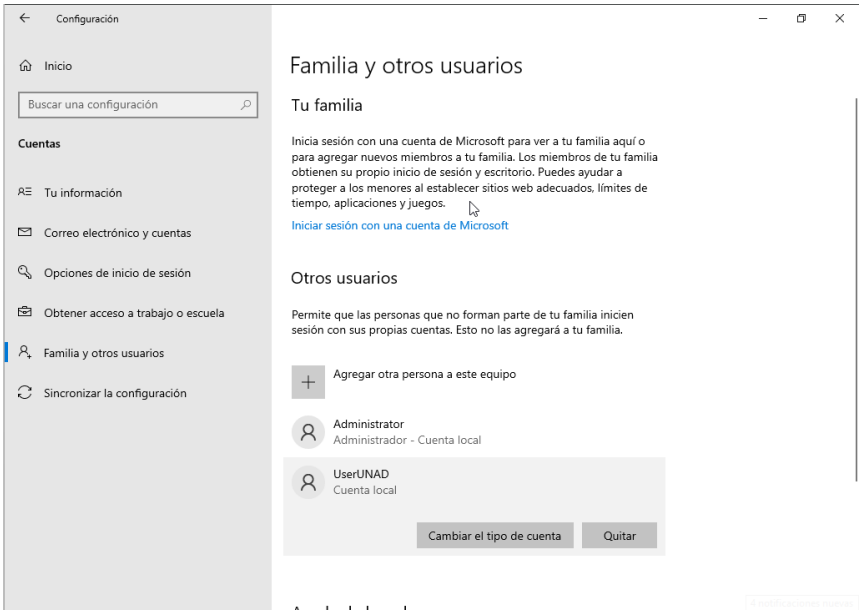


Fuente: Propia.

Es importante siempre contar con una copia de seguridad ya que, si el equipo es infectado, sufre un daño físico o la información es eliminada. Se contará con un respaldo de esta. Windows tiene la facilidad de realizar estas copias por medio de OneDrive o agregar un disco externo para realizar las copias.

Paso 6: Cuentas de usuario.

Figura 52. Cuentas de usuario.



Fuente: Propia.

Es importante configurar los perfiles de las cuentas de usuario, esto con el fin de dar los permisos necesarios a los usuario y evitar que instalen o ejecuten algún software malicioso.

Adicionales:

- Implementación de BitLocker.
- Política de cambio de contraseñas de forma periódica.
- Crear punto de restauración.
- Capacitación a personal de la organización sobre la importancia de la ciberseguridad.
- Implementación de IPS y IDS para el monitoreo en tiempo real de amenazas y vulnerabilidades.
- Bloqueo de puertos (USB) en los usuarios finales.
- Implementación y mejora de control de acceso (lógicos, físicos).
- Establecer reglas de conexión para los distintos puertos.

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

El Purple Team es el encargado del fortalecimiento de las labores de los dos equipos mencionados con anterioridad, esto con el fin de tener objetivos en común y a su vez mejorar la comunicación y labores conjuntas del Blue Team y Red Team, esta labor que hace el Purple Team es fundamental para cada proceso de la organización ya que, si todos los equipos trabajan en conjunto, la ciberseguridad dentro de las organizaciones no se verá afectada.

CONCLUSIONES

Teniendo en cuenta el desarrollo de cada una de las etapas propuestas durante el semanario, se logra concluir la importancia de cada uno de los equipos involucrados en la ciberseguridad de una organización, estos son el Red Team, Blue Team y Purple Team. Cada uno de ellos cumple una labor fundamental para garantizar la seguridad de la información y a su vez velar por el funcionamiento óptimo de servicios, procesos de la organización en cuestión, por eso es de gran importación la inversión, innovación de nuevas tecnologías.

Por otro lado, la alta gerencia debe estar involucrada en la creación de políticas de seguridad ya que respecto a las necesidades que tienen y con la infraestructura actual. De ahí parte el Blue Team para generar un plan o estrategia para el aseguramiento de la información, infraestructura, servicios y procesos de la organización.

Se puede concluir que la implementación del diseño para la ejecución de las pruebas de intrusión permite al Red Team y cualquier especialista que sea contrata por alguna de las organizaciones en cuestión, tener un manual o metodología el cual permitirá hacer pruebas de calidad, las cuales conllevan a la entrega de informes de calidad lo cual dará parte de tranquilidad a las partes involucradas. Por otro lado, la implementación y diseño de las pruebas de intrusión, es fundamental que las haga personal especialista en este tipo de ejecuciones, se debe de tener como referencia la metodología planteada con anterioridad para garantizar la operatividad de procesos y servicios de la organización.

RECOMENDACIONES

- Realizar análisis de vulnerabilidades, haciendo uso de herramientas de detección de vulnerabilidades las cuales tengan alta confiabilidad, evitado alguna afectación en la organización a intervenir. Por otro lado, el uso de estas herramientas por el Red Team, se recomienda realizarlas en un ambiente controlado antes de realizar las pruebas de penetración.

- Realizar pruebas de intrusión, es recomendable hacer uso de pruebas de caja gris, este tipo de pruebas permiten a la organización hacer entrega de información, pero no de toda así logrando tener confidencialidad y por otro lado permite al especialista ser más creativo al momento de realizar estas pruebas.

- Definir estrategias, metodologías para la realización de pruebas de intrusión esto con el fin de estandarizar cada proceso relacionado con la seguridad de la información, garantizando la disponibilidad de esta y a sus vez el funcionamiento óptimo de procesos y servicios dispuestos por la organización que se va a intervenir.

- Construir e implementar, formatos, guías de buenas prácticas relacionadas con ciberseguridad con el fin mitigar riesgos, amenazas y demás aspectos relacionados.

BIBLIOGRAFÍA

Cañón Parada del artículo Ataques informáticos, Ethical Hacking para la Universidad Piloto de Colombia, 2015, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://polux.unipiloto.edu.co:8080/00002427.pdf

COMMIX-COMMAND INJECTION Exploiter (Beginner's Guide) - Hacking Articles [Anónimo]. Hacking Articles [página web]. (2017). [Consultado el 8, marzo, 2023]. Disponible en Internet: <https://www.hackingarticles.in/commix-command-injection-exploiter-beginners-guide/>.

CIBERSEG1922. ¿Qué es Metasploit Framework y cómo funciona? | Ciberseguridad. Ciberseguridad [página web]. (13, diciembre, 2021). [Consultado el 8, agosto, 2023]. Disponible en Internet: <https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/#Usos_de_Metasploit>.

EL PASADO, el presente y el futuro de las pruebas de penetración - Ridge Security [Anónimo]. Ridge Security - Robotic Automated Penetration Testing [página web]. (2021). [Consultado el 7, noviembre, 2022]. Disponible en Internet: <https://ridgesecurity.ai/es/blog/el-pasado-el-presente-y-el-futuro-de-las-pruebas-de-penetracion>.

ESCANEANDO LA red con nmap en Kali Linux - Byte Mind [Anónimo]. Byte Mind [página web]. [Consultado el 19, marzo, 2023]. Disponible en Internet: <https://byte-mind.net/escaneando-la-red-con-nmap/#Instalacion-de-Nmap-en-Linux>.

GARCÍA, Leonardo. Gestión de la ciberseguridad con el estándar ISO. El Economista [página web]. (2019). Disponible en Internet: <https://www.eleconomista.com.mx/empresas/Gestion-de-la-ciberseguridad-con-el-estandar-ISO-20210908-0158.html>.

ISO27001 SEGURIDAD Información [Anónimo]. DNV [página web]. (2022). [Consultado el 1, octubre, 2022]. Disponible en Internet: <https://www.dnv.com/ar/services/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-3327>.

LEY 1273 de 2009 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. [Consultado el 16, agosto, 2023]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>.

PENTEST: LAS 10 mejores herramientas usadas en el mercado - OSTEC | Segurança digital de resultados [Anónimo]. OSTEC | Segurança digital de resultados [página web]. (2022). [Consultado el 17, noviembre, 2022]. Disponible en Internet: <https://ostec.blog/es/aprendizaje-descubrimiento/pentest-las-10-mejores-herramientas-usadas-en-el-mercado>.

PTES TECHNICAL Guidelines - The Penetration Testing Execution Standard [Anónimo]. The Penetration Testing Execution Standard [página web]. (2022). [Consultado el 17, noviembre, 2022]. Disponible en Internet: <http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines>.

QUÉ ES Red Team en Ciberseguridad | KeepCoding Tech School [Anónimo]. KeepCoding Tech School [página web]. [Consultado el 7, diciembre, 2022]. Disponible en Internet: <https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad.>.

QUÉ ES Purple Team en ciberseguridad [Anónimo]. KeepCoding Bootcamps [página web]. [Consultado el 17, septiembre, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/#Que_es_Purple_Team_en_ciberseguridad>.

QUÉ ES Meterpreter | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. [Consultado el 5, septiembre, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-meterpreter/>.

QUÉ ES un payload | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. [Consultado el 5, septiembre, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-un-payload/>.

RED and Blue Team Survey Reveals Positive Trends [Anónimo].2020, Exabeam [página web]. [Consultado el 6, diciembre, 2022]. Disponible en Internet: https://www.exabeam.com/security-operations-center/2020-red-and-blue-team-survey.

ANEXOS

Link video: https://www.youtube.com/watch?v=7OZztJy0Vv8