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

ELIZABETH GAMA MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO EN EQUIPOS ESTRATÉGICOS SOBRE CIBERSEGURIDAD RED-TEAM & BLUE-TEAM
GIRARDOT 2021

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

ELIZABETH GAMA MARTINEZ

Trabajo final para la aprobación del seminario especializado en equipos de ciberseguridad red team & blue team

DIRECTOR DE CURSO
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO EN EQUIPOS ESTRATÉGICOS SOBRE CIBERSEGURIDAD RED-TEAM & BLUE-TEAM
GIRARDOT 2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

Girardot, (10 de octubre de 2021)

Jurado

Girardot, (10 de octubre de 2021)

Primeramente, a Dios quien es la base de mi vida quien me ayuda a seguir adelante y quien me ha permitido cumplir mis sueños, a mi esposo quien me motiva y me anima a prepárame más y está siempre hay para mí al mi pedacito de vida a la razón por la que nos preparamos para darle lo mejor mi hijo hermoso y a mi familia que desde siempre me han apoyado y me han ayudado en todo.

Contenido

TABLA DE FIGURAS

LISTA DE TABLAS

RESUMEN

La informática y la tecnología son conceptos que no son estáticos son cambiantes y van avanzado es por esta razón las empresas y todo tipo de organizaciones deben estar actualizadas en cuanto a su infraestructura tecnológica pero supremamente importante sin dejar de lado la seguridad ya que existen amenazas y vulnerabilidades que avanzan de igual manera que la tecnología.

En este informe propondremos mecanismos de contención de ataques logrando mínimas las posibilidades de estos esto claro esta mediante el estudio de casos que se puedan o estén presentando en las empresas y organizaciones.

Debemos ser conscientes que un ataque informático aprovecha cualquier vulnerabilidad en el software, hardware inclusive en las personas que administran la información únicamente con el fin de beneficiarse y claro está perjudicando directamente a una organización.

Para este fin existen expertos equipos expertos y estratégicos en Ciberseguridad lod cuales son el RedTeam y Blue Team los cuales trabajan contra las actividades delictivas minimizando el campo de acción de estos ataques.

INTRODUCCIÓN

Cuando hablamos de seguridad informática hablamos del hecho de asegurarse que el sistema de información se mantenga de una manera correcta y se utilice de la manera que se decidió y controlar el acceso a la información restringiéndose a todo aquello que carezca de autorización ahora bien para lograr sus objetivos la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático.

La seguridad informática tiene técnicas o herramientas llamados mecanismos que se utilizan para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático y es de vital importancia que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.

El ámbito de la seguridad de información dentro de una organización cada día va cobrando más vigencia más importancia cada día la información se vuelve más preciada y es necesario protegerla de terceros que buscan otras finalidades como duplicación, alteración, robo, piratería abuso de confianza, beneficio propio o con otra intención etc.

Debemos como expertos en el área de la ciberseguridad estar al tanto de las últimas tendencias y procesos de seguridad, así como total conocimiento y actualización de las leyes y decretos que rigen esta área para así mismo desarrollar una labor correcta precisa y contundente con el fin de proteger la información.

Como se ha trabajado y hemos repetido constantemente el ámbito de la Ciberseguridad cobra más vigencia cada día, por esto debemos estar al tanto de las herramientas de contención de ataques y respondiendo rápidamente a las amenazas que se presenten y así minimizar de alguna manera el daño y que permita trabajar bajo ataque, teniendo en cuenta obviamente el presupuesto de la organización.

JUSTIFICACION

Es necesario aclarar algunos conceptos que se han considerado exclusivos de ciertas áreas de la informática pero que son un tema muy actual ya que las nuevas tecnologías traen condigo nuevos retos y nuevas formas de introducción a un sistema de información ya que si lo bueno lo de mejorar avanza el lado negativo de la historia como todo también avanza igual.

Este informe es supremamente importante ya que debido a estudios realizados y como ya lo hemos dicho los expertos en la materia los especialistas en ciberseguridad señalan que los ataques a la seguridad informática han evolucionado, por lo que los hackers están evolucionando también y han desarrollado software maliciosos cada vez más asombrosos y especializados para destapar las vulnerabilidades en los sistemas para hacer el respectivo robo de la información digital con el fin de lograr su objetivo.

Es por ello la gran importancia de elaborar planes de acción y estrategias para minimizar los riesgos, que las empresas refresquen su enfoque y establezcan las políticas y todo lo necesario para garantizar la seguridad informática.

Ahora bien, este tema no es solo de las empresas o de las personas en general es cuestión del estado también ya que se comenten crímenes a través de los sistemas también hay robo por lo que el estado genera leyes y decretos que nos ayudan a minimizar estos crímenes y genera planes de acción para mantener la paz y la información a salvo.

OBJETIVOS

OBJETIVO GENERAL:
Evaluar todos los aspectos relacionados a la ciberseguridad incluyendo el análisis según los roles y las diferencias entre los equipos RedTeam Y BlueTeam para definir las responsabilidades a ejecutar dentro de una organización.

OBJETIVOS ESPECIFICOS:

Evaluar las políticas y estándares de seguridad que rigen la ciberseguridad para poder implementarlas en las organizaciones y actuar como profesionales de ética y de bien.

Evaluar y acoplar las acciones de los equipos Red Team & Blue Team de una organizaciónen siempre bajo el marco de los criterios éticos y legales.

Buscar y evaluar las vulnerabilidades en un sistema informático a partir del uso demetodologías y técnicas de intrusión.

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en toda la infraestructura TI.

1. ETAPA CONCEPTOS EQUIPOS DE SEGURIDAD

1.1 MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMATICOS Y TRATAMIENTO DE DATOS PERSONALES.

Desde el inicio de los tiempos la prioridad de todos es proteger con celosía la información, nuestros datos y comunicación con otros y en Colombia no es la excepción y para protegerla el país ha tomado una serie de medidas que nos ayudan a esa labor.

En el código penal colombiano se estipula se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos ahora bien estos se preservan íntegramente en los sistemas que usan las tecnologías de la información.

Aunque hay un sin número de leyes y decretos que regulan dicho tema una de las más importantes es la ley 1373 de 2009 y esta viene desde 20 años atrás a través del decreto 1360 de 1989 en el cual se evidencia la reglamentación de la inscripción del soporte lógico que es más conocido como software en el registro nacional de derechos de autor.

Los principios de implementación de la seguridad de la información fueron alrededor de los años 1980 -1989 en el transcurso de este periodo se crearon 3 leyes con el fin de reglamentar el código penal que necesitaba para el estado colombiano se necesitó de reglamentar con urgencia ya que se empiezan a incluir en el mercado las nuevas tecnologías y el internet.

Otra de las leyes más trascendentales en este ámbito es la promulgada en el año 1982 en el cual se pudo establecer mecanismos de protección a los derechos de autor en Colombia, pero se notaron algunos vacíos legales que como fue mencionado anteriormente tuvo que requerirse de tres leyes de reglamentación dos reglamentarios y uno modificatorio con el fin de tener las herramientas necesarias para la inminente incursión de la tecnología.

Mas adelante entonces el gobierno nacional de Colombia ya dos años adelante empieza a tomar acciones de protección de blindaje donde se dicta la ley 23 de 1982 la cual protegía los derechos de autor en Colombia pero que realmente significa un avance

increíble y necesario en la protección de la información recordemos que la información también es un bien muy preciado hoy en día.

Ya para el año 1989 a través de la ley 72 empezamos ya a notar los principios y nuevos conceptos en el ámbito de las telecomunicaciones y a su vez el régimen de concesión de servicios.

Ya para los años 1990 y 1999 se empezó en forma la formolización de la constitución política de Colombia estableciendo los derechos y deberes del pueblo colombiano sin distinción alguna donde se empezaron a implementar en cuanto a las nuevas tecnologías y la protección y mitigación de lo que dicha incursión traería al país.

Importante resaltar que ya para el año 2006 y 2008 Colombia o más exactamente el estado colombiano empieza la travesía de promover un estado total de derecho e implementar el uso de las nuevas tecnologías, pero con un plus que se ingresara el uso del internet como una herramienta muy necesaria en cada uno de los procesos normales del funcionamiento a nivel Colombia y al interior de cada ciudad pueblo etc., ahora vemos leyes claras como la ley 1266 de 31 de diciembre de 2008 donde se dictan las disposiciones necesarias en cuanto al Habeas Data y se regula el manejo como tal de la información contenida en bases de datos personales.

Alrededor de ya el año 2009 al 2014 vemos ya la inclusión de los delitos informáticos en el código penal de Colombia y esto llega a convertiré en el impacto más pronunciado en la historia del país ya que se determina que existen los delitos informáticos se ve una realidad y se crea obviamente la necesidad de reglamentar este hecho para mantener la paz y la justicia en el país vemos también como se empieza a reglamentar el uso de firmas digitales algo lo cual fue muy novedoso y los servicios electrónicos como el caso de la correspondencia y más.

De ahí a la fecha se han dispuesto de diferentes normativas con el fin de llevar un control justo de las nuevas tecnologías y se siguen elaborando las distintas leyes ya que el tema del tic no se detiene es en evolución constante por ello la normatividad debe hacer lo mismo.

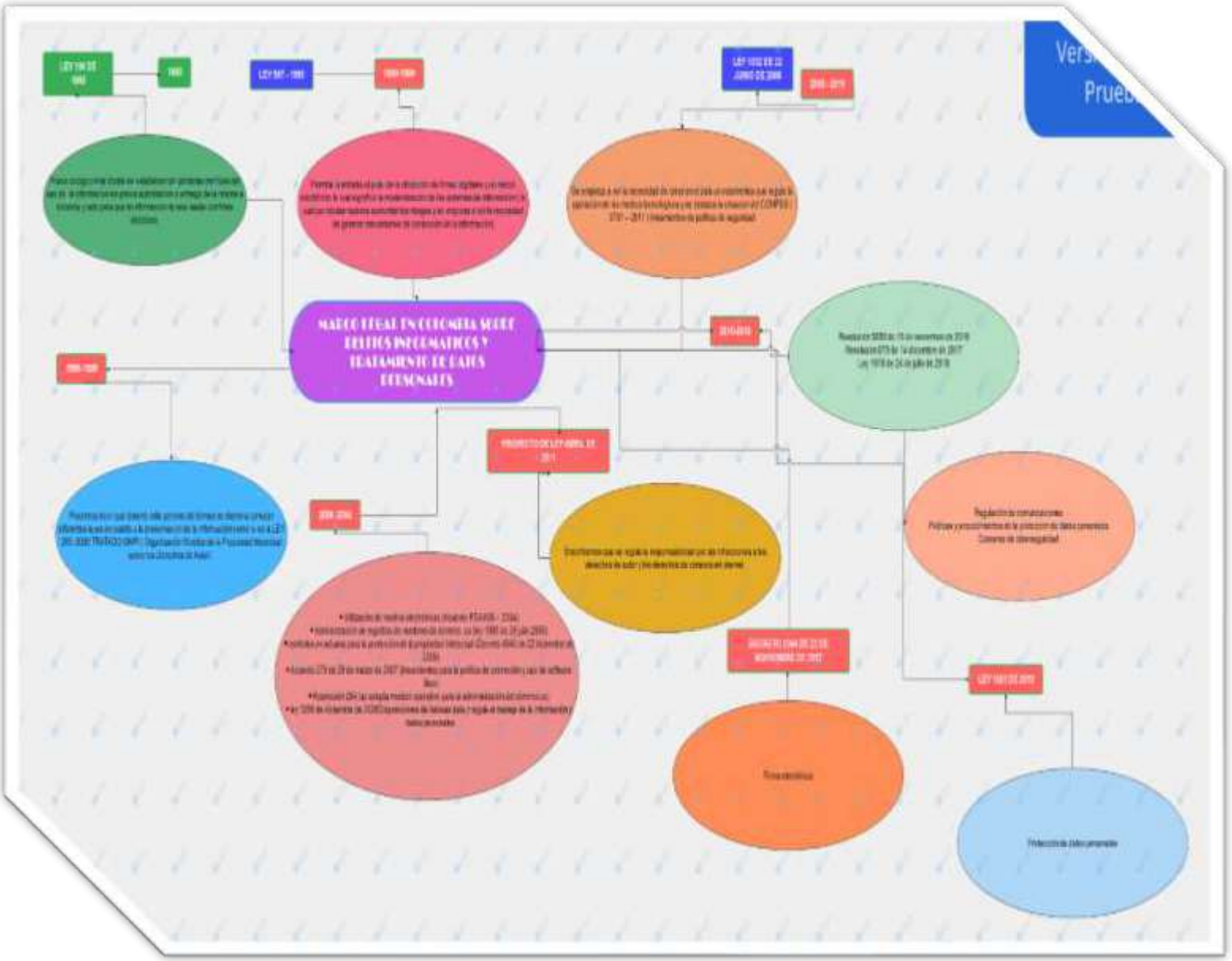


Figura 1 Mapa conceptual leyes y decretos en Colombia

1.2 HERRAMIENTAS UTILIZADAS EN LAS ETAPAS DEL PENTESTING

Consiste en atacar los diferentes entornos y sistemas de una empresa con la finalidad de encontrar y prevenir las posibles brechas de seguridad esta práctica podemos decir es la más conocidas a nivel de seguridad y la más demandada para las empresas debido a que sus pruebas, herramientas y análisis pueden darnos con exactitud el nivel verdadero de seguridad y con esto poder defenderse y actualizar todo su nivel de seguridad siempre con el fin principal que es la protección de la información.

En el campo de la seguridad informática y más exactamente la práctica del pentesting tiene como protagonistas dos equipos de ejecución de esta práctica y son el RED TEAM & BLUE TEAM en donde el RED TEAM se va encargar de la parte atacante u ofensiva y el BLUE TEAM pasa a ser la parte defensiva a proteger, ahora bien el trabajo de estos dos equipos de pentesters es correr a la misma velocidad que los atacantes es esa la verdadera operación del pentesting.

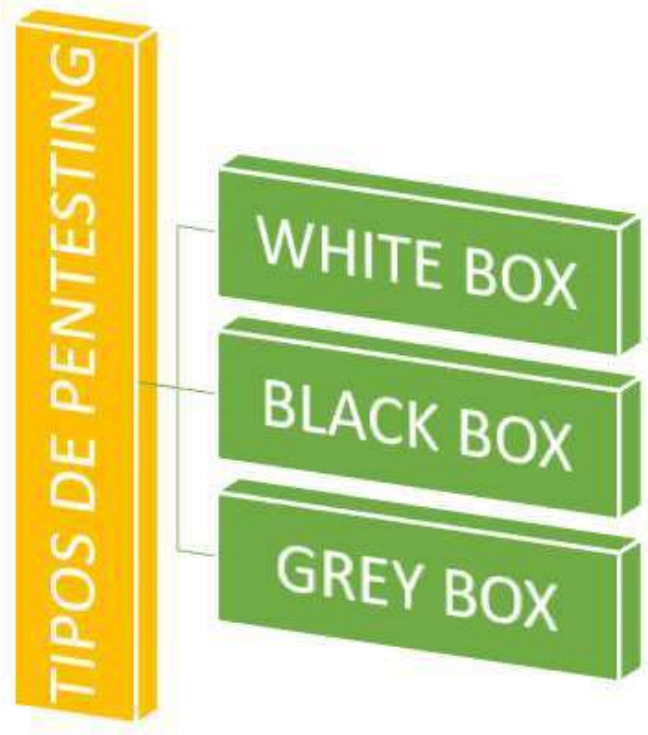


Figura 2 Pentesting

White box: En el caso de esta prueba el auditor o tester es quien conoce todos los datos del del sistema ya que en ocasiones o más exactamente es casi siempre una persona del mismo equipo tecnológico de la empresa es considerada una de las pruebas más completas ya que desde la información preliminar es fácil concluir que falta o que hay que cambiar y proteger.

Black box: Es una de las pruebas técnicas más real ya que el propio pentester no tiene los datos suficientes lo que lo obliga a realizar una actuación de ciberdelincuente por lo que sería por decirlo así una prueba a ciegas y es en ese momento donde descubre las vulnerabilidades y amenazas estructurales en la red.

Grey box: este tipo es una combinación de ambas pruebas anteriores, pero en este caso el auditor tiene solamente cierta información a la hora de realizar el testeo, este proceso es altamente recomendado ya que es un proceso de calidad que requiere de la máxima atención y tiempo.

Figura 3 Etapas pruebas

- Iniciamos con la preparación que es como su nombre lo indica lo que se va a preparar lo que se va a evaluar tanto datos como áreas etc.
- Luego procedemos a realizar el testing que para que sea optimo la empresa debe previamente haber realizado una auditoria completa a los sistemas y sabe por qué puntos puede entrar.
- Luego procedemos a realizar un plan de ataque para poder definir el cual será el acceso o más exactamente el nivel de acceso que tendrá el tester.
- Al realizar este tipo de pruebas se debe tener muy en cuenta el equipo de trabajo las personas que van a estar involucradas elegir muy bien los pentesters.
- Muy importante el costo – valor es decir que costo y que valor tiene para la empresa los daros que están vulnerables.
- Ya para realizar la prueba se deben utilizar herramientas apropiadas para cada zona a evaluar.
- Una de las cosas más importantes a la hora de realizar la prueba es documentar los datos encontrados todo el proceso ya que así mismo se toman medidas y se deja registro para el tema legal que es crucial en todo sentido al igual que las recomendaciones y soluciones.

Figura 4 Proceso de las pruebas de intrusión

RECOGIDA DE LA INFORMACION

Esta es la mayor etapa diríamos que la más demorada, pero de mayor importancia ya que se tienen que recoger los datos necesarios para la prueba como lo son los correos, ingeniería social, búsqueda en navegador web, números de teléfono, usuarios y administradores y hoja de vida de los involucrados. A su vez se debe escoger el método a realizar la prueba.

Ejemplo: caja negra o black box

ESCANEO

Esta etapa es donde se empiezan a analizar todos los puntos de ingreso sin tapar nada antes de realizar la explotación es donde se analizan los puntos vulnerables y brechas existentes el éxito de un buen escaneo es el éxito de una prueba con resultados excelentes.

Figura 5 Ejemplo extraido de internet escaneo Nmap

ENUMERACIÓN

Aquí procedemos el diseño que se basa en los resultados obtenidos enumerando las vulnerabilidades y los riesgos que se tengan se debe haber recolectado efectivamente la información y haber realizado una escaneo correspondiente o escaneos a las áreas previamente establecidas.

EXPLOTACIÓN

Es donde ganamos ya acceso y comenzamos a explotar los puntos vulnerables o fallos potenciales después de las etapas anteriores podemos realizar los exploits pero debemos garantizar fuentes confiables y seguras,

Figura 6 Ejemplo Metasploit

INFORME

Este proceso como ya se ha mencionado puede llegar a ser tedioso o aburrido, pero si seguimos correctamente el paso a paso y el estándar sin embargo si se siguió el estándar no tendremos complicaciones, pero lo que si se recomienda es que en el paso a paso se valla documentando para que así al final el reporte sea efectivo y rápido.

1.3 HERRAMIENTAS Y SOFTWARE ESPECIALIZADO DE CIBERSEGURIDAD

Definiremos las herramientas más utilizadas en este proceso de seguridad de la información utilizados en el campo del a ciberseguridad:

METASPLOIT

Cuando hablamos de esta herramienta es otra de esas navajas suizas o herramienta multiusos que debe tener a mano cualquier pentatester o que dice ser un experto en este campo el objetivo es encontrar agujeros de seguridad en todo tipo de redes, aplicaciones y dispositivos ahora bien si es cierto que el uso de Metasploit suele seguir al de nmap (o similar), el uso de Metasploit puede ser fundamental a la hora de entender dónde se encuentran los eslabones más débiles.

NMAP

Esta herramienta podríamos decir que es de las veteranas en el tema de escaneo de puertos y vulnerabilidades y forma parte vital del auditor de sistemas es interesante esta aplicación ya que es como tocar a la puerta de una máquina de un sistema y preguntar… ¿hay alguien ahí? ¿quién es?

OPEN VAS (OPEN VULNERABILITY ASSESSMENT SYSTEM,)

Esta herramienta es catalogada como es una suite de software, que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos. La versión actual (4.0.0) permite la actualización continua - solamente en periodos inferiores a 24 horas, de la base de Pruebas de Vulnerabilidades de Red.

EXPLOIT-DB (BASE DE DATOS DE EXPLOITS O BRECHAS DE SEGURIDAD)

Es un directorio web donde muchos hackers cuelgan vulnerabilidades de aplicaciones y cómo aprovecharse de ellas, con instrucciones específicas y cada día aparecen nuevas y es un lugar donde se puede aprender mucho, pero también se puede hacer daño a terceros si hacemos un mal uso de sus instrucciones y lo hacemos con fines malévolos.

CVE VULNERABILIDADES Y EXPOSICIONES COMUNES (COMMON VULNERABILITIES AND EXPOSURES)

Hablamos de una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID,

descripción de la vulnerabilidad, que versiones del software están afectadas, posible solución al fallo (si existe) o como configurar para mitigar la vulnerabilidad y referencias a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se demuestra su explotación. Además, suele también mostrarse un enlace directo a la información de la base de datos de vulnerabilidades del NIST (NVD), en la que pueden conseguirse más detalles de la vulnerabilidad y su valoración.

1.4 DESARROLLO BANCO DE TRABAJO

Iniciamos la importación de la maquina Kali Linux con todos sus componentes para poder realizar el banco de trabajo con el caso propuesto:

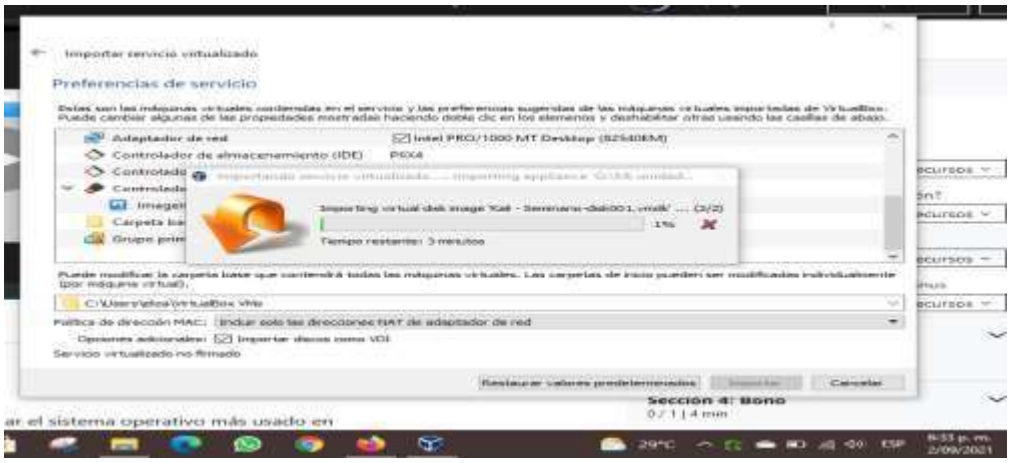


Figura 7 importación maquina KALI LINUX

Encontramos a continuación las herramientas necesarias para un banco de trabajo exitoso:

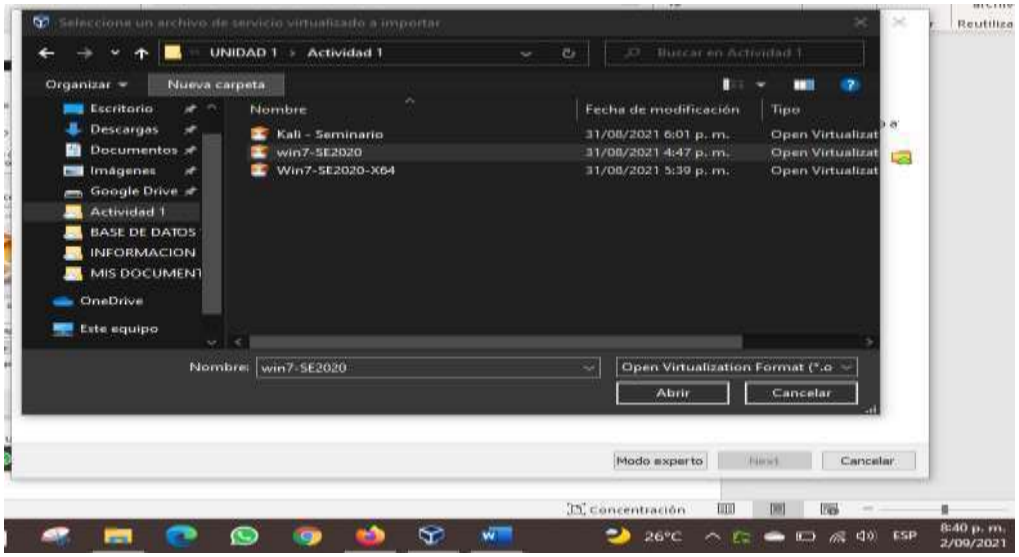


Figura 8 importación maquina 1WINDOWS

Procesdemos a importar la maquina windows de 64 requerida para los procesos:

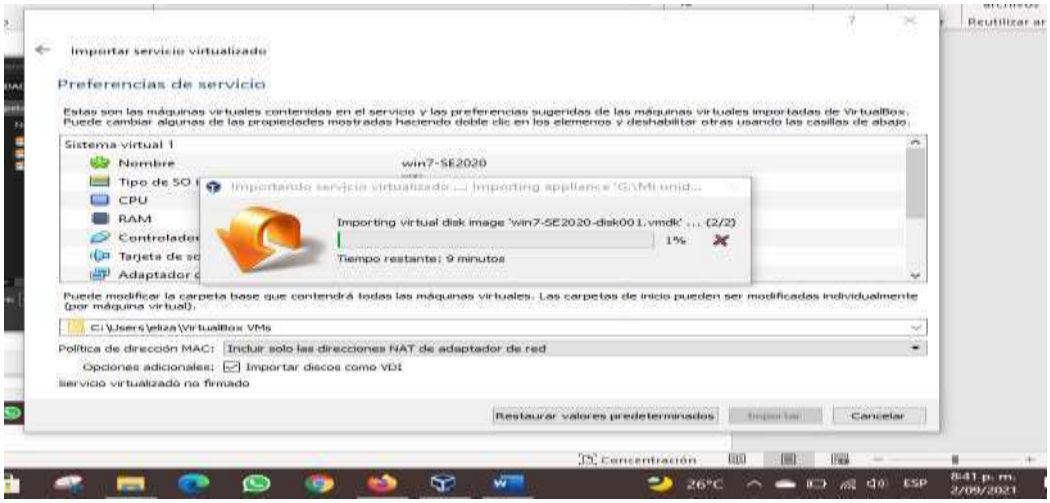
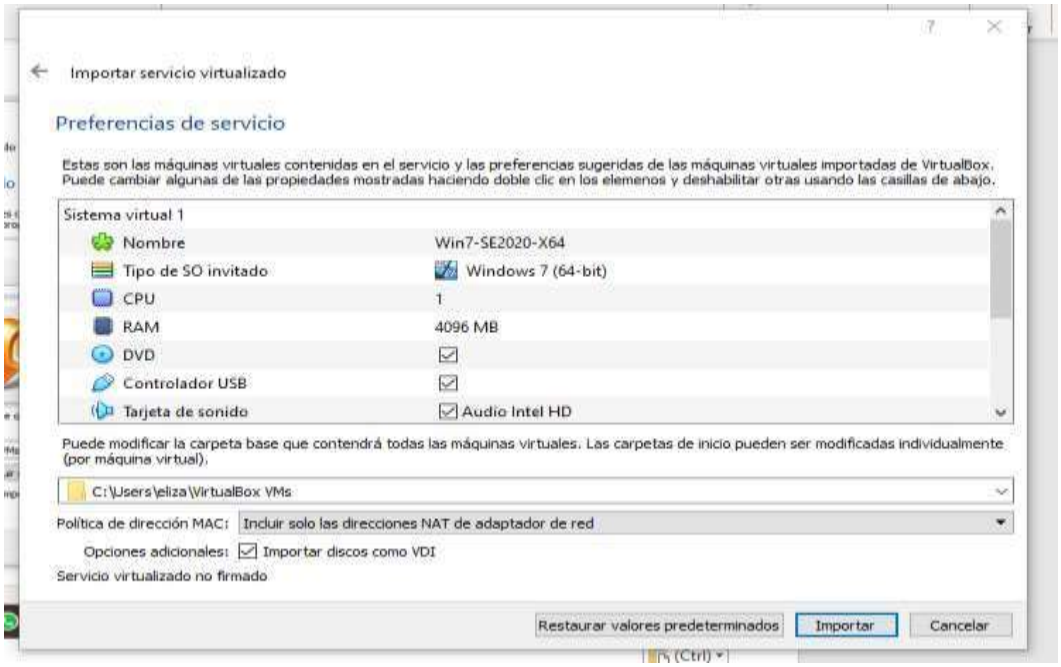


Figura 9 importación maquina 2 WINDOWS

No se cambia ningún parámetro de la configuración inicial ya que viene establecido para el trabajo que se va a realizar:



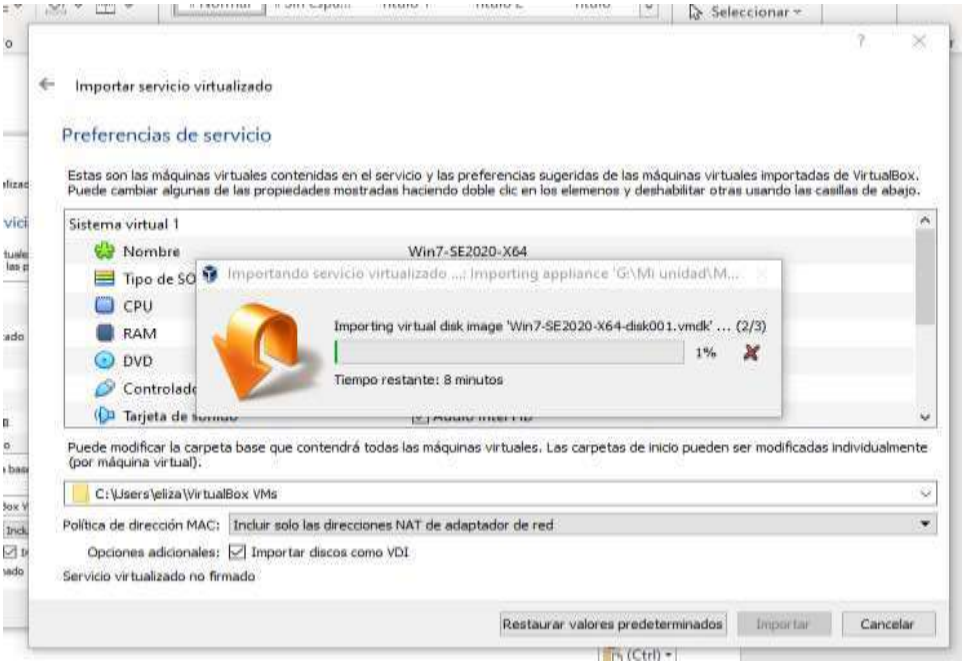


Figura 10 Encendido maquina kali linux

Como podemos evidenciar se realizó la correcta importación de las maquinas y herramientas de nuestro banco de trabajo:

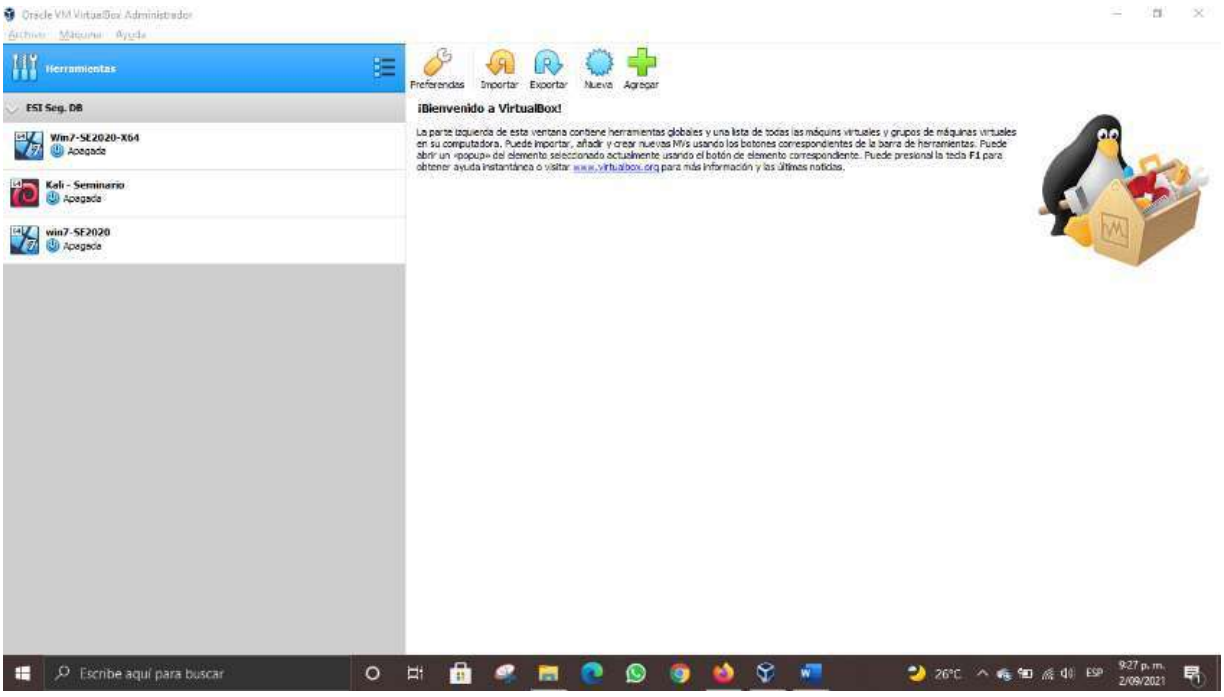


Figura 11 Evidencia maquinas importadas correctamente

Se da inicio a la maquina kali linux la cual sera nuesto atacante o desde donde se dirijira cualquier operación durante el estudio de casos:

Figura 12 Inicialización maquina kali linux

Encontramos pantalla de inicio del entorno de kalilinux

Iniciamos maquina Windows de 32:

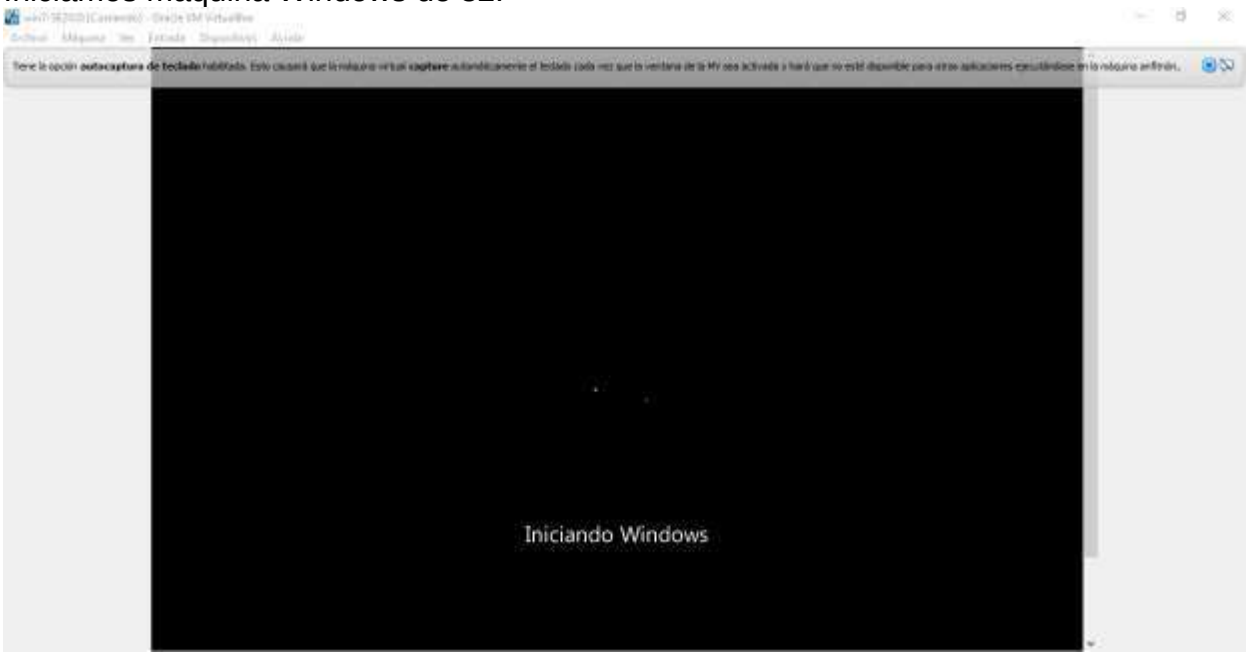


Figura 13 inicialización de la maquina Windows 32

Luego de haber iniciado la maquina Windows procedemos a revisar su configuración de red y extraer la ip :

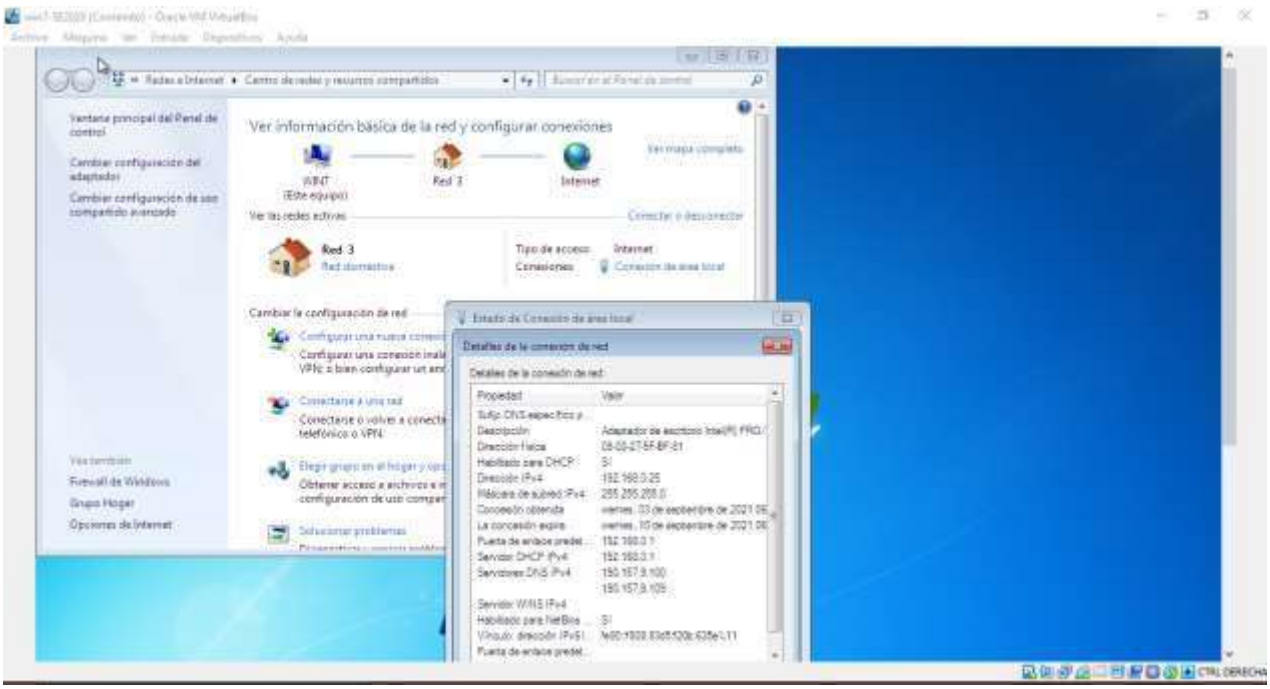


Figura 14 localizacion de la direccion ip de la maquina

Procedemos desde la maquina kali Linux a establecer comunicación con la maquina Windows x32 mediante un ping a la ip 192.168.0.25.

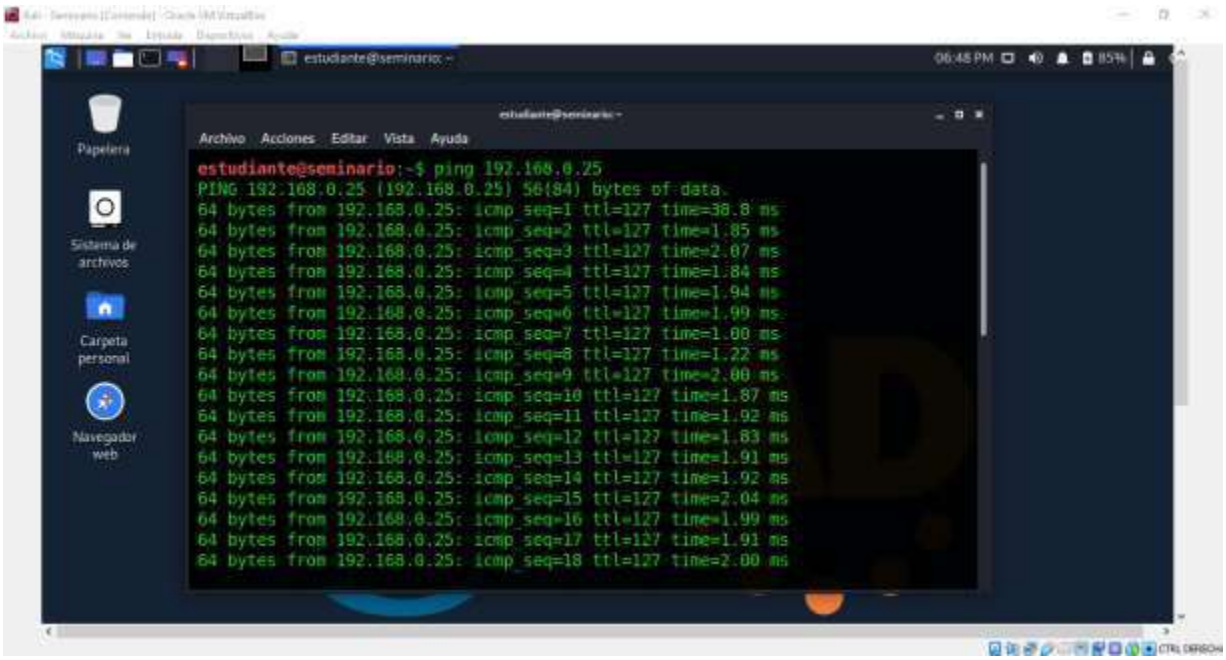


Figura 15 Comprobando conexión entre Kali Linux y win 32 (Maquina 1)

Encontramos ya el resultado exitoso de la comunicación de las dos máquinas.

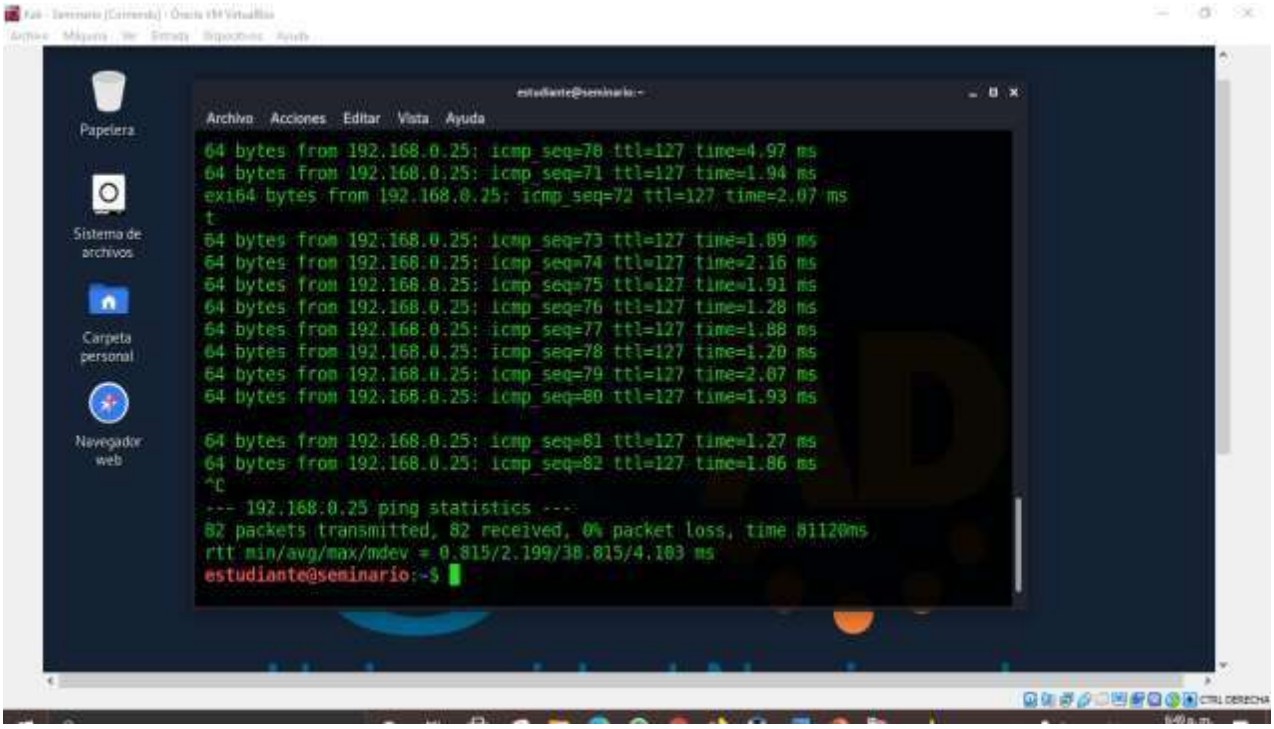


Figura 16 Comprobando conexión entre Kali Linux y win 32 (Maquina 1)

Inicializamos la maquina win de 64 para realizar el mismo proceso de la máquina anterior:

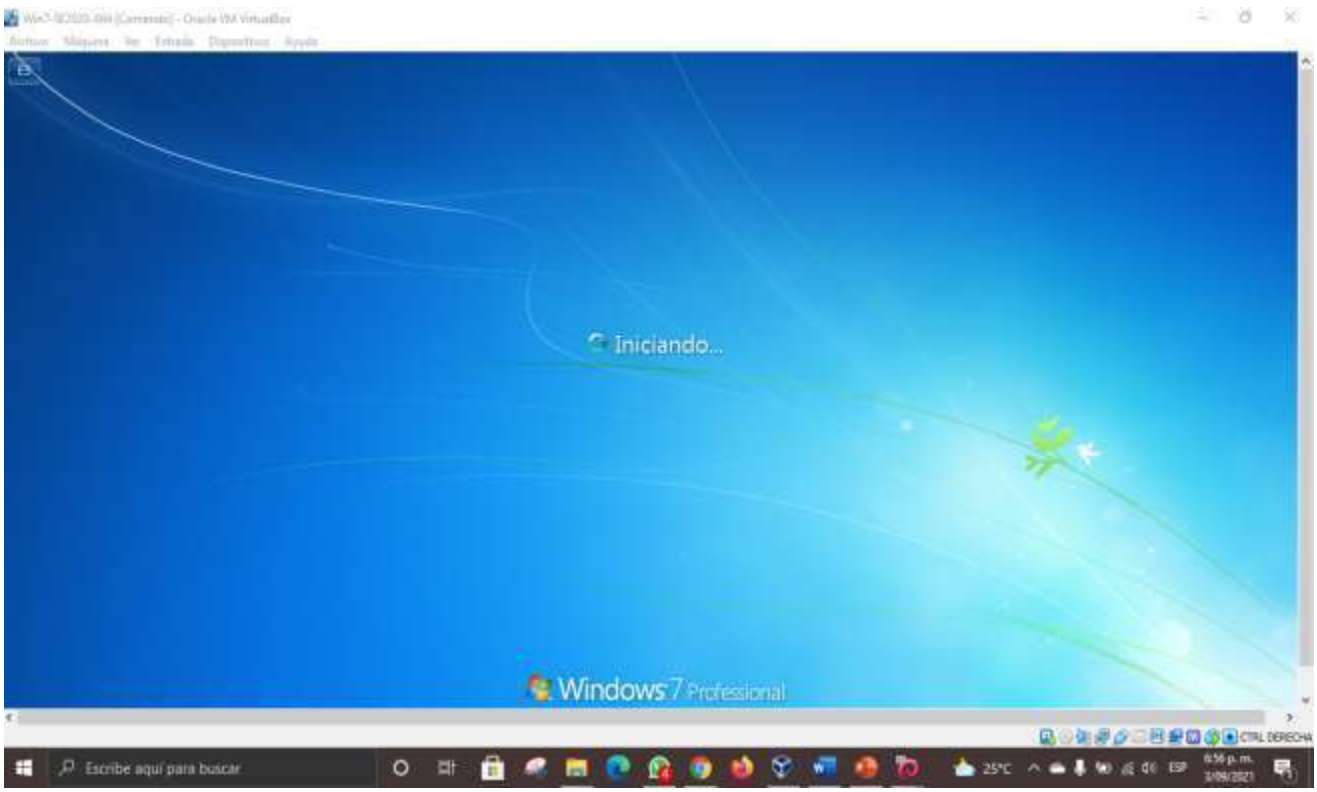


Figura 17 Comunicación Kali Linux maquina win 64

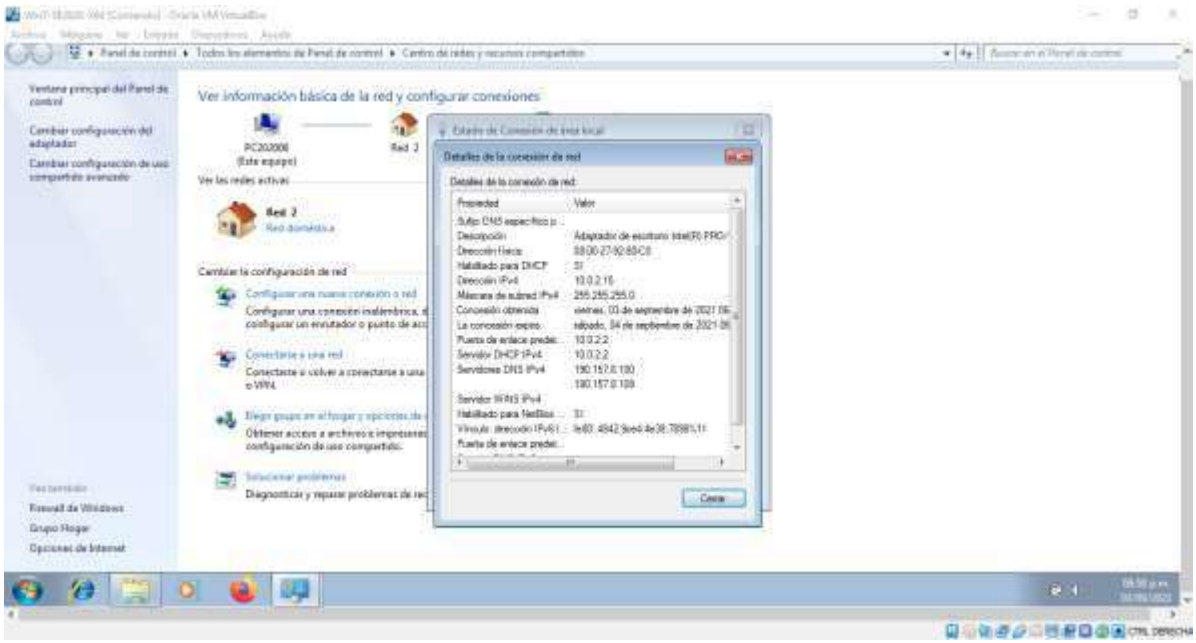


Figura 18 localización ip Windows

Realizamos el ping de comunicación:

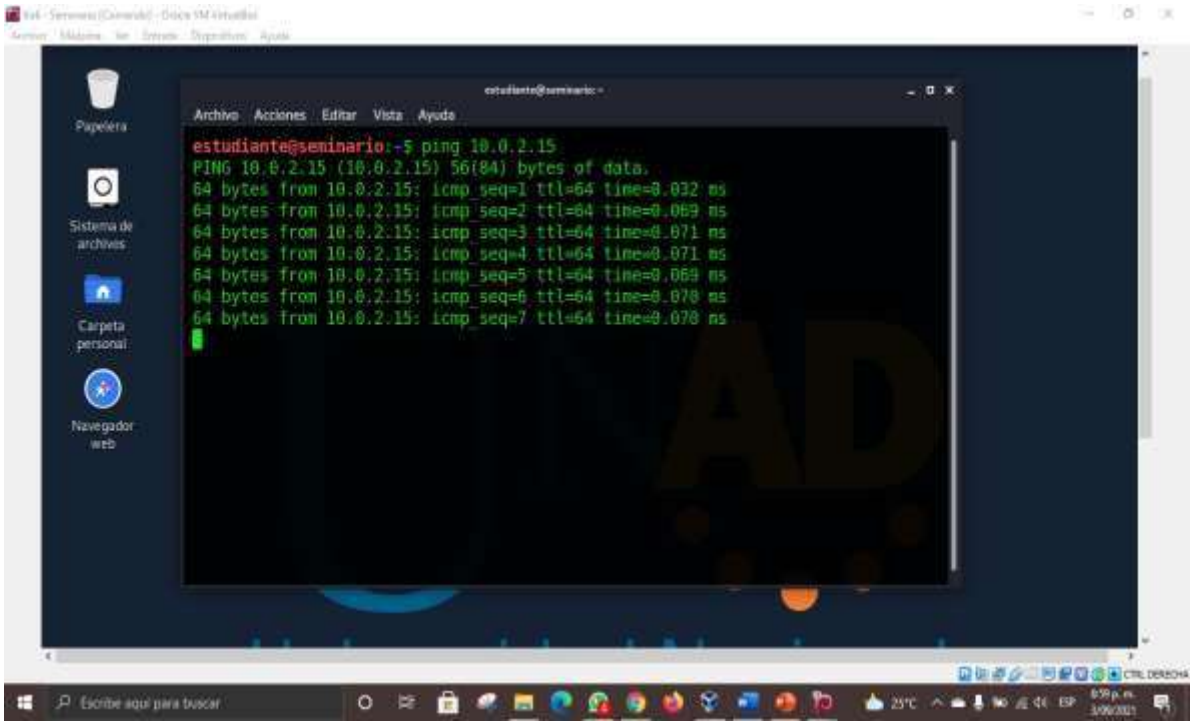


Figura 19 Comunicación Kali Linux maquina win 64

Resultado ping exitoso de la maquina de 64 :

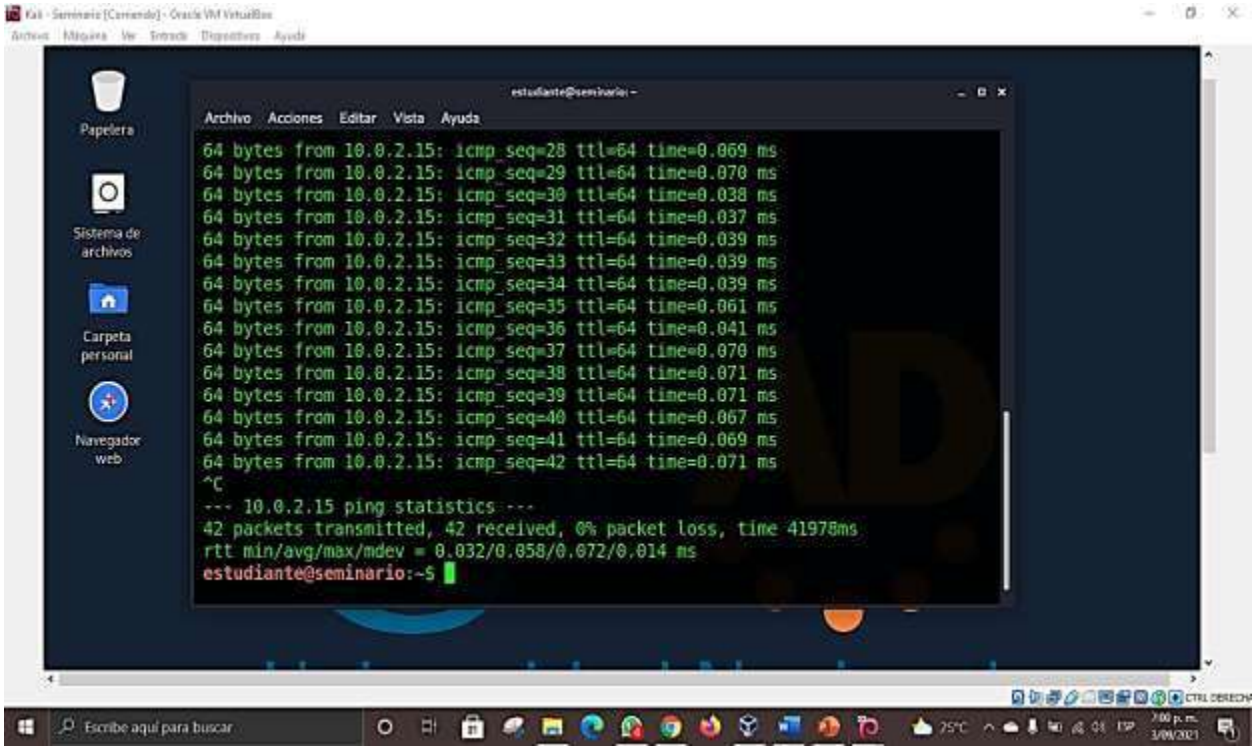


Figura 20 Comunicación Kali Linux maquina win 64

2. ETAPA ACTUACIÓN ÉTICA Y LEGAL

Al revisar el contrato y el caso anexo podemos concluir que existen varias irregularidades las cuales se señaran a continuación junto con su argumento y recomendaciones.

FRACMENTOS EXTRAIDOS DEL CONTRATO CON IRREGULARIDAD

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la **información confidencial** o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.

Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

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

Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

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

Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.

ARGUMENTACION

En el contrato estipulado para la contratación del personal para los equipos red team & blue team se logra evidenciar la ilegalidad al incluir en los requerimientos o clausulas, ítems o deberes del trabajador que violan tanto el código penal del país como el código ética del profesional, toda la información debe ser protegida y manejarse con confidencialidad y esto se debe manejar con toda la seguridad se debe informar cualquier irregularidad y no se debe llevar a la compañía a procesos ilegales mucho menos participar de los mismos.

Cuando hablamos de información esta debe ser protegida y cualquier movimiento de la misma manejo o manipulación debe ser informado correctamente a los superiores o autoridades respectivas, es por ello que los ítems irregulares señalados anteriormente encontrados en el contrato corresponden a un mal manejo de la información y al incurrir en los delitos informáticos que se mencionan en nuestras leyes y decretos representa una gran pérdida tanto para la empresa como para el profesional en cuestión que se presta para dichas tareas ilícitas.

Es necesario recordar que la información es un bien valioso y la pérdida o vulneración de esta repercute en grandes pérdidas económicas.

RECOMENDACIONES

Como profesional experto en el campo de la ciberseguridad tomaría la libertad de recomendarle a withehouse segurity que podría tomar el contrato como prueba dentro del proceso de selección para validar ética de los aspirantes, pero no a nivel de contratación fija ya que esto puede hablar muy mal de la empresa y puede repercutir en pérdidas económicas hasta el cierre de esta.

Se debe ser más severos en el proceso de contratación ya que al no tener los filtros adecuados se puede caer en el error de contratar personal que pueda vulnerar la información o incluso sacar información sin autorización para compartirla a terceros que se consideren competencia y al igual que los filtros la

evaluación psicológica puede mostrar patrones del comportamiento y futuro del profesional a contratar entes de ser contratado.

2.1 ANÁLISIS Y ARGUMENTACIÓN DE CUALQUIER PROCESO ILEGAL EN RELACIÓN DE LA LEY 1273 DEL ACUERDO

De acuerdo con la presente ley y realizando las comparativas y respectivas validaciones encontramos que el anexo vulnera los siguientes artículos:

La primera irregularidad que se encuentra es que el contrato refiere en un item a que el trabajador puede realizar o la empresa puede realizar accesos abusivos al sistema con diferentes fines ya sea más lucro entre otros y esto no se debe informar se menciona nuevamente la parte que hace alusión (datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.) y esta parte vulnera el siguiente artículo de la ley mencionada con anterioridad:

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

El contrato relacionado en el anexo vulnera los decretos de la ley 1273 que se mencionaron anteriormente ya que se encuentra trato indebido de la información cuando se menciona el manejo de la información el acuerdo de confidencialidad destaca que el aspirante a dicho trabajo no debe notificar ningún tipo de trato de la información ni tampoco notificar procesos ilegales que se realicen al interior hay se puede notar un fallo al siguiente artículo de la ley:

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

Item 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

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

El contrato actual vulnera la integridad profesional tanto de la empresa como del aspirante si este aceptara dichos ítems de contratación vemos claramente como incurriría el trabajado en conductas irresponsables y mal manejo de la información ya que en el contrato dice que debe abstenerse de publicar o dar notificación de procesos ilegales denunciar dicha información o procesamiento ilegal y esto vulnera también el:

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

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

El robo se cualquier tipo es considerado un delito grave y cuando se habla de datos personales cuando se habla de información empresarial o de terceros hablamos de un bien que al ser vulnerado repercute en pérdidas y cárcel sabiendo esto en el contrato se menciona que En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security. Esto vulnera el :

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

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

2.2 ANALISIS Y REVISIÓN DESDE EL PUNTO DE VISTA LEGAL Y ÉTICO DE LA PROPUESTA LABORAL

si bien es cierto que en ocasiones la situación del país a nivel económico y mucho más en la travesía de una pandemia ha obligado a muchas personas a dejar a un lado su ética y moral por si claro es obvio que de ética no se come pero leyendo con cabeza fría nuestro código de ética encontramos que su fin es que el profesional actúe de manera legal y honesta y es mucho más tranquilo ganarse dos o tres pesos de manera legal que ilegal porque al fin y al cabo por más necesidad si se descubre se paga más caro de lo que se hizo y la reputación del profesional quedaría en el piso.

consideró que por más difícil que sea la situación le ira mejor a la persona honesta y legal que al contrario desde cualquier punto de vista, como esta debe ser una respuesta honesta en mis principios y valores sé que debo trabajar diligentemente porque el que no trabaja no come, pero más es porque he sido criada en los valores cristianos donde mi trabajo debe reflejar a Dios y el me proveerá si yo cumplo con honestidad por esa razón no aceptaría el trabajo.

2.3 ANÁLISIS DE LOS ASPECTOS LEGALES Y ETICOS DE LA NOTICIA DEL CASO “OPERACIÓN ANDROMEDA BUGGLY” DESDE MI PUNTO DE VISTA COMO EXPERTO.

Desde todo punto de vista la operación Andrómeda es un acto deshonesto y sediento de más y más podemos ver claramente como a partir de una fachada de un intento “sociable o amigable” se atraía a las personas a los profesionales en este campo de la seguridad par vulnerar sus derechos y robar técnicas para hacer el mal en cuanto a mi punto de vista destaco primero la falta de ética profesional y personal de este exmilitar experto en seguridad.

según se entiende lo que tenían pensado era una comunidad inocente de exertos en el área que pudieran compartir lo mejor de la seguridad informática aunque no fueran muy avanzados su propósito era hacer parte de una comunidad grande y de reconocimiento y digamos que aparentemente funcionaba con legalidad pero la realidad era otra lo que realmente se hacia su fin era llamar la atención de hackers experimentados y algo más técnicos para usar sus conocimientos para sin idea alguna de que esto era una operación militar y no solo eso realizaban operaciones o actividades ilícitas como espionaje y violación de datos personales esto con técnicas como software de interceptación que era de uso exclusivo del gobierno o conseguido en el mercado negro.

Esto es inaudito para un experto en seguridad o cualquier área desde mi concepto personal puedo decir que son personas aparentemente inteligentes pero no

realmente ya que lo único que hacen es empobrecer al país y después quejarse del gobierno es enseñarle a las nuevas generación a que lo que da es la ilegalidad es generar o educar personas en la ilegalidad y a ese paso se deberían construir cárceles y no casas es duro pero es una realidad consideró la honestidad y los valores por sobre todo pienso que los involucrados en este caso dejan un mensaje muy negativo y de desesperanza para los que vamos en proceso a ser procesionales que aportan algo positivo a todos y nuestras familias.

3. ETAPA EJECUCIÓN PRUEBAS DE INTRUSIÓN

3.1 INFORME DE HERRAMIENTAS Y PROCEDIMIENTOS UTILIZADOS PARA DAR SOLUCIÓN AL ESCENARIO DE RED TEAM DE ACUERDO CON LOS PASOS DEL PENTESTING.

Las herramientas que se utilizaron en el proceso según los pasos de la operación de pentesting son:

Iniciamos la máquina Kali Linux desde la cual realizaremos el proceso de pentesting Primero realizaremos un ping para evidenciar que tengamos conexión exitosa entre el equipo Kali y la maquina Windows:

Procedemos como muestra la imagen nuevamente a validar la comunicación entre las máquinas para así comenzar el ejercicio:

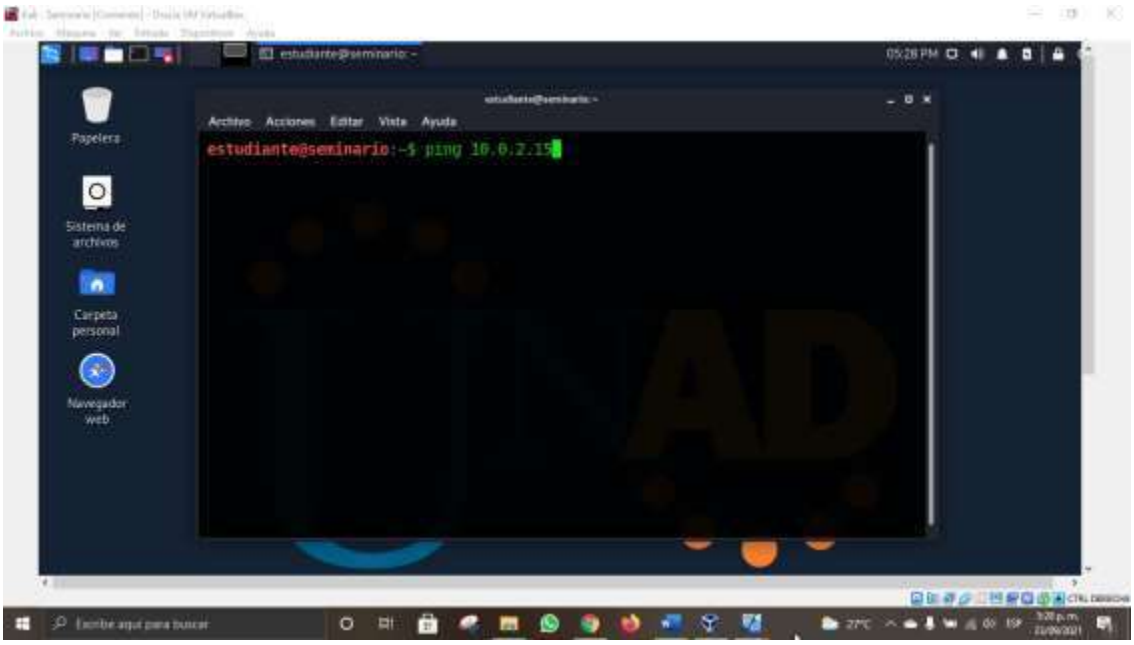


Figura 21 Comunicación Kali Linux maquina win 64

Se valida la conexión iniciando correctamente:

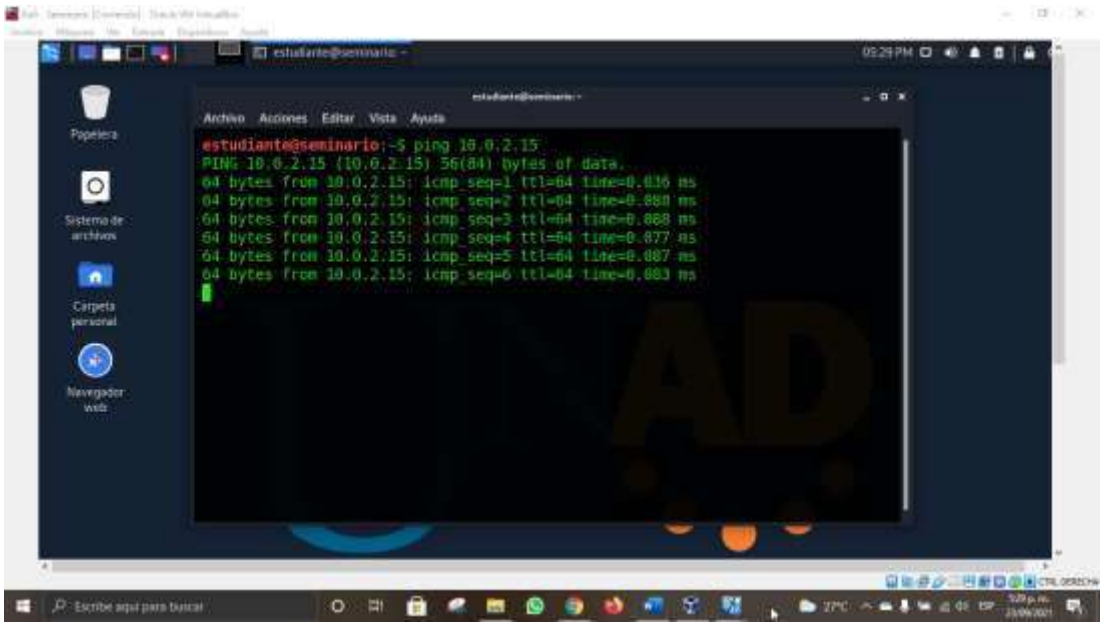
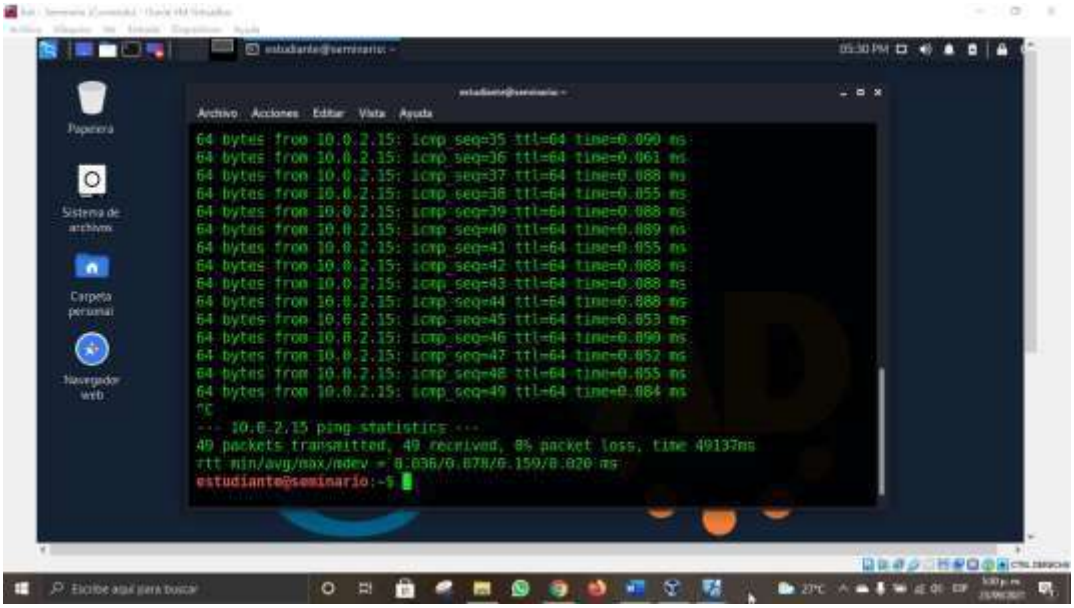


Figura 22 validación de conexión

Se encontró un resultado exitoso:



Procedemos a iniciar el escaneo con las aplicaciones nmap y Nessus:

Nmap: Herramienta multiplataforma para exploración de red, identifica puertos abiertos, que servicios produce, versión del sistema operativo y es fácil de

adaptarse a la red incluyendo su congestión y latencia.

Esta aplicación nos permitirá verificar la seguridad por medio de los puertos y los servicios.

Escaneo de puertos: lo primero que realizamos con la herramienta seleccionada es el escaneo de los puertos para saber que puertos están abiertos y cerrados:

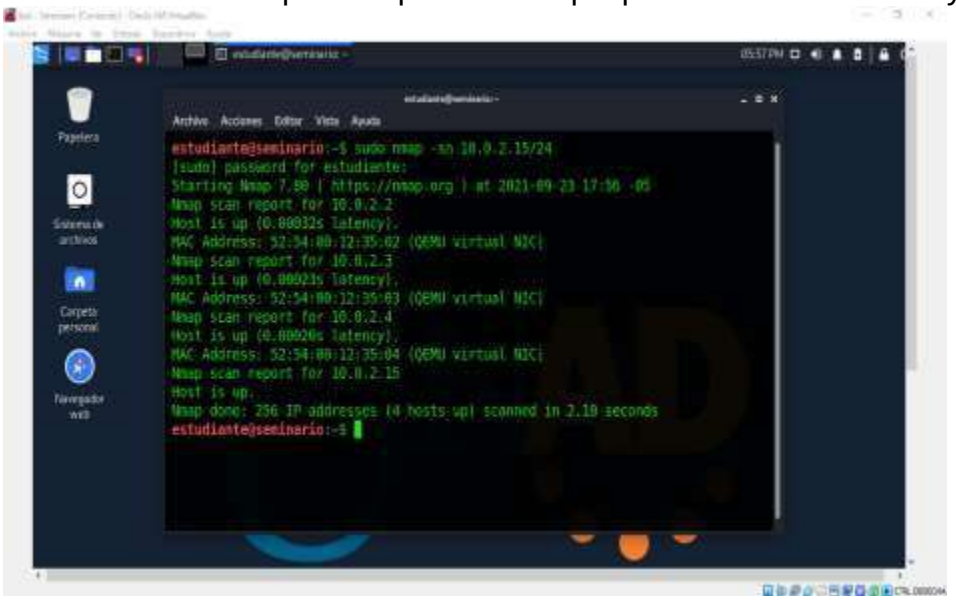


Figura 23 Escaneo de puertos

Escaneo de servicios: realizamos a continuación el escaneo de servicios revisando así su correcto funcionamiento:

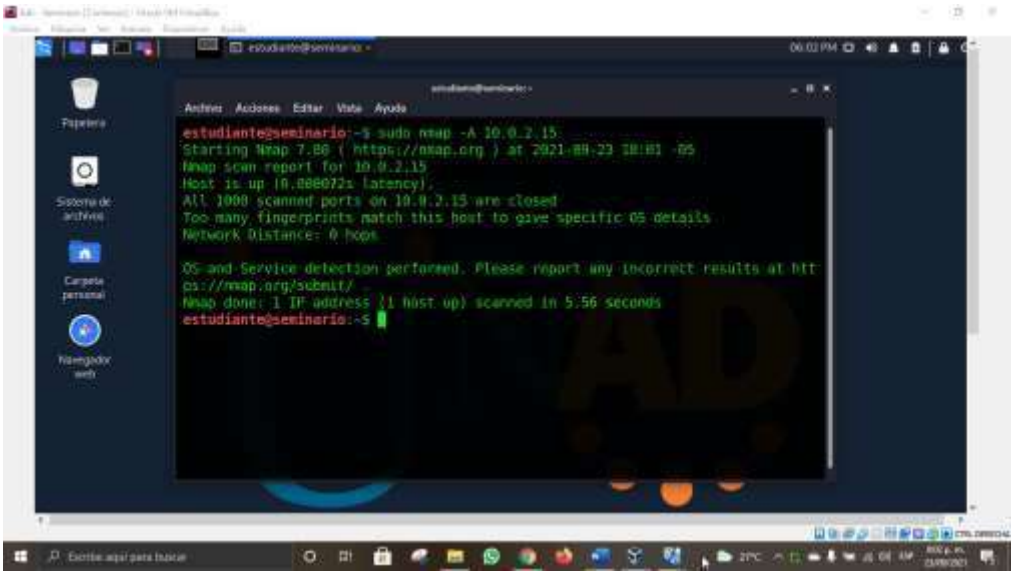


Figura 24 Escaneo de servicios

Nessus: Estructura de trabajo que ofrece escaneo, búsqueda de vulnerabilidades en una red y posibles soluciones, clasifica los resultados encontrados para entrega de informes.

3.2 ANÁLISIS DEL ATAQUE PRESENTADO A CADA UNA DE LAS MAQUINAS IDENTIFICADAS.

La fuga de información se realizaba a través de la aplicación HFS la cual nos permite compartir archivos por medio de la ip a la web lo que pudimos descubrir es que esta aplicación está presente en el equipo win 7 de 64 la cual es la que se encuentra en análisis ya que presenta sospechas de filtración de información y es la maquina la cual como equipo redteam se procesar.

A continuación, el proceso: inicializamos herramienta HFS con el fin de ver por donde se esta realizando la fuga de la información.

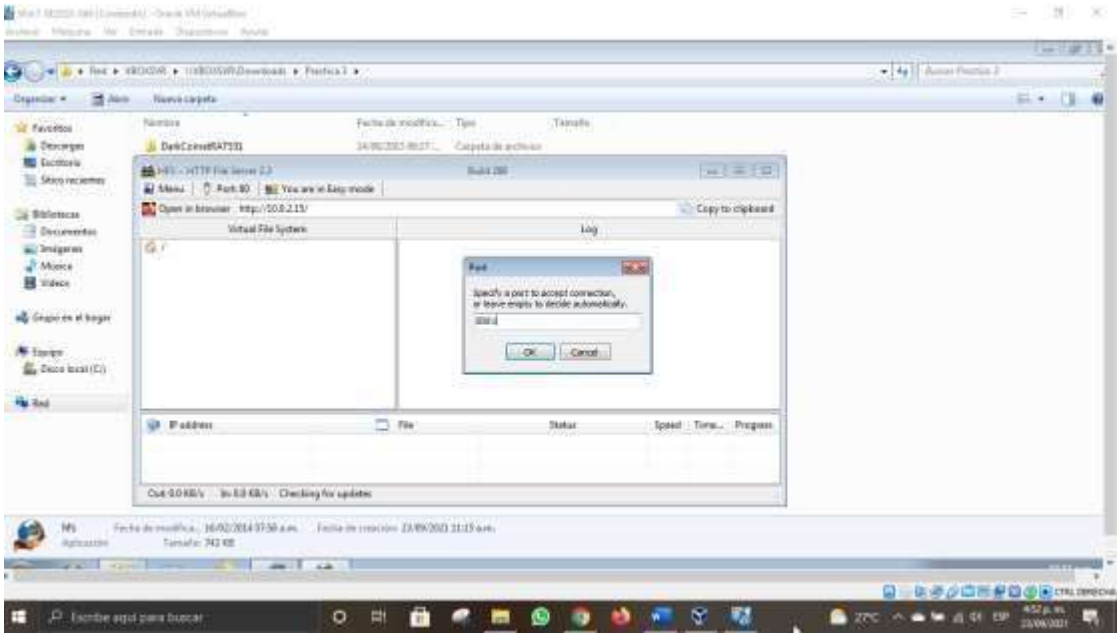


Figura 25 proceso con la herramienta HFS

Se realiza a continuación una prueba que nos permitirá corroborar esa fuga la prueba se realiza mediante una imagen cualquiera que se pasa por la herramienta y se comprueba su filtración a la web sencillamente con un link:

Imagen del koala es la seleccionada para el proceso:

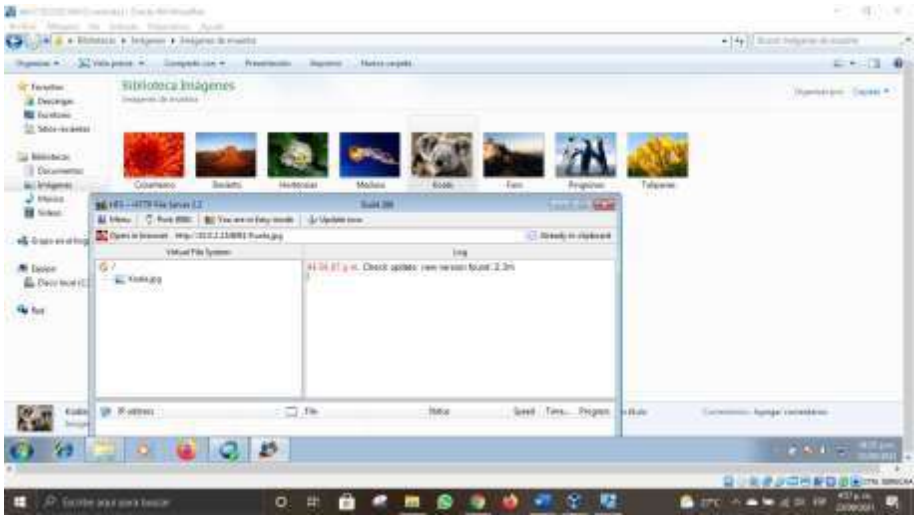


Figura 26 proceso con la herramienta HFS

Revisamos mediante el link y efectivamente corroboramos la filtración:

Figura 27 proceso con la herramienta HFS

A continuación el resultado:

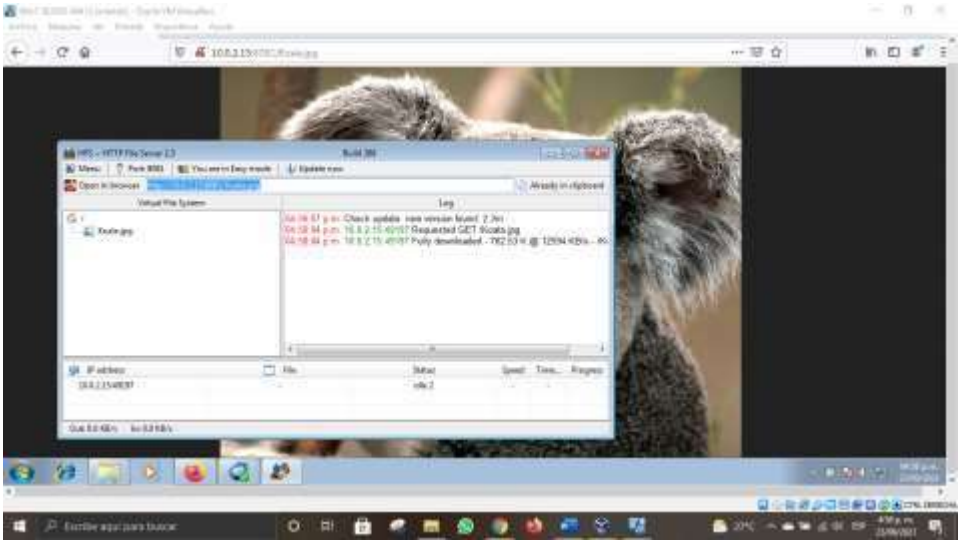


Figura 28 resultados con la herramienta HFS

Equipo con victima con aplicación Rejetto:

En esta parte del proceso lo primero a realizar es desactivar todas las aplicaciones de seguridad que nos causan conflicto a la hora de ejecutar la aplicación entonces se procese a la desactivación del firewall, update y antivirus en ambas máquinas identificadas con Windows 7 y Windows 7x64.

Figura 29 Iniciamos maquina Windows 7x 64:

Procedemos a desactivar el firewall de Windows

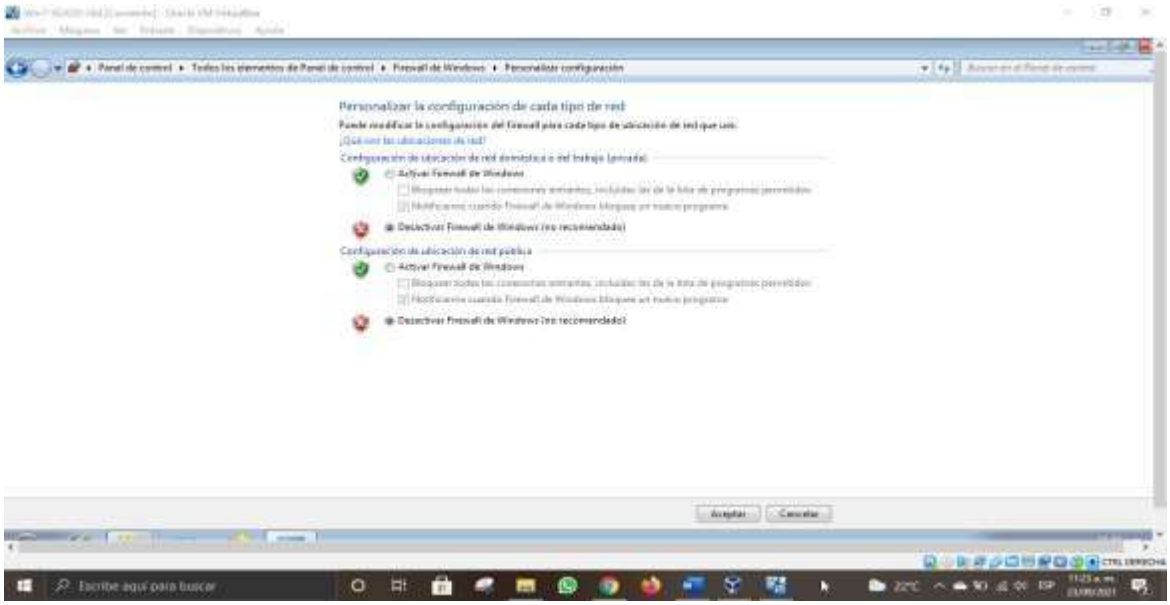


Figura 30 Desactivación firewall de Windows

Procedemos a desactivar el antivirus y protección del sistema

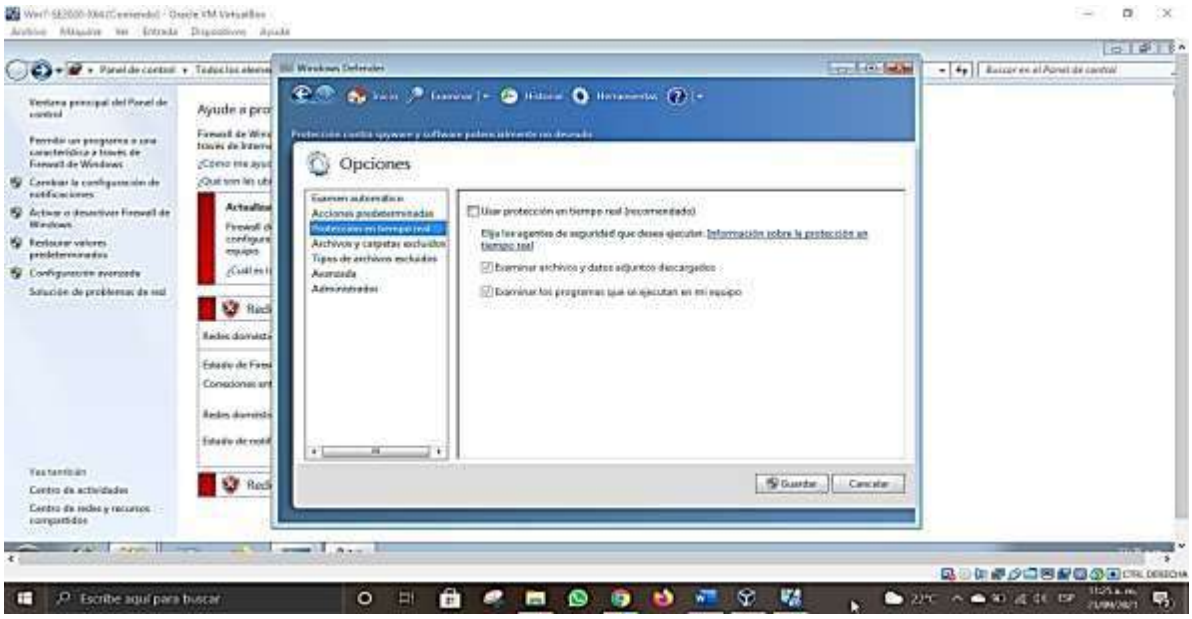


Figura 31 desactivación Windows defender

Procedemos a continuación a hacer la ejecución de la vulnerabilidad rejetto

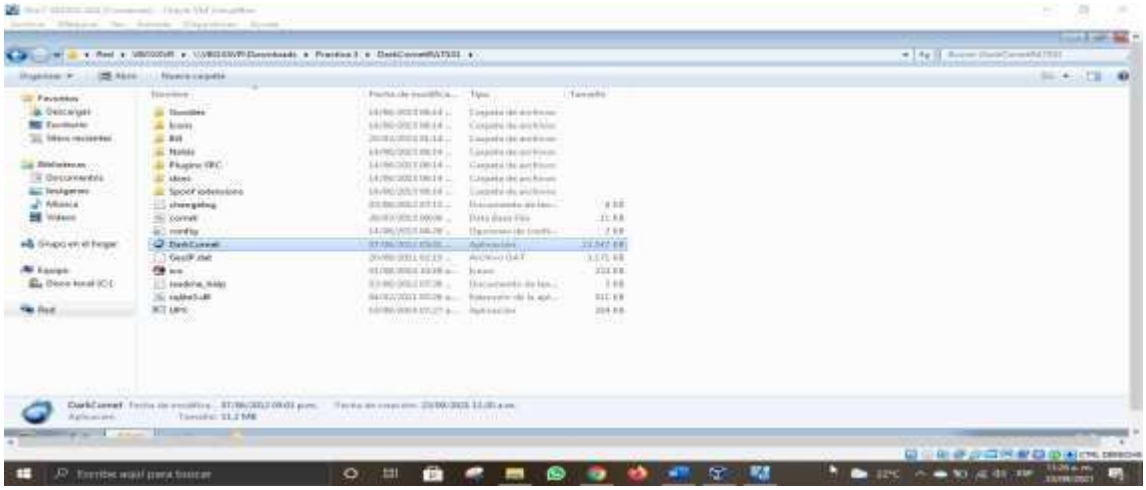
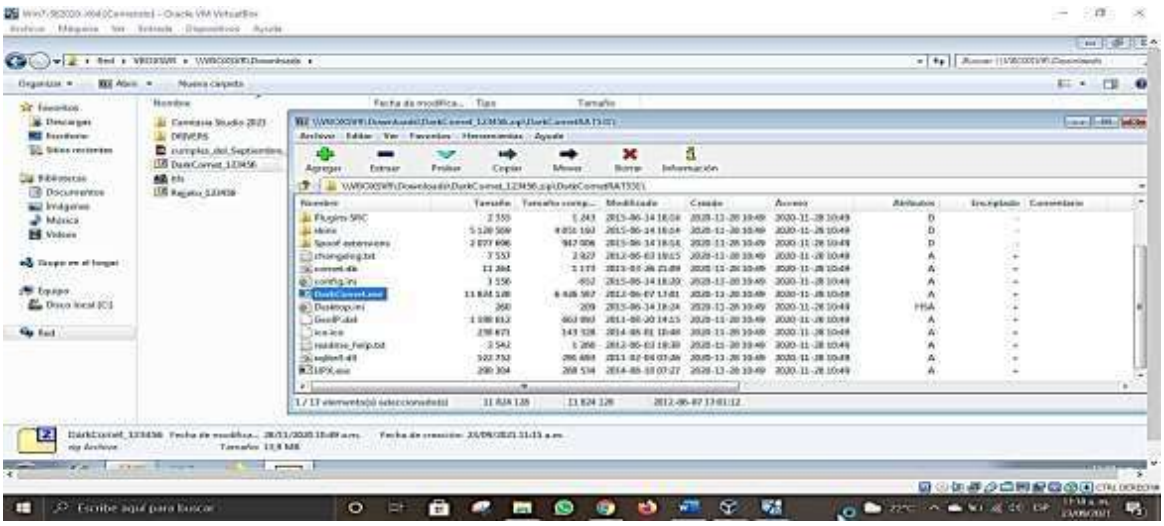
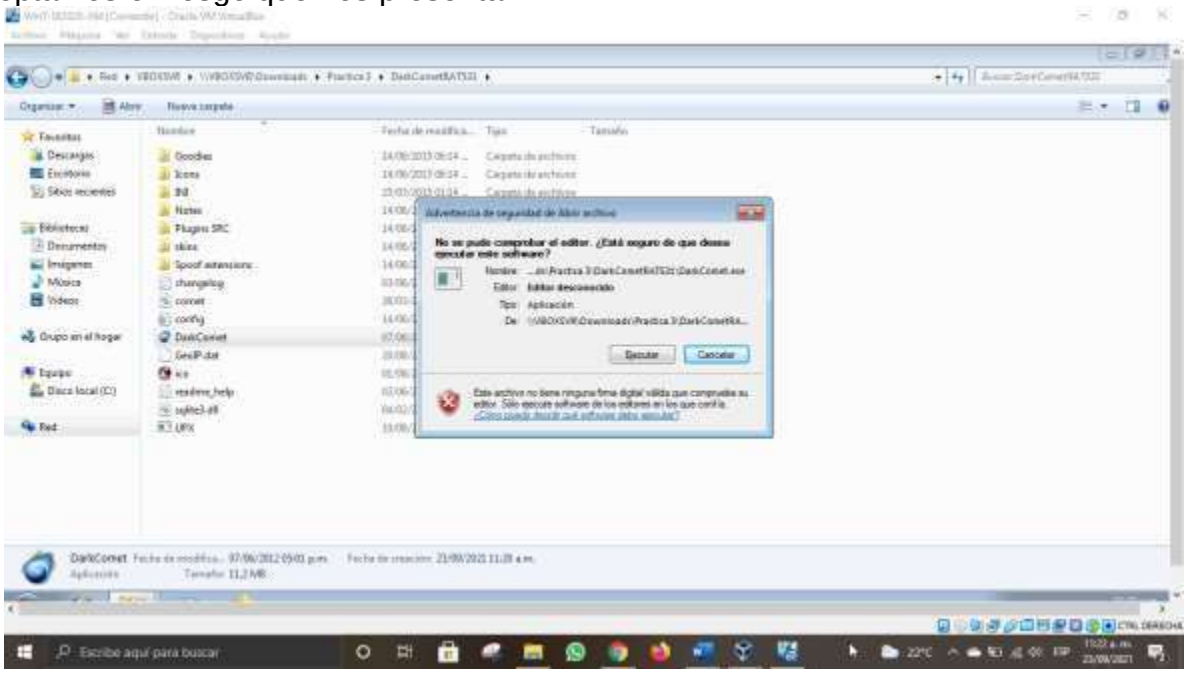


Figura 32 Ejecutamos la aplicación Rejetto

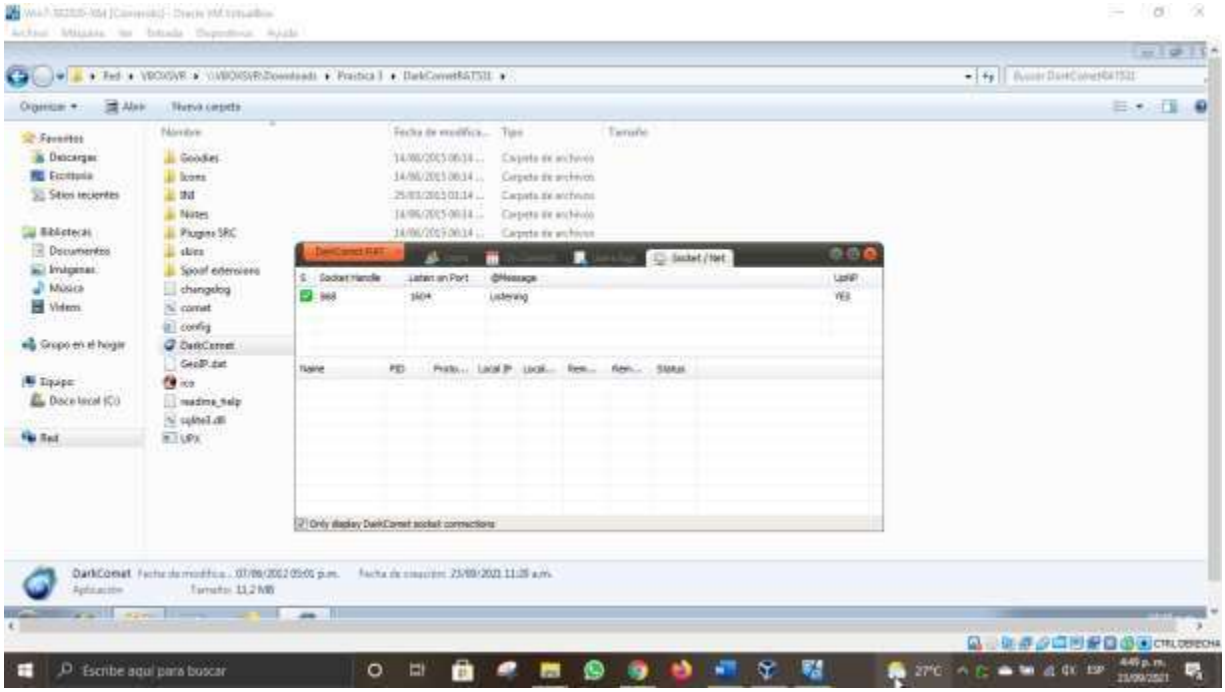
Seleccionamos para la ejecución



Aceptamos el riesgo que nos presenta:



Observamos en la imagen a continuación el resultado de la ejecución:



3.3 ANALISIS DE SEGURIDAD DONDE SE IDENTIFICO EL FALLO DE SEGURIDAD EL CUAL ATACA LA MAQUINA WINDOWS USO Y APLICACIÓN DE LAS HERRAMIENTAS PARA LAS PRUEBAS

Se pudo identificar que el equipo sospechoso cuenta con Windows 7 X86 y X64 dado que el equipo en cuestión cuenta con un sistema operativo antiguo dando paso a la aplicación en cuestión que veíamos anteriormente la cual solo es compatible con dicho sistema operativo.

Se evidencio que el equipo cuenta con SMBv1 activo para compartir impresoras y archivos dentro de la red, es posible que la fuga de información se presente también aprovechando la vulnerabilidad de que no estaba actualizado el sistema operativo.

Para este proceso utilizaremos la búsqueda de amenazas mediante la aplicación o herramienta Nessus:

Figura 33 Iniciamos la maquina Kali Linux

Se procede a realizar la descarga de la herramienta Nessus desde la página o fuente oficial para evitar el mal funcionamiento o amenaza:

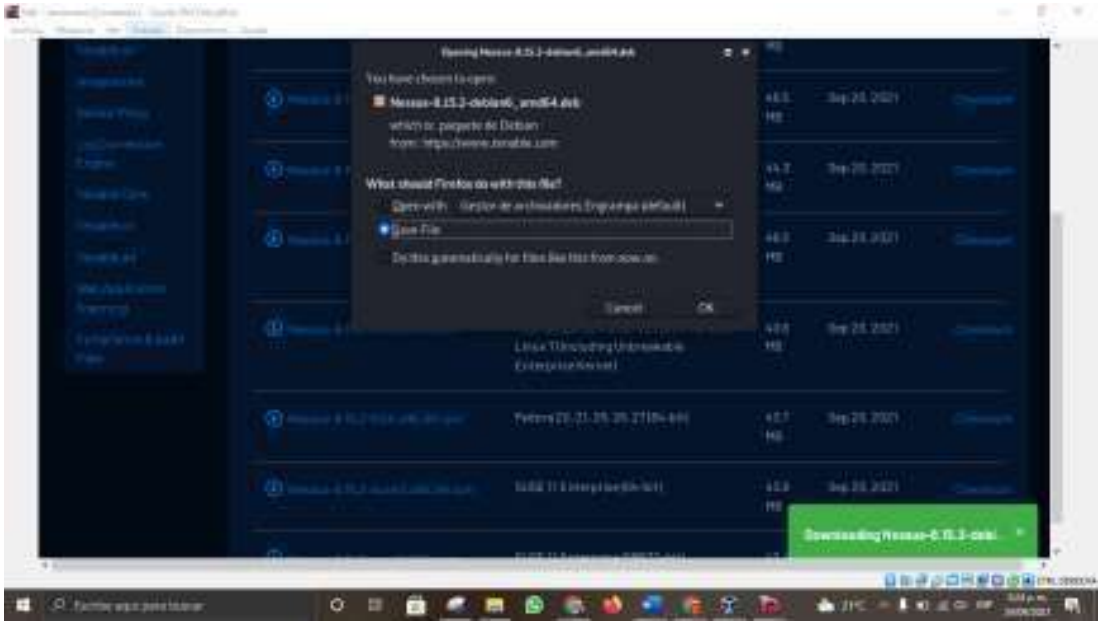


Figura 34 Descarga de la herramienta Nessus:

Realizamos la instalación por medio de consola revisando parámetros todo con permisos de administrador para que todas las herramientas estén instaladas de manera correcta y el programa funcione con el fin propuesto:

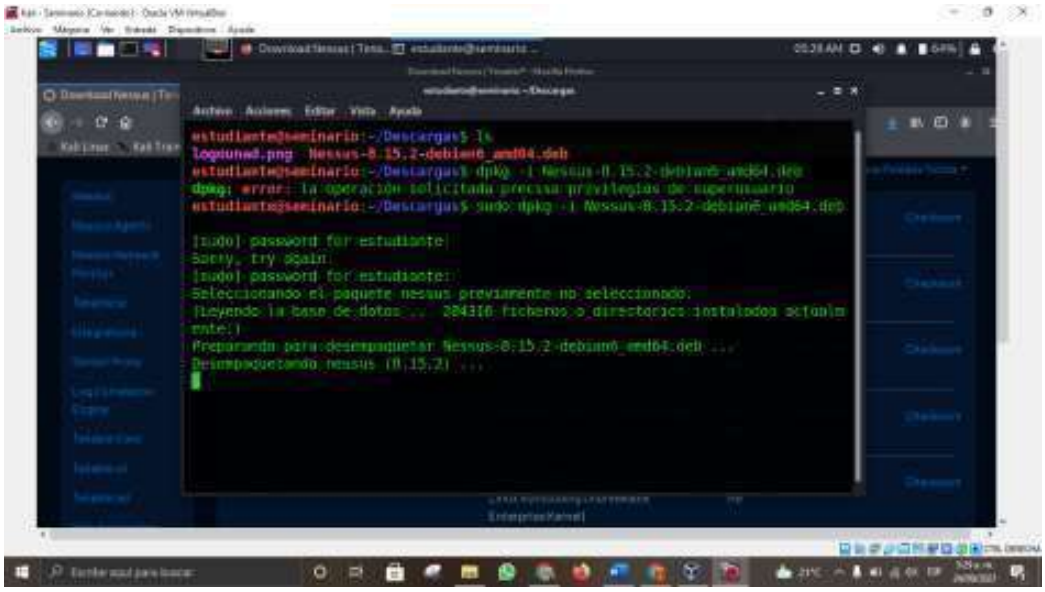


Figura 35 Iniciamos nessus

Inicializamos la aplicación la cual nos arroja los lincks de inicio y de ingreso como tal a ala palicacion lo obcervamos a continuacion:

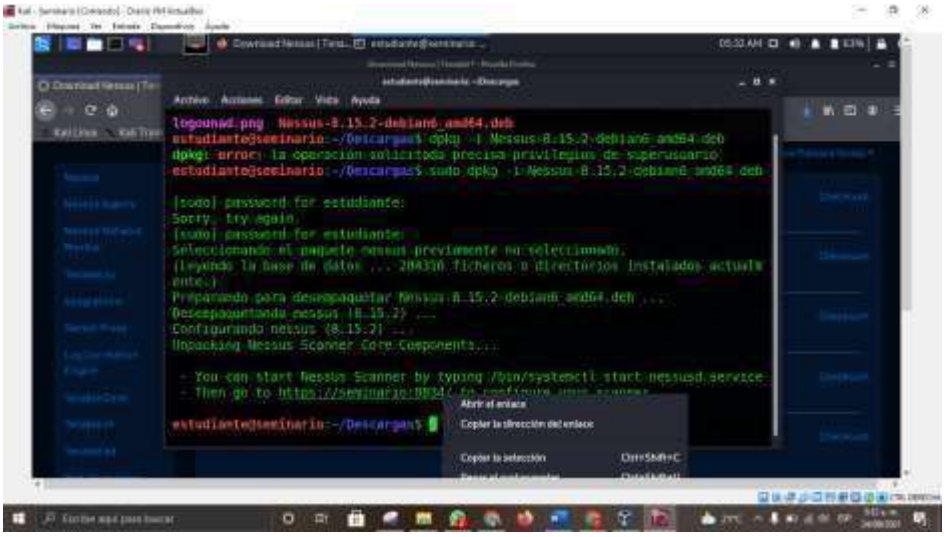


Figura 36 inicialización de la herramienta nessus

Procesemos a ingresar a la web de la herramienta que es donde esta funciona y la cual ya hemos inicializado previamente:

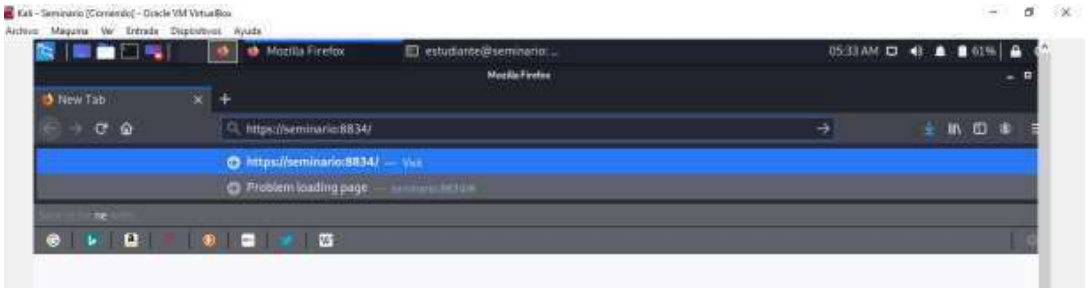


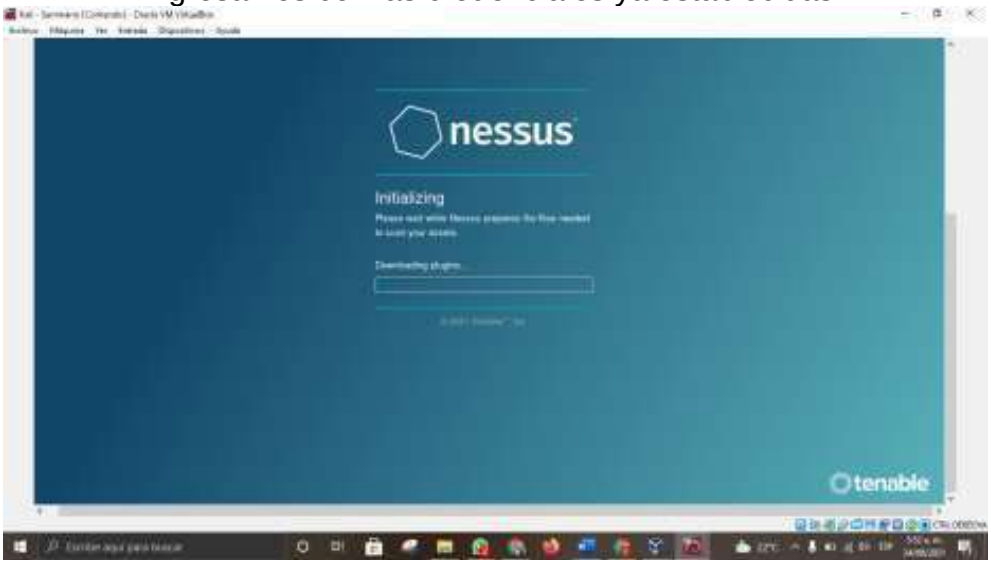
Figura 37 ingreso a la web de nessus para el proceso de escaneo

Procedemos a esperar que los componentes carguen para ingresar a la herramienta:

Figura 38 inserción del Código de ingreso a nessus

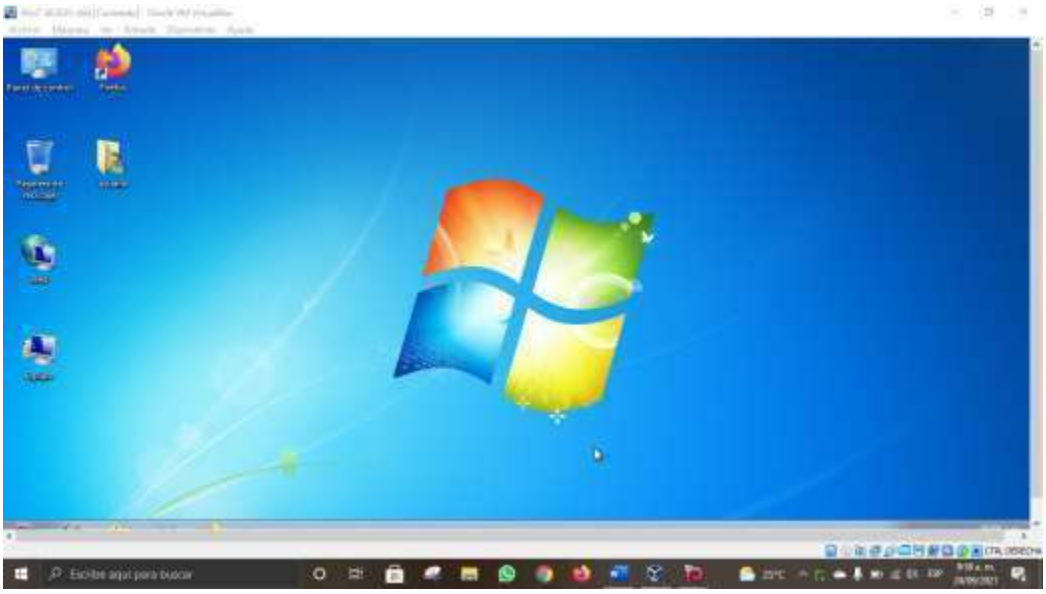
Figura 39 ingreso a nessus

Ingresamos con las credenciales ya establecidas.



procedemos a inicializar la maquina Windows x 64 a la cual es la que se le realizara el respectivo escaneo:

Figura 40 Iniciamos maquina Windows la cual es la que se le realizara el escaneo



Empezamos el proceso de escaneo donde se adicionan los datos de la maquina a la cual le realizaremos el escaneo:

Procedemos a ejecutar el escaneo ingresando los datos:

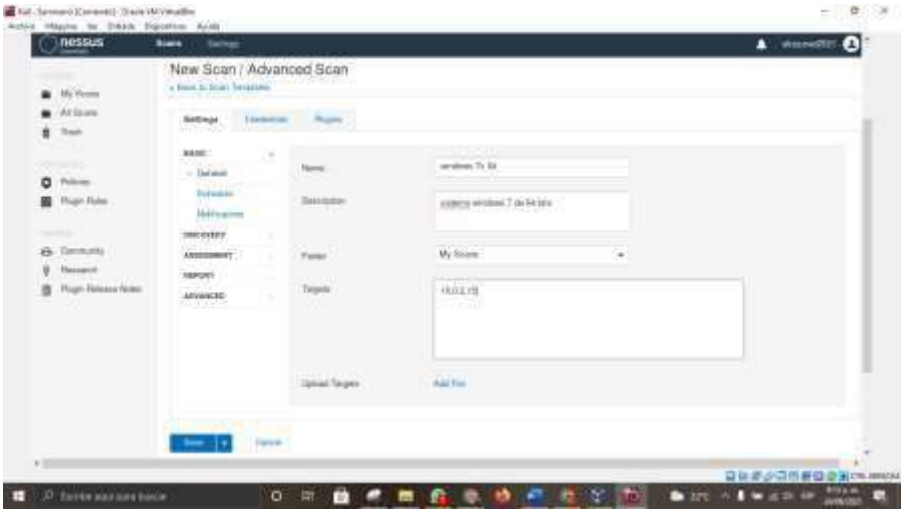


Figura 41 escaneo con Nessus

Obtenemos los resultados los cuales nos arrojan unas vulnerabilidades nivel medio como podemos

ver ninguna crítica:

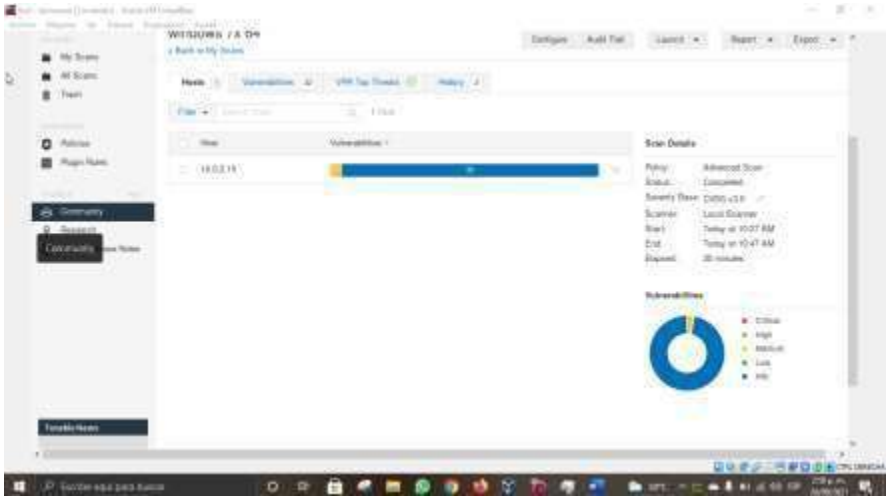
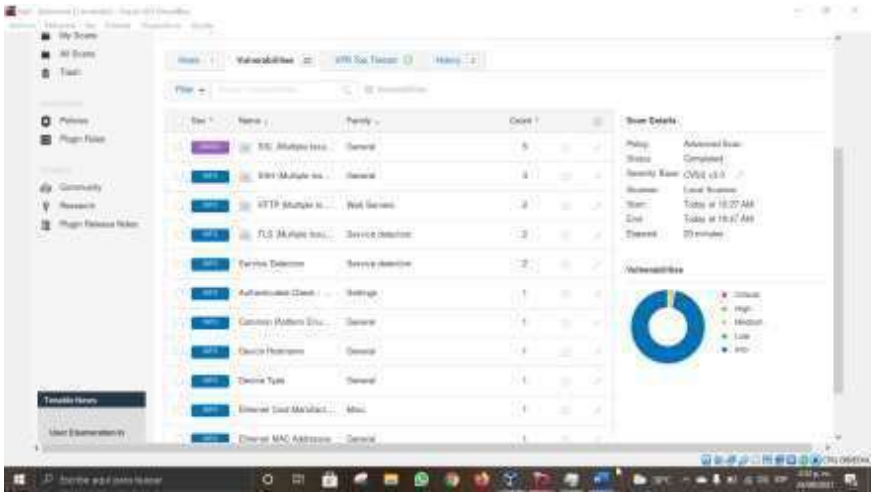


Figura 42 escaneo con nessus



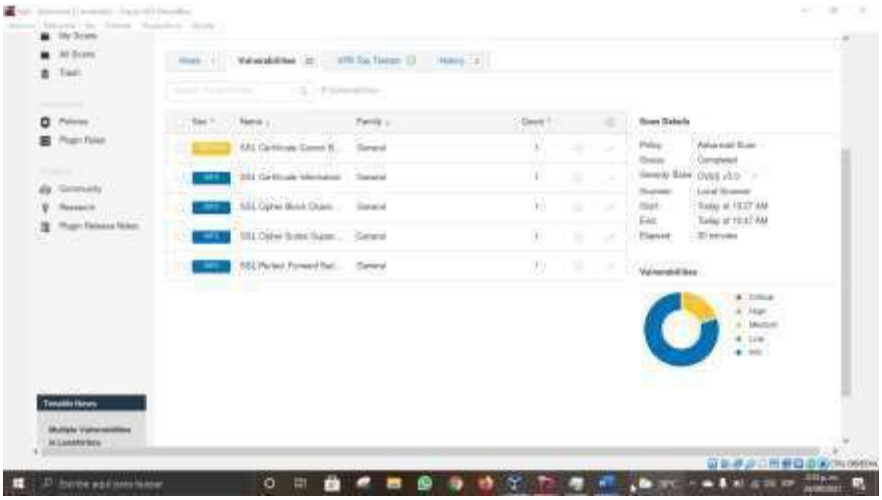


Figura 43 resultados nessus

Observamos en la imagen anterior y la siguiente el detalle de el escaneo y el detalle especifico de la vulnerabilidad nivel medio que se encontró.

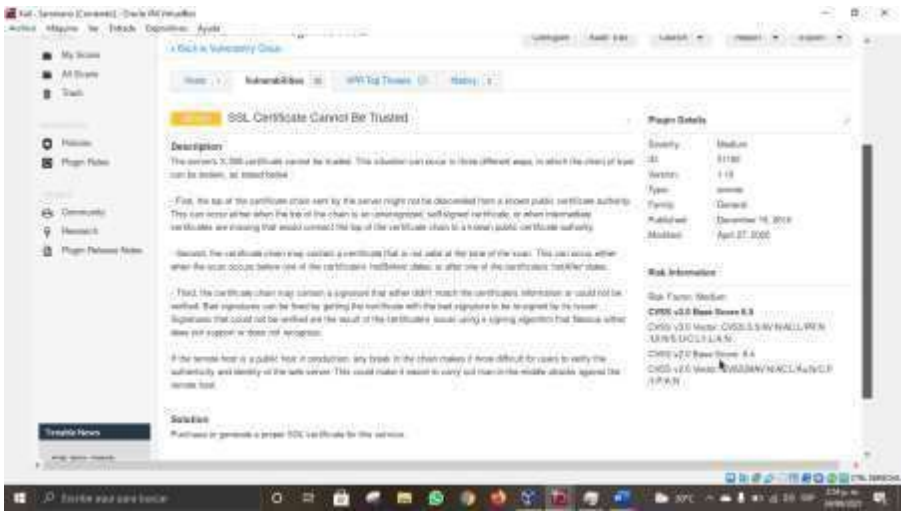


Figura 44 resultados nessus

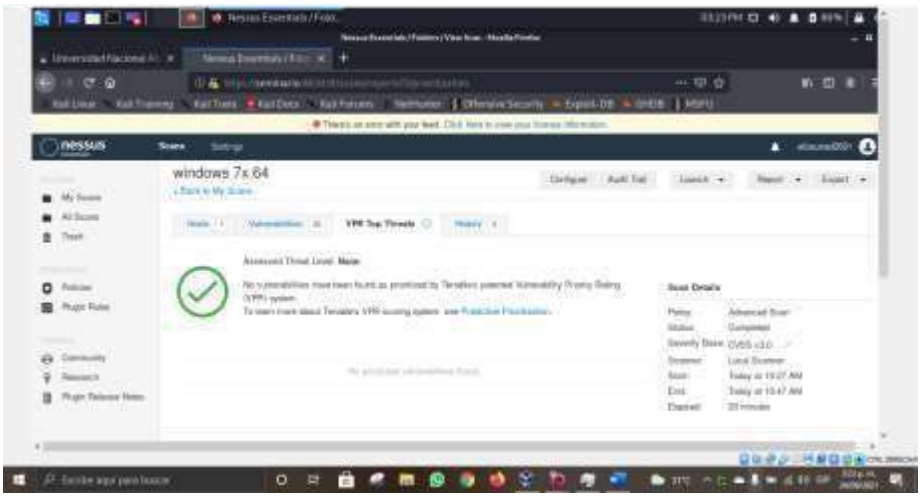


Figura 45 resultados nessus

Finalizamos con el reporte de estado de la maquina en cuestión.

3.4. EXPLICACION DE EL EFECTO DEL ATAQUE A LA MAQUINA (WINDOWS 7 X64).

Bueno inicialmente el tema de la penetración mediante distintos métodos y pruebas en las cuales se identifican las debilidades y puntos débiles de los programas y a su vez las vulnerabilidades.

En este proceso podemos evidenciar mediante la simulación métodos que un atacante puede utilizar para entrar a una organización a nivel de accesos sabemos que en cuanto al sistema operativo windows vulnerabilidades son explotadas mediante o atreves de los puertos en este caso el 445 lo que nos va a hacer la tarea más sencilla y va a permitir que mediante un exploit y claro esta y un payload únicamente con la ip se consiga la Shell remota.

La herramienta utilizada para el ataque (Metasploit) esta herramienta nos va a proporcionar una infraestructura para automatizar tareas rutinarias y complejas permitiendo la identificación de fallas dentro de una organización

3.5. EXPLOTACION DE VULNERABILIDADES

Procedemos a iniciar la herramienta de metaexploit para realizar la explotación de vulnerabilidades:

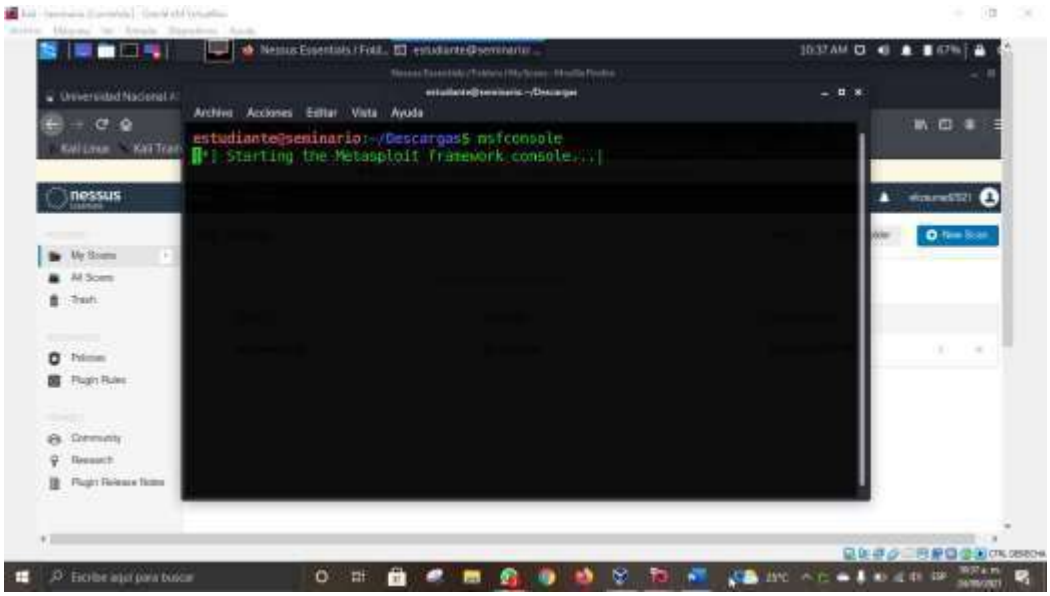
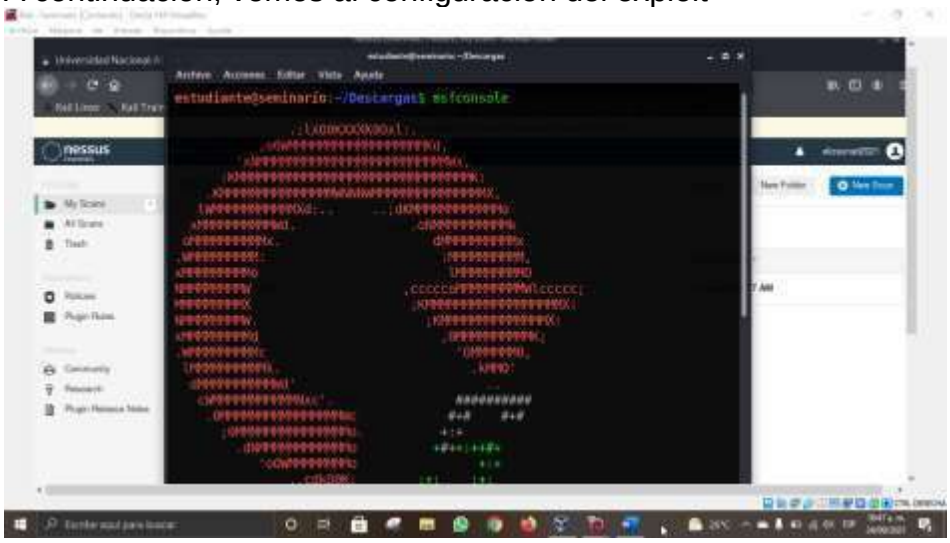


Figura 46 Inicio Metasploit Framework

A continuación, vemos al configuración del exploit



Evidenciamos el proceso que se lleva a cabo la herramienta.
Figura 47 Proceso de metasploit

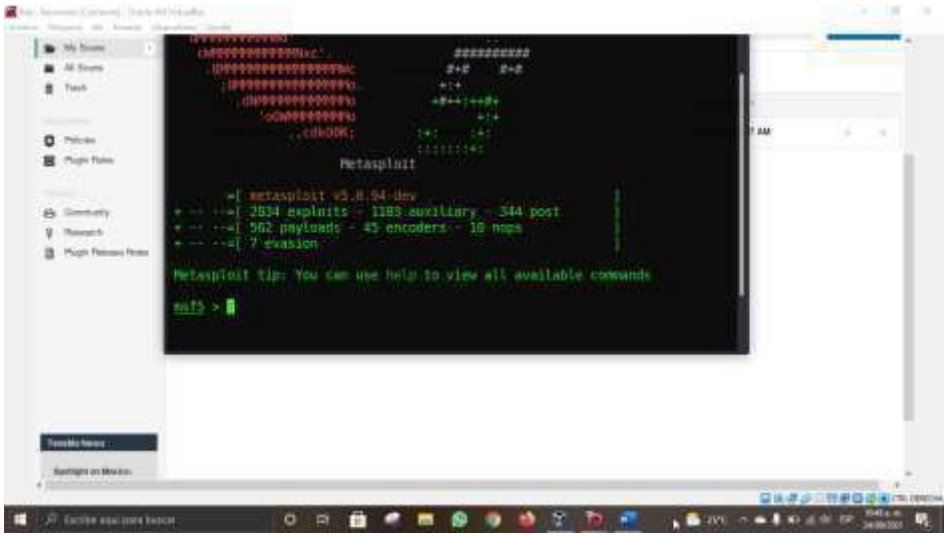


Figura 48 Proceso de metasploit Resultados

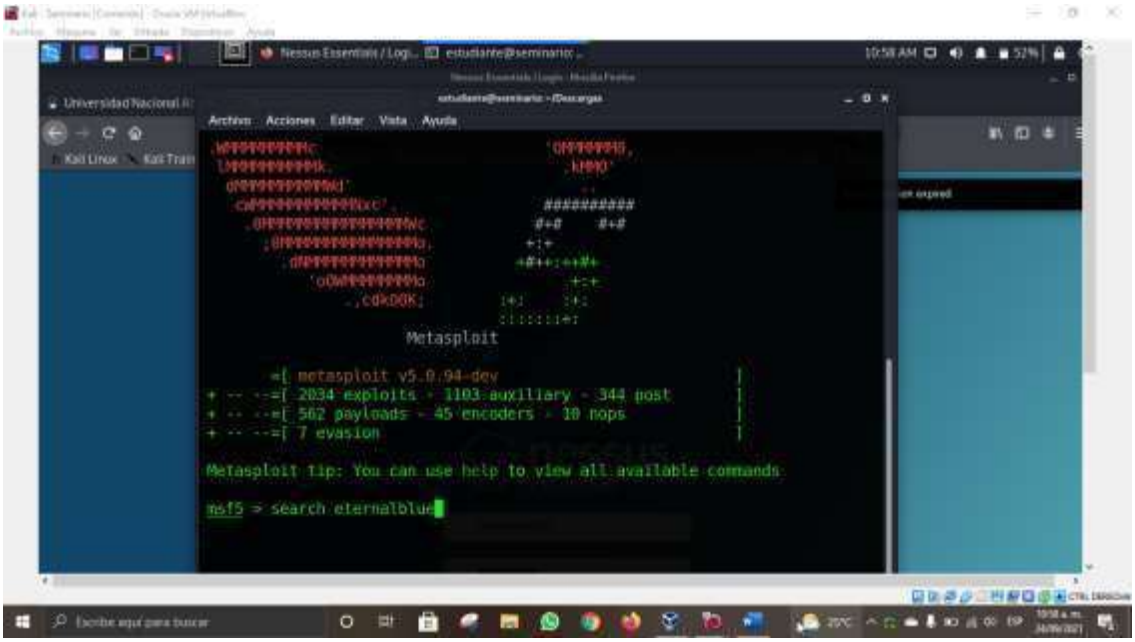


Figura 49 Realizamos ahora la búsqueda de exploit: usamos el comando search eternalblue

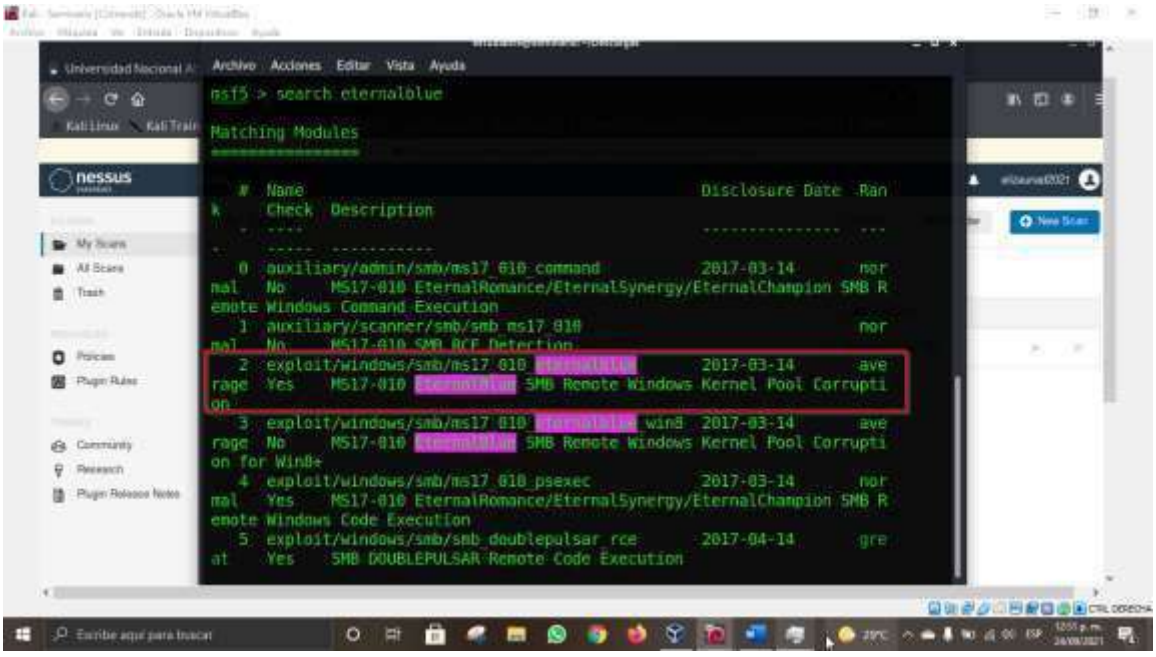


Figura 50 Resultados comando search eternalblue

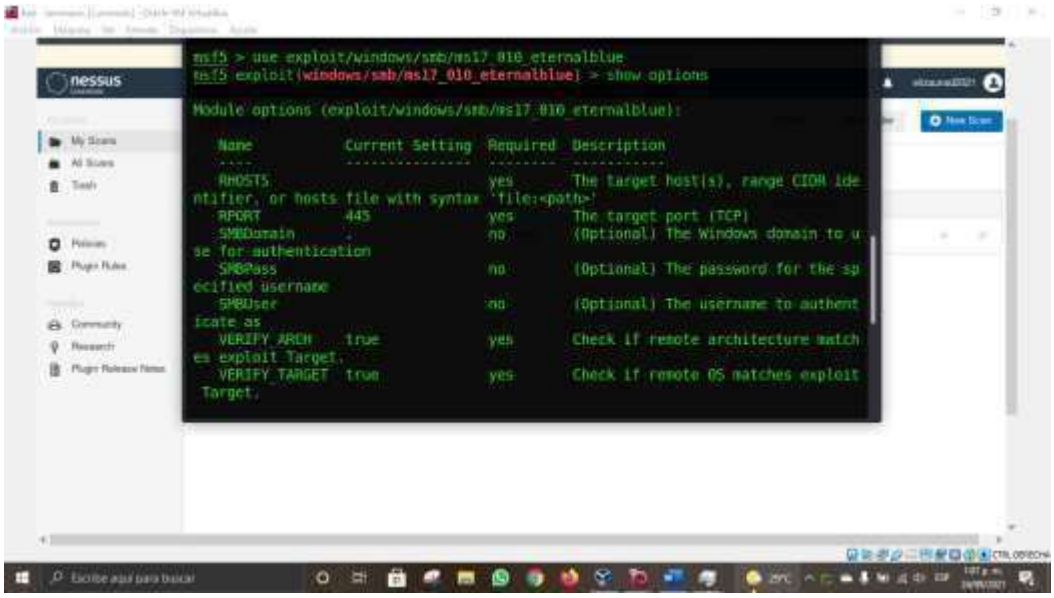


Figura 51 selección y configuración del Exploit

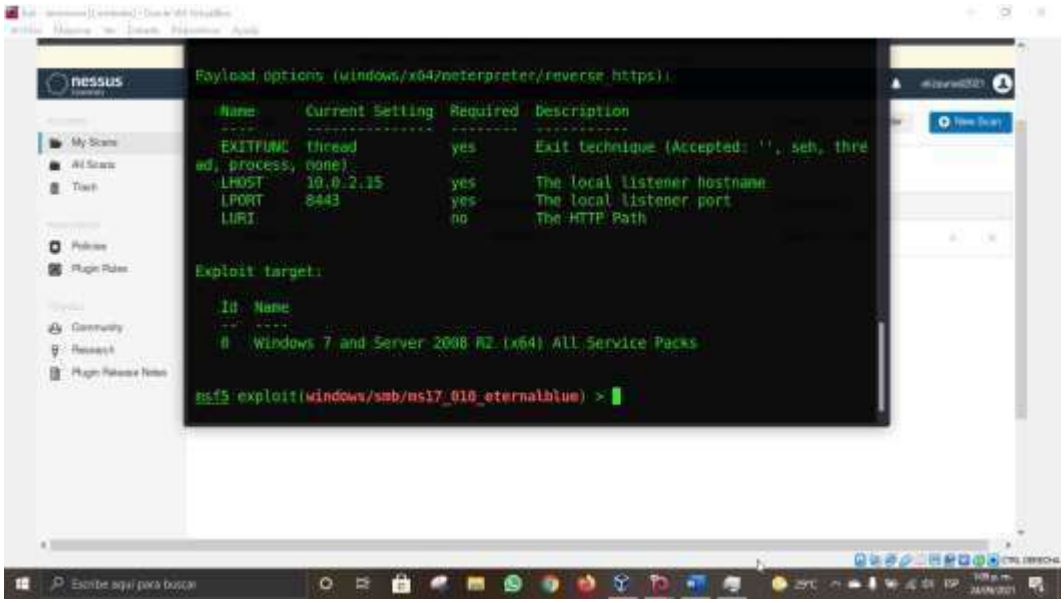


Figura 52 continuacion de la selección y configuración del Exploit

Procedemos a atacar el hots correspondiente a la ip de la maquina Windows 7 x 64 de hay procedemos a realizar el cargue y configuración del payload-ip.

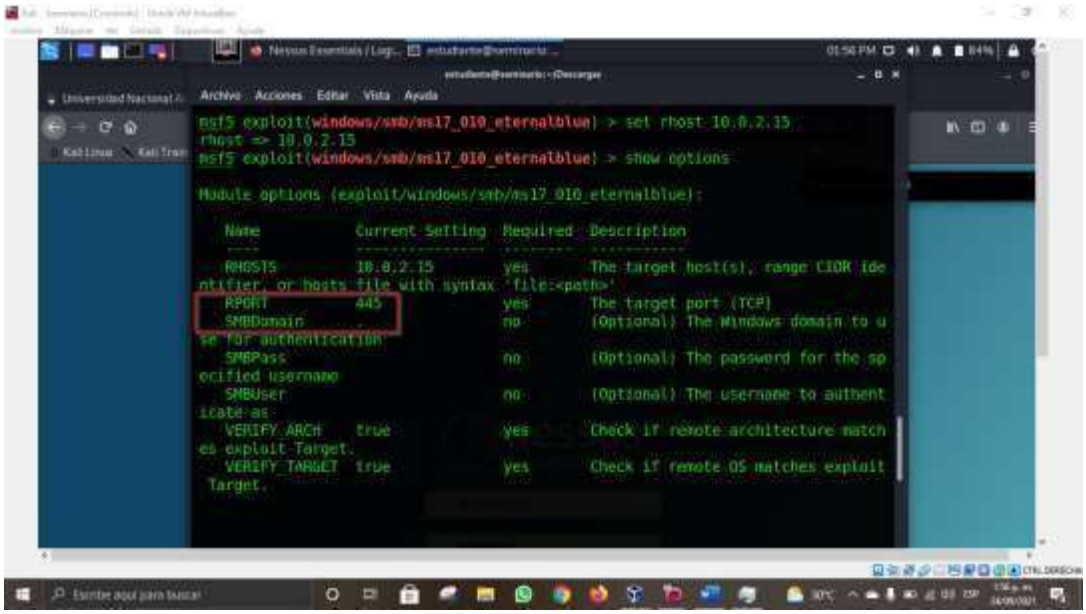


Figura 53 host a atacar con la IP de la máquina Windows 7X64

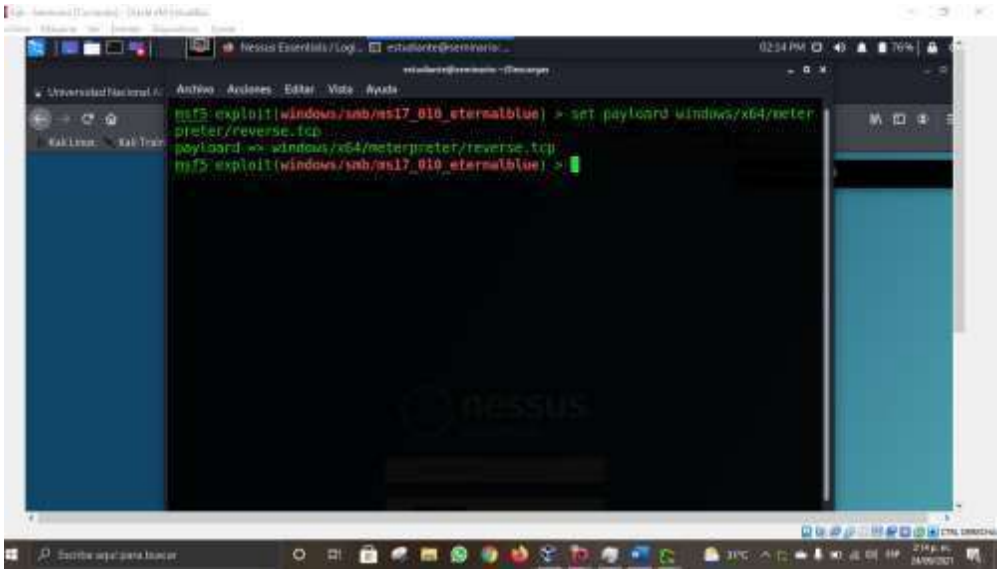


Figura 54 cargue y configuración del Payload-IP de la máquina atacante

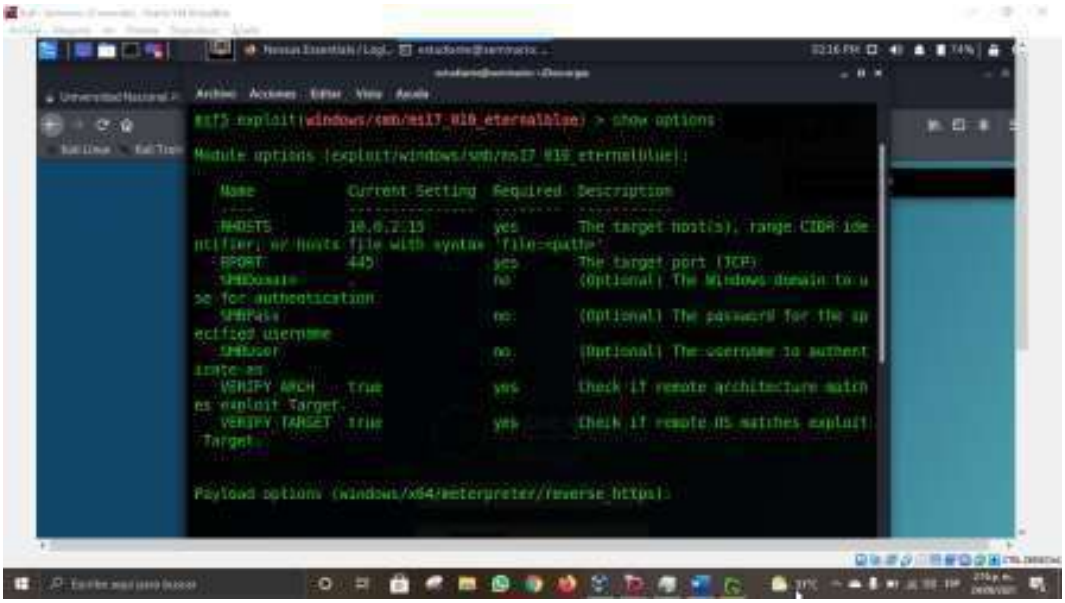


Figura 55 Figura 51 cargue y configuración del Payload-IP de la máquina atacante 2

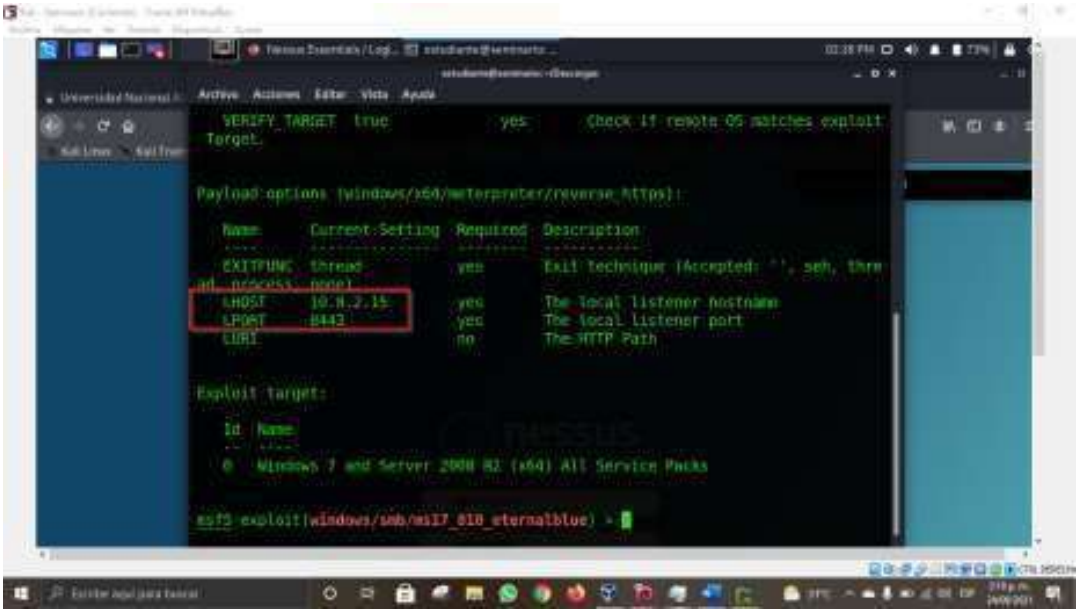


Figura 56 Resultados exploit

Se generan los resultados esperados y se procede al ataque con exploit a continuación evidenciamos la intrusión que se logra hacer.

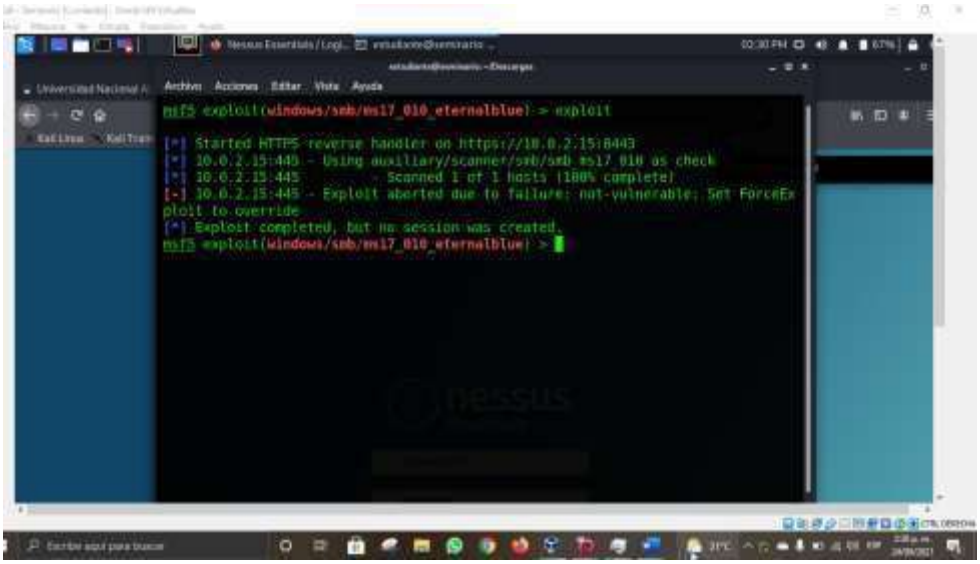


Figura 57 ataque con exploit intrusión realizada

4. **CONTENCIÓN DE ATAQUES INFORMÁTICOS**

4.1 ANÁLISIS CON ACCIONES NECESARIAS PARA CONTENER UN ATAQUE EN TIEMPO REAL.

En el proceso del ataque en tiempo real realizaremos como primera medida un trabajo de **prevención** donde definimos procedimientos preventivos y lo que hacemos es reunir la mayor cantidad de información, pero siempre manteniendo la comunicación con el cliente dándole la seguridad y concientizándolo se lo que está pasando y como debe estar alerta. Los métodos de prevención que debemos comunicar al cliente y tener en cuenta nosotros también es las copias de seguridad es importante mantener actualizados los sistemas y los equipos de tecnología, se debe tener en constante actualizarse los sistemas de antivirus, contraseñas seguras y contante escaneo de vulnerabilidades.

Como segunda medida en este proceso sería el paso de la **detección** que consiste en averiguar he indagar en el tipo de ataque que se está realizando se debe tener en cuenta todos los patrones alcance, monitoreo se deben incluir todo lo concerniente y la información necesaria normalmente los ataques más comunes son los **Troyanos**: Software malicioso que se hace pasar como un programa, pero al ser instalado tiene acceso remoto al servidor y los quipos que estén conectados a este Virus: Tiene el alcance de manipular el buen funcionamiento del equipo también está el **Phising**: Cuando por medio de comunicación electrónica simula ser una empresa yaccede a datos personales y uno de los más comunes como el de **Denegación de servicios DoS:** Cuando el atacante evita que los usuarios accedan a información y servicios.

El paso 3 sería uno de los más importantes que es el paso de **recuperación** aquí buscaremos mitigar las consecuencias que haya dejado el ataque esto por medio del uso de una herramienta de contención que nos permita limitar el impacto y consecuencias del ataque ahora bien es necesario utilizar las medidas y las herramientas necesarias para detener el ataque removiendo la amenaza y así crear planes de contingencia donde se contemple desde robo de información, suplantación, bloqueo del sistema y hasta el borrador de la información que es vital esto para así poder volver a una etapa normal de funcionamiento teniendo en cuenta la implantación de medidas como backups y copias de seguridad.

Y lo que consideramos como el paso final a seguir es dar a conocer la información de lo acontecido a los interesados como lo son los clientes, trabajadores y a los respectivos entes para denunciarlo, dando a conocer las consecuencias del ataque, las medidas adoptadas después del daño ocasionado ahora bien debe haber una disposición de nuestra parte para responder dudas que puedan surgir y una total comunicación con los involucrados.

4.2 INFORME DE ACCIONES DE HARDENIZACIÓN A IMPLEMENTAR PARA EVITAR QUE SUCEDAN ATAQUES DE SEGURIDAD INFORMÁTICA.

Cuando hablamos de Hardenización hablamos de seguridad total de asegurar el sistema de información de tal forma que le hacemos la vida más difícil al atacante esto con el fin de ir reduciendo las vulnerabilidades eliminando servicios, usuarios, funciones u otros que no son necesarios llevando a endurecer la seguridad, lo que podemos hacer para lograr endurecer la seguridad es establecer primero políticas de seguridad y herramientas de trabajo que nos permitan lograr ese objetivo con esto realizaremos una autenticación mediante llaves SSH que nos permita que el se cuente con una llave secreta y una que será la que se compartirá con los otros usuarios sin ninguna restricción.

Utilizaremos también un cortafuegos el cual se encargará de inspeccionar los servicios expuestos en la red teniendo en cuenta que hay servicios públicos los cuales no tienen ninguna restricción y estan disponibles para todos como por ejemplo el servidor web, es importante la utilización de VPN y redes privadas las cuales nos permiten crear conexiones remotas disponibles exclusivamente para ciertos usuarios/servidores.

Y ya como tema de revisión procederíamos a realizar las respectivas auditorias como la auditoria de servicio la cual nos da a conocer que servicios se ejecutan, los puntos débiles expuestos al ataque, que puertos son utilizados en cada comunicación y cuales protocolos son aceptados, también auditoria de archivos en donde se realizara la comparación del sistema actual con uno que se encuentre en los archivos revisando actividades no usuales o no autorizadas e importante para

para revisar si el sistema ha tenido algún cambio y brinda la certeza de no haber sido alterado.

Una vez realizásemos estos procesos procedemos a realizar ya la parte de protección donde primero aislamos los procesos en donde el servidor individual en donde se ejecuta en su propio espacio dedicado creando un aislamiento, dependiendo de las características dela aplicación y de las condiciones en que se encuentre la infraestructura limitando así el acceso a intrusos a su vez se realiza de igual importancia procedemos a realizar una protección de Hardware esto con el fin de que al arrancar la maquina se establezcan contraseñas complejas y denegar el encendido del sistema a menos que se realice desde el disco duro.
Se debe realizar una instalación correcta y completa de todos los componentes del sistema operativo y Instalar programas de seguridad como Antivirus, Antispyware y Antispam, es importante que todo debe tener un orden por lo que procedemos a la configuración de la política local del sistema en donde se busca que se cumpla con los requisitos de complejidad de contraseñas, des habilitación de las cuentas administrador e invitado y limitar los privilegios de los usuarios.

4.3 ANÁLISIS SOBRE LAS DIFERENCIAS ENTRE EL EQUIPO DE BLUE TEAM Y EL EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

Es importante destacar que el equipo blue team es un equipo de defensa es decir su trabajo va siempre orientado a la seguridad defensiva siendo así mostraremos a continuación las diferencias:

EQUIPO BLUE TEAM	**EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS**
Análisis forense de las máquinas afectadas, propuesta de soluciones y establece medidas de detección para futuros casos.	Endurecimiento de software y estructura para reducir el número de incidencias a largo plazo
Vigilancia Constante lo que lleva a un proceso de documentación completa que permite ejecutar procesos en bienestar de la organización	Vigilancia periódica ya que los objetivos de este equipo son específicos y en algunos casos ha servido para que ataques no se lleven a cabo

Enfocado a la contención de ataques y proponer mejoras para la Ciberseguridad de una Organización	Gestiona incidencias de una organización mayor (Gobierno, empresa, universidad red)	
Verifica la efectividad de las medidas de seguridad	Respuesta rápida y efectiva, lo cual le permitirá a la organización operar con total, normalidad	
Análisis y evaluación de riesgos, auditorias e implementación de soluciones SIEM	Analiza las situaciones y responde a las incidencias	
Analiza comportamientos del sistema, aplicaciones y personas	Identifica los causantes del incidente y las consecuencias que conlleva mediante la preservación y documentación de la evidencia.	
Este equipo se basa en la seguridad defensiva.	El equipo de respuesta se enfoca en las incidencias de seguridad informática	
Rastrea incidentes de Ciberseguridad	Gestión de incidentes	

Tabla 1 Diferencias entre el equipo blue team y red team

4.4 ANÁLISIS DEL TRABAJO CIS “CENTER FOR INTERNET SECURITY” COMO PROPUESTA DE ASEGURAMIENTO POR PARTE DE UN EQUIPO DE BLUE TEAM.

Como primera medida sabemos y establecemos que propósito tendría el CIS ya sabiendo y definiendo que es podríamos definir para que lo utilizásemos entonces el Centro para la seguridad de internet su trabajo principal es identificar, ejecutar, validar y mantener soluciones para ciberdefensa esto claro está con bases sólidas fundamentadas en la experiencia de los profesionales en esta rama.

Con esto claro y sabiendo que contamos con una herramienta poderosa contra los ciberataques partiendo de esto lo utilizaría para controlar en tiempo real cuando el atacante espera la oportunidad de que se conecten a la red equipos que no cuentan con la seguridad necesaria es decir que se encuentran desprotegidos cuando aprovecha los avisos de seguridad y cuando aprovecha el mal uso de privilegios como ser engañados para abrir un archivo malicioso o ingresar a páginas que permiten ala atacante acceder alsistema.

La idea principal de contar con el apoyo del CIS es poder realizar pruebas es identificar cuando se explota ciertas vulnerabilidades como puertos abiertos, contraseñas/cuentasinseguras o predeterminadas y preinstalación de software que no es necesario, ahora bien es necesario aprovechar esta ayuda de la CIS para indagar y registrar las inconsistencias en el registro que oculta ubicación, software malicioso y actividades a ejecutar en las maquinas victimas pasa prácticamente desapercibido buscar servicios mal configurados servicios mal configurados, contraseñas para ser explotados.

Utilizaremos para descubrir y explotar cuentas de usuario que por diferentes motivos ya no se utilizan, pero son legítimas y así suplantarlas lo que le permite no ser descubierto y a su vez aprovechan las vulnerabilidades de software como errores de programación, delógica, y gestión de memoria deficiente.

En conclusión, la ventaja que genera CIS es muy grande a la hora de defender un sistema contra los ataques de ciberseguridad cosa que es vital en el equipo BLUE TEAM.

4.5 ANÁLISIS DE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALESDE UN SIEM

Cuando hablamos de SIEM Seguridad de Información y Gestión de eventos hablamos de un conjunto de funciones como detectar amenazas potenciales y resolverlas con eficacia en el menor tiempo posible lo cual es un rol importantísimo en el campo de la seguridad a continuación describiremos sus funciones y características:

Funciones:

Detecta amenazas, ataques, mal funcionamiento, mal uso pudiendo precisar cuáles son de mayor riesgo.	Da una solución y respuesta de manera rápida y eficaz la respuesta ante amenazas

Presenta en tiempo real análisis de ataques de seguridad tanto hardware como software alertando, dependiendo el progreso de estas.	Centraliza el almacenamiento en un solo punto y acorta los tiempos de actuación.
Presenta una visión global de la seguridad en cuanto a las tecnologías de la información.	

Tabla 2 Funciones de un SIEM

Características:

Arquitectura: Proporciona los requisitos mínimos y es adaptable a cualquier cambio	Administración y registro de datos: Capaz de recolectar todo lo que genere ya que trabaja con gran cantidad de datos
Monitoreo en tiempo real: En cuanto a detección de amenazas, respuesta a incidentes, creación de indicadores y priorización de alertas	Análisis: Detección de eventos discretos, comportamientos anómalos, coincidencias en listas blancas etc.

Monitoreo de datos y aplicaciones: Integración de diferentes aplicaciones, fuentes de datos e interfaz y así lograr la extracción, clasificación o visibilidad de la información	Amenaza y contexto: Permite la validación de eventos detectados para así evaluar los riesgos y priorizar los de mayor impacto
Contexto de usuario y monitoreo: Dar a conocer las infracciones de políticas, bloqueo y desbloqueos de cuentas, falta de uso de cuentas, cambios en privilegios, cuentas promiscuas etc.	Administración de incidentes: Permite notificar a usuarios específicos, configuración de alertas y agregar acciones automatizadas
Herramientas de detección de amenazas: Crear o implementar aplicaciones de seguridad.	

Tabla 3 Características de un SIEM

4.6 INFORME DE LAS HERRAMIENTAS ELEGIDAS QUE PERMITAN CONTENER ATAQUES INFORMÁTICOS.

Se seleccionaron 3 herramientas que permitan contener ataques y que sean de licencia GPL:

OPENWIPS-NG	SNORT	OSSEC
es un sistema de detección de y prevención de ataques inalámbricos que se basa en tres partes: Sensores: Responden a las amenazas, capturan el tráfico y lo envían para su posterior análisis. Servidores: Alerta y responde ante amenazas, analiza los datos enviados por los sensores Interfaces: Muestra detalles sobre los ataques en las redes inalámbricas	es una herramienta de código abierto para análisis y registro de paquetes en tiempo real, capaz de identificar los ataques DoS y DDoS, es útil para detectar exploits, gusanos y exploración de puertos. Durante su ejecución dará a conocer si el tráfico coincide con alguna de la regla de ser así rechazará el tráfico permitiendo así bloquear al atacante.	es una herramienta gratuita: Permite realizar análisis de registro Detección de rootkit, Verificación de integridad e información de alertas, Permite administrar y llevar fácilmente el monitoreo de varios sistemas, Lleva el registro de varios dispositivos y formatos gracias a que cuenta con un motor de análisis, Puede realizar la detección de ataques para casi todos los sistemas operativos.

CONCLUSIONES

La base de todo proyecto, empresa o a nivel personal incluso de las relaciones personales es la comunicación y la información precisa es pensar antes de cualquier cosa en fin es supremamente importante que estemos bien informados en cuanto a las leyes que rigen en nuestro país en este caso en Colombia sobre la protección de la información, la protección de datos personales y de todos los riesgos que pueden o presentan con la información al estar en las manos de un tercero o expuesta a malos manejos.

Podemos concluir también que al ser profesionales en el área de la ciberseguridad estamos amparados como profesionales con un código de ética y conducta para poder llevar a cabo un trabajo profesional y exitoso, pudimos evidenciar y concluir a raíz de los casos presentados que no es más importante el dinero de una oferta laboral a la paz y la tranquilidad de un buen trabajo realizado con respeto y legalidad además los beneficios recibidos son mayores.

Se evidencio el proceso total del caso de penetración el cual tiene cuatro etapas definidas y estructuradas que nos permitió analizar el sistema de información n en buscando vulnerabilidades y permitiendo así el poder presentar un informe concreto de los hallazgos y la explotación realizada a esas vulnerabilidades al realizar este proceso se nos permitió identificar aquellas debilidades y vulnerabilidades para realizar el ataque y así obtener información valiosa del objetivo, se utiliza Nmap ,Nessus y Metasploit para dicho proceso.

Es importante que al momento de seleccionar una herramienta de contención se tengan en cuenta los factores del sistema y obviamente la capacidad de respuesta ante las incidencias presentadas en tiempo real, es en este momento donde realmente se evidencia o más bien se evalúa la capacidad tanto del experto como de la herramienta seleccionada.

RECOMENDACIONES

Las recomendaciones son una parte crucial en el proceso de seguridad informática es importante tener en cuenta todos los aspectos y herramientas para llevar a cabo un proceso exitoso dado es se recomienda que:

Las empresas tengan activado y actualizado software de seguridad, sistema operativo y programas ya que esto minimizará los riesgos y todo pueda tener buen funcionamiento y tendrá un nivel de pérdida o posibilidad mínimos de ataques.

Se recomienda estar constantemente actualizados en cuanto a las normas y leyes que rigen en nuestro país, así como el código de ética que nos rige como profesionales sobre todo lo que tiene que ver con delitos informáticos y sobre la protección de datos personales.

Las empresas deben estar actualizados en todos los procesos de ciberseguridad, así como las herramientas diseñadas para la detección de vulnerabilidades, explotación y contención de ataques, así como el manejo y mantenimiento de estas igualmente las estrategias del trabajo en equipo.

BIBLIOGRAFIA

COLOMBIA. CODIGO PENAL. Ley 1273. (5, enero, 2009). “Por la cual se crea un nuevo bien jurídico tutelado - denominado “De la protección de la información y de los datos” Y se preservan integralmente de los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1377 (27, junio, 2013) “Por lo cual se reglamenta parcialmente la Ley 1581 de 2012”

REVISTA HACKING ÉTICO “Fases del pentesting, aprende como hacer auditoria de hacking a empresas”. Internet: (https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-como-hacer.html)

OPENWEBINARS “Qué es metasploit framework”. Internet: (https://openwebinars.net/blog/que-es-metasploit/)

MELIVESECURITY “Cómo utilizar OpenVAS para la evaluación de vulnerabilidades”. Internet: (https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/)

ECURED “OpenVas”. Internet: (https://www.ecured.cu/OpenVas)

OPANDA “¿Qué es un exploit?)”. Internet: (https://www.pandasecurity.com/es/security-info/exploit/)

MELIVESECURITY “¿Sabes qué es un exploit y cómo funciona?”. Internet: (https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/#:~:text=Existe%20confusi%C3%B3n%20entre%20los%20usuarios,estos%20accedan%20a%20nuestro%20sistema.)

GFI LANGUARD 12 “Vulnerabilidades y exposiciones comunes (CVE)”. Internet: (https://manuals.gfi.com/es/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures_cve_.htm)

PCHARDWAREPRO “¿Qué es mestasploit y cómo utilizarlo correctamente”? Internet: (https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente/)

NESSUS “Instalación en Kali Linux” Internet video YouTube: https://www.youtube.com/watch?v=6erDDE5evIQ&feature=youtu.be

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION. Trabajos escritos: presentación y referencias bibliográficas. Sexta actualización. Bogotá: ICONTEC, 2008 110 p.

TECHTARGET, “Equipo de respuesta frente a incidencias de seguridad informática (CSIRT)”. Internet: https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT#:~:text=Un%20Equipo%20de%20Respuesta%20frente,o%20un%20grupo%20ad%20hoc

WELIVE SECURITY, “¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?”. Internet: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

CIS CENTER FOR INTERNET SECURITY, “CIS Benchmarks”. Internet: https://www.cisecurity.org/cis-benchmarks/

CIS. CENTER FOR INTERNET SECURITY, “CIS controls”. Internet: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

ANALIZADOR DE VULNERABILIDADES NESSUS “Hacking Ético Video Series #6”. Internet: (https://www.youtube.com/watch?v=7qJ1wNRkEt4&feature=youtu.be)

HACKLAB “Explotación de un servidor (Metasploitable) con Kali Linux” Internet: (https://www.youtube.com/watch?v=vW-agN1t9Rg&feature=youtu.be)

PENTESTING “Kali Linux – Metasploit VM” Internet: (https://www.youtube.com/watch?v=r7wJfOGsIr4&feature=youtu.be)

DELOITTE, “Pasos a seguir ante un ataque informático”. Internet: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

DSKconceta, “Medidas preventivas para evitar ataques informáticos” Internet: http://dskconecta.com/tecnoloxia/evitar-ataques-informaticos/

BLOG SMARTEKH, “¿Qué es hardening?”. Internet: https://blog.smartekh.com/que-es-hardening

UNIRrevista, “Red Team, Blue Team y Purple Team, ¿Cuáles son sus funciones y diferencias?”. Internet: https://www.unir.net/ingenieria/revista/noticias/red-blue-purple-team-ciberseguridad/549204773062/

IT DIGITAL Security, “¿Qué es un Blue Team y cómo trabaja?”. Internet: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

TECNICAS DE DETECCIÓN DE ATAQUES EN UN SISTEMA SIEM, “Security Information and Event Management”. Internet: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

A3SEC, “Capacidades que deben considerarse para la elección de un SIEM”. Internet: https://blog.a3sec.com/capacidades-que-deben-considerarse-para-la-seleccion-de-un-siem

TUYÚ TECHNOLOGY, “Soluciones SIEM permiten detectar amenazas de seguridad en tu empresa”. Internet: https://www.tuyu.es/soluciones-siem/

DATACOM.GLOBAL, “Cisco seguridad: Contención rápida de amenazas”. Internet: https://datacom.global/cisco-seguridad-deteccion-de-amenazas-en-las-organizaciones/

ONDATA INTERNATIONAL, “Guidance software: Herramientas de análisis forense”. Internet https://www.ondata.es/recuperar/forensics-guidance.htm

OPEN WEBINARS, “Las 8 mejores herramientas opensource”. Internet: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

ANEXOS

ANEXO A. PLANTILLA PRESENTACIÓN POWERPOINT

El Anexo referente a la presentación del informe final se encuentra en el siguiente Enlace:

DRIVE:

https://docs.google.com/presentation/d/1ObDRh-enFNB5GpWlwgYc40Df2QuYNjlHjYl7XgpgIfY/edit?usp=sharing

ANEXO B. VÍDEO SUSTENTACIÓN INFORME TÉCNICO

El Anexo referente al video de sustentación del informe final se encuentra en el siguiente Enlace:

DRIVE:

https://drive.google.com/file/d/1QYT1EL-ZSSp_-YSum7m-NArOJTQAEIt_/view?usp=sharing

YOUTUBE

https://youtu.be/UW6eBUAtURc