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

ANA DELCY NOMESQUE PATIÑO

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
PAIPA
2020

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

ANA DELCY NOMESQUE PATIÑO

SOCIALIZACIÓN INFORME TÉCNICO

DIRECTOR DE CURSO
M.Sc. 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
PAIPA
2020

Nota de Aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Paipa, (16 de Octubre de 2020)

A mi padre que desde el cielo me inspira cada día para salir adelante y a mi madre hermosa por su apoyo y dedicación, infinita gracias por todo, los amo…

CONTENIDO

LISTA DE FIGURAS

Pág.

GLOSARIO

BLUE TEAM: Un equipo azul es un grupo de personas que realiza un análisis de los sistemas de información para garantizar la seguridad, identificar fallas de seguridad, verificar la efectividad de cada medida de seguridad y asegurarse de que todas las medidas de seguridad continuarán siendo efectivas después de la implementación.

COPNIA: autoridad pública encargada de proteger a la sociedad del inadecuado ejercicio profesional de los ingenieros, profesionales afines y auxiliares, mediante la autorización, inspección, control y vigilancia, que se concreta, de acuerdo con las competencias otorgadas por la Ley, con la inscripción en el Registro Profesional y con la función como Tribunal de Ética Profesional.

CVE: es 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.

EXPLOIT DB: es un archivo definitivo de exploits y software vulnerable. Un gran recurso para probadores de penetración, investigadores de vulnerabilidades y adictos a la seguridad.

HOST: El término host o anfitrión se usa en informática para referirse a las computadoras u otros dispositivos conectados a una red que proveen y utilizan servicios de ella

METASPLOIT: es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

NESSUS: es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente que muestra el avance e informa sobre el estado de los escaneos.

NMAP: es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma.

OPENVAS: 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

OVA: Los Objetos Virtuales de Aprendizaje (OVA) son un conjunto de recursos digitales, auto contenible y reutilizable. Hacen posible el acceso a contenidos educativos, integrando diferentes elementos multimedia para presentar un recurso más didáctico para el estudiante.

PENTESTING: Una prueba de penetración, o pentest, es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos. El proceso consiste en identificar el o los sistemas del objetivo.

REDTEAM: Se denomina equipo rojo a un grupo independiente que ayuda a una organización a mejorarse a sí misma al oponerse al punto de vista de la organización a la que están ayudando. Por medio de la realización de ataques a un objetivo, se estudian sus debilidades.

VIRTUAL BOX: es un software de virtualización para arquitecturas x86/amd64. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización.

VULNERABILIDAD: es un término de ciberseguridad que se refiere a un defecto en un sistema que podría dejarlo desprotegido ante los atacantes. Bajo el mismo nombre también se engloba cualquier tipo de debilidad presente en un ordenador o en un conjunto de procedimientos que permita que la seguridad de la información esté expuesta a una amenaza.

RESUMEN

Hoy en día la tecnología ha avanzado y por esta razón las organizaciones deben estar actualizadas en cuanto a su infraestructura tecnológica sin dejar de lado la seguridad ya que existen amenazas y vulnerabilidades. En este informe se busca proponer mecanismos de contención de ataques minimizando las posibilidades de los mismos mediante el estudio de casos que se pueden presentar en las organizaciones Un ataque informático aprovecha cualquier vulnerabilidad en el software, hardware, o en las personas que administran la información con el fin de obtener un beneficio propio perjudicando directamente a una organización.

Para reducir el impacto generado por los ataques, existen equipos estratégicos en Ciberseguridad RedTeam y Blue Team que trabajan contra las actividades delictivas minimizando el campo de acción de estos ataques. En este informe también se dará a conocer como debe ser el actuar ante estos casos teniendo como partida los criterios éticos y legales que rigen nuestra profesión. Además se exponen las vulnerabilidades utilizando técnicas de intrusión para así formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades encontradas dentro del sistema de la organización

INTRODUCCIÓN

El siguiente trabajo presenta las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales. Descripción de herramientas para realizar pruebas de penetración y herramientas especializadas en Ciberseguridad

Como ingeniera de sistemas, estudiante de este seminario veo que el ámbito de la seguridad cobra más vigencia cada día, por esta razón debo tener en cuenta y dar a conocer los derechos y deberes en cuanto al manejo y trato de información dentro de una organización, así como protegerla de terceros que buscan otras finalidades como duplicación, alteración, robo, piratería abuso de confianza, beneficio propio o con otra intención.

Como futura especialista en seguridad informática debo establecer los criterios éticos y legales que rigen las leyes y el consejo de mi profesión; ya que serán de gran ayuda desde la firma de un contrato donde debo leer muy bien cada uno de los ítems que disponga la empresa contratante como funciones a realizar, el actuar ante ciertas situaciones y las limitaciones impuestas en el mismo. El ámbito de la Ciberseguridad cobra más vigencia cada día, por esta razón debo tener en cuenta y dar a conocer los derechos y deberes en cuanto al manejo y trato de información dentro de una empresa por esto es fundamental analizar las leyes colombianas y el código de ética que rigen para desempeñarnos como excelentes profesionales y mejores seres humanos en nuestro actuar.

En el siguiente informe se dará a conocer las etapas del pentesting, que herramienta utilizar en cada una de las fases y su finalidad dentro de un sistema para lograr el objetivo deseado. También se establecen estrategias de contención por medio del análisis de riesgos y vulnerabilidades en una infraestructura TI, dando a conocer las acciones para contener un ataque en tiempo real, teniendo en cuenta las funciones y características de la informática SIEM y seleccionando correctamente las herramientas de contención a utilizar.

El ámbito de la Ciberseguridad cobra más vigencia cada día, por esto es de suma importancia saber que herramientas de contención de ataques manipular, 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.

OBJETIVOS

OBJETIVO GENERAL:
Evaluar las diferencias entre los equipos RedTeam Y blueTeam para definir roles y responsabilidades a ejecutar dentro de una organización

OBJETIVOS ESPECIFICOS:

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

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

1. ETAPA CONCEPTOS EQUIPOS DE SEGURIDAD

1.1 LEYES SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES

Características principales de la Leyes 1273 de 2009 y 1581 de 2012

1.1.1 Ley 1273 de 2009: Ésta ley habla de la pena de prisión y multa que puede incurrir una persona no autorizada al realizar las siguientes acciones:

CAPITULO PRIMERO: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos
Artículo 269A: El abuso al acceder a información sea protegida o no
Artículo 269B: Impedir el normal funcionamiento de un sistema o red
Artículo 269C: Cuando sin orden judicial se acceda a datos de un sistema
Artículo 269D: Destruir, eliminar o alterar datos de un sistema informático
Artículo 269E: Fabricar, comprar, vender, introducir o extraer software malicioso dentro del territorio Colombiano
Artículo 269F: Manipular de alguna manera datos personales alojados en bases de datos y demás para beneficio propio o de un tercero
Artículo 269G: Diseñar, traficar o enviar páginas electrónicas, enlaces o ventanas emergentes, alterar nombres de dominio con el objetivo de que el usuario crea ingresar a su sitio normalmente
Artículo 269H: Se ampliarán las penas si realiza: Sobre sistemas estatales u oficiales, sector financiero, nacionales o extranjeros, si es servidor Público, si se presenta abuso de confianza, si se da información para perjudicar a otro, para beneficio propio o de un tercero, con intención terrorista, manipulando una tercera persona y si el que incurrir en los delitos es el responsable de administrar la información se le inhabilitará de sus funciones.

CAPITULO SEGUNDO: De los atentados informáticos y otras infracciones.
Artículo 269I: Cuando valiéndose del uso de un sistema o red suplanta a un usuario ante los sistemas de autorización y autenticación
Artículo 269J: Cuando mediante engaño o manipulación informática consiga transferir sin consentimiento

1.1.2 Ley 1581 de 2012: Ésta ley habla de la autorización, tratamiento, políticas y transferencias de datos así como los derechos con que cuanta toda persona a la hora de conocer, actualizar y confirmar los datos recogidos sobre ellos.

Capítulo 1 Disposiciones generales: En el campo personal y domestico el responsable debe comunicar al titular sobre la aplicación de la política de tratamiento y la finalidad que se le van a dar a sus datos
Capítulo 2 Autorización: Solo se solicitarán los datos que sean necesarios para la finalidad para lo cual son requeridos, los datos públicos podrán ser manejados por

cualquier persona mientras que si son datos sensibles el titular no está obligado a autorizar su tratamiento y la manera de autorizarlo se dará de forma escrita, verbal o mediante conductas aprobadas. Se deberá disponer de medios de fácil acceso y gratuitos en caso de que el titular desea eliminar algún dato o anular la autorización. El tratamiento de datos de menores de edad está prohibido, solo cuando se respete sus derechos fundamentales y el interés superior de los mismos el representante autorizará.

Capítulo 3 Políticas de tratamiento: Deben ser redactadas en un lenguaje claro y sencillo de entender y reposar en medio físico y electrónico de haber algún cambio debe ser notificado y garantizar que se le informará al titular

Capítulo 4 Ejercicio de los derechos de los titulares: Los derechos podrán ejercerse por el titular, sucesores, representante y por estipulación a favor de otro o para otro

Capítulo 5 Transferencias y transmisiones internacionales de datos personales: En el tratamiento deben reposar los alcances, siempre velando por la seguridad de los datos personales y guardando confidencialidad de los mismos

Capítulo 6 Responsabilidad demostrada frente al tratamiento de datos personales: Los responsables deben demostrar que implementan medidas apropiadas y efectivas para cumplir con las leyes

1.2 HERRAMIENTAS UTILIZADAS EN LAS ETAPAS DEL PENTESTING

1.2.1 Recopilación de información: Conocer y disponer de la mayor cantidad de información del sistema que nos permita llevar a cabo el objetivo, en esta etapa utilizaría la herramienta Nmap

1.2.2 Búsqueda de vulnerabilidades: Se analiza la información recolectada en búsqueda de amenazas, utilizaría la herramienta Nessus

1.2.3 Explotación de vulnerabilidades: Una vez identificadas las vulnerabilidades se definirá como aprovecharlas y así comprometer el sistema, la herramienta a utilizar Metasploit

1.2.4 Elaboración de informe: Se describe detalladamente las vulnerabilidades encontradas y su respectiva explotación la cual permitirá al cliente tomar las decisiones pertinentes.

1.3 HERRAMIENTAS Y SOFTWARE ESPECIALIZADO DE CIBERSEGURIDAD

1.3.1 Herramientas:

Metasploit: Proyecto de código abierto y gratuito el cual da a conocer las debilidades de seguridad en un sistema y también asiste en las etapas de penetración con el fin de protegerlo. Permite utilizar otras herramientas como Nessus y Nmap

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.

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

OpenVas: Estructura de trabajo que ofrece escaneo, búsqueda de vulnerabilidades en una red y posibles soluciones. Ofrece dos servicios uno de Servidor que realiza las pruebas de vulnerabilidad en la red y el Cliente que filtra y clasifica los resultados encontrados para entrega de informes.

1.3.2 Servicios en línea:

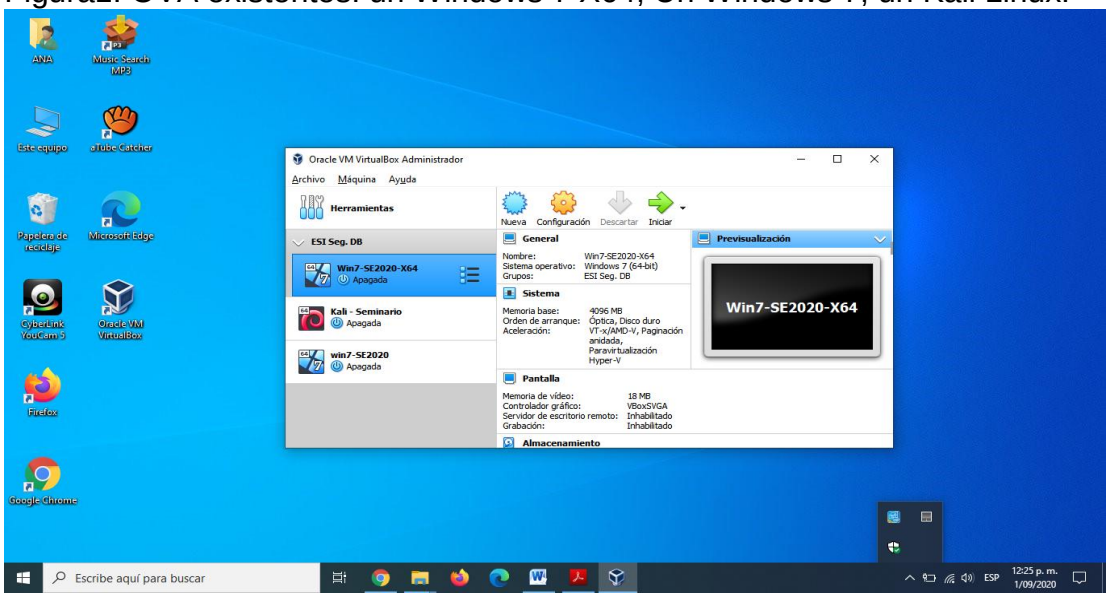
ExploitDB: Código que hace de llave para aprovecha las vulnerabilidades bien sea para tomar el control, tener privilegios de administrador o atacar un sistema. Existen dos tipos: los conocidos (De los que ya estamos al tanto y se sabe cómo tomar las medidas necesarias) y los desconocidos o 0-day (De los cuales no se sabe nada hasta el momento del ataque)

CVE: Diccionario de vulnerabilidades y exposiciones comunes identificadas de conocimiento público con un código único (CVE-ID), seguido por el año y un número de 4 o más dígitos, esto permite diferenciar una de la otra y así mantenerse actualizada

1.4 DESARROLLO BANCO DE TRABAJO

1.4.1 Paso A: Descarga e instalación de la herramienta virtualizadora VirtualBox versión 6.1.12-139181 https://www.virtualbox.org/wiki/Downloads

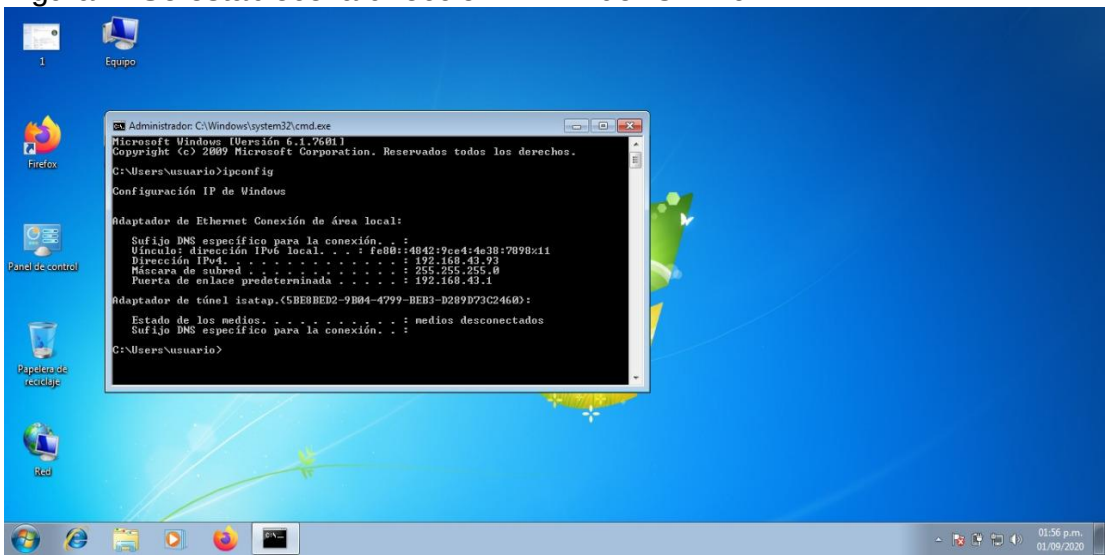
Figura1. OVA existentes: un Windows 7 X64, Un Windows 7, un Kali Linux.



Fuente: Autor

1.4.2 Paso B: Establecer comunicación entre la máquina Kali Linux y las de Windows por separado ya que no se pueden prender al mismo tiempo.

Figura 2. Se establece la dirección IP Windows 7 X64

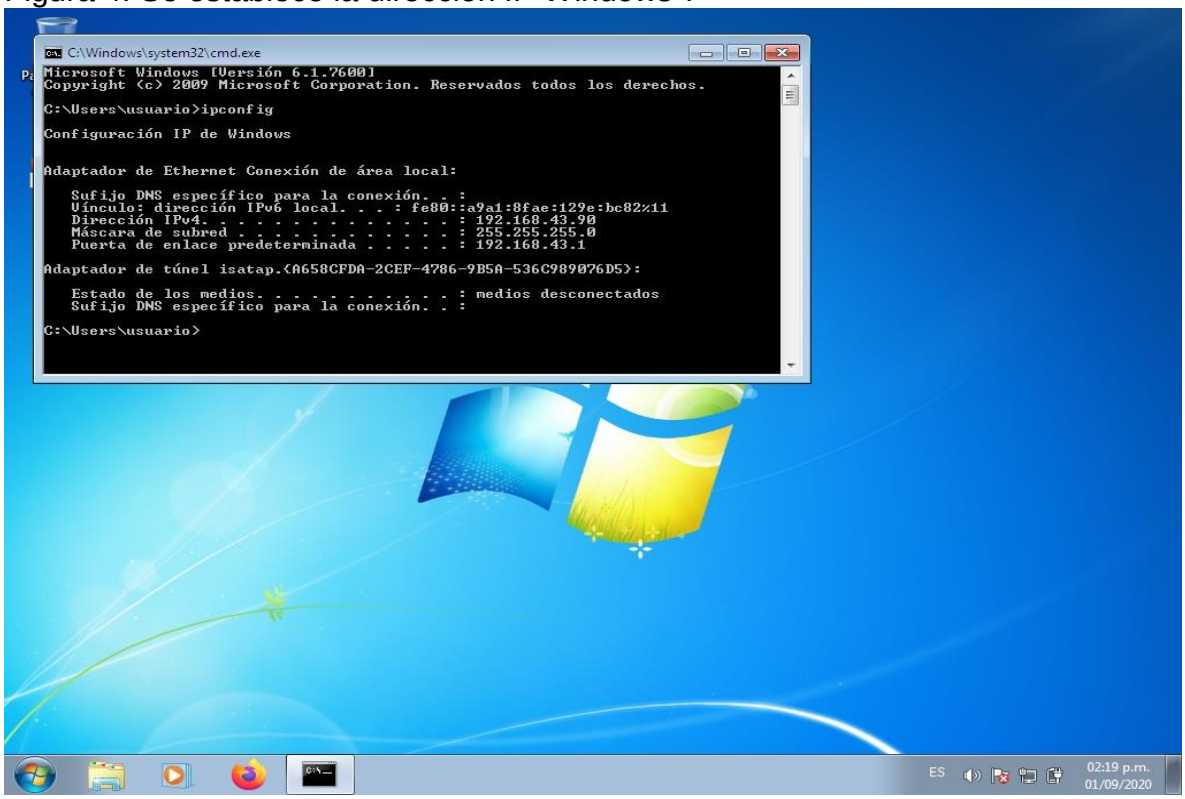


Fuente: Autor

Figura 3: Se realiza ping desde la máquina Kali Linux a Windows 7 X64

Fuente: Autor

Figura 4. Se establece la dirección IP Windows 7



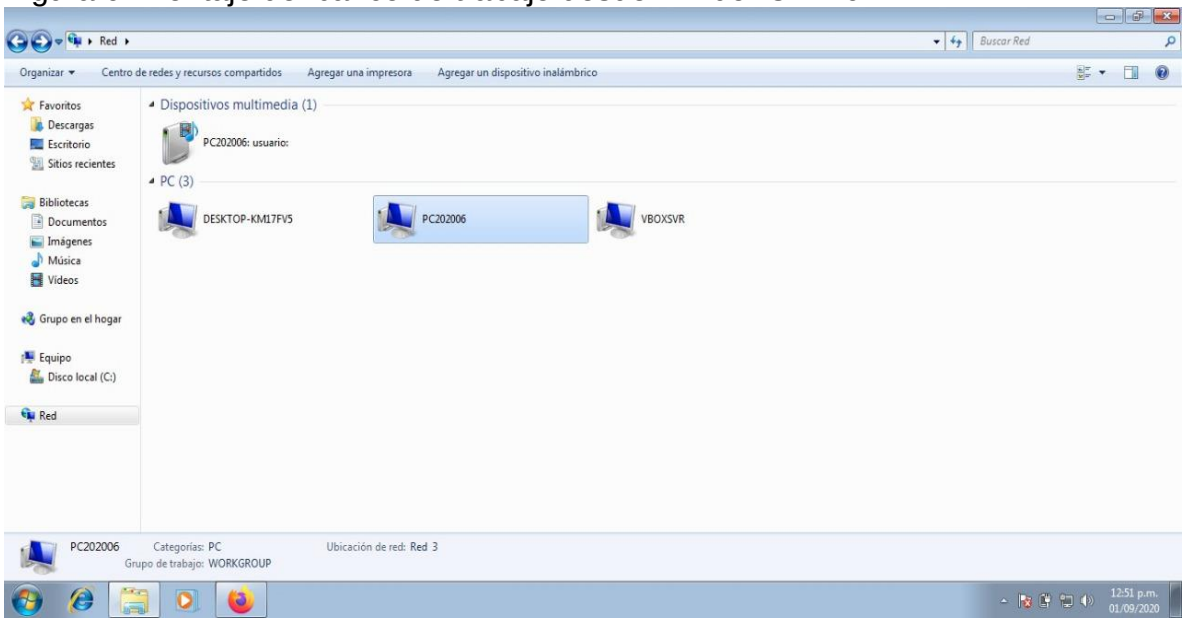
Fuente: Autor

Figura 5: Se realiza ping desde la máquina Kali Linux a Windows 7

Fuente: Autor

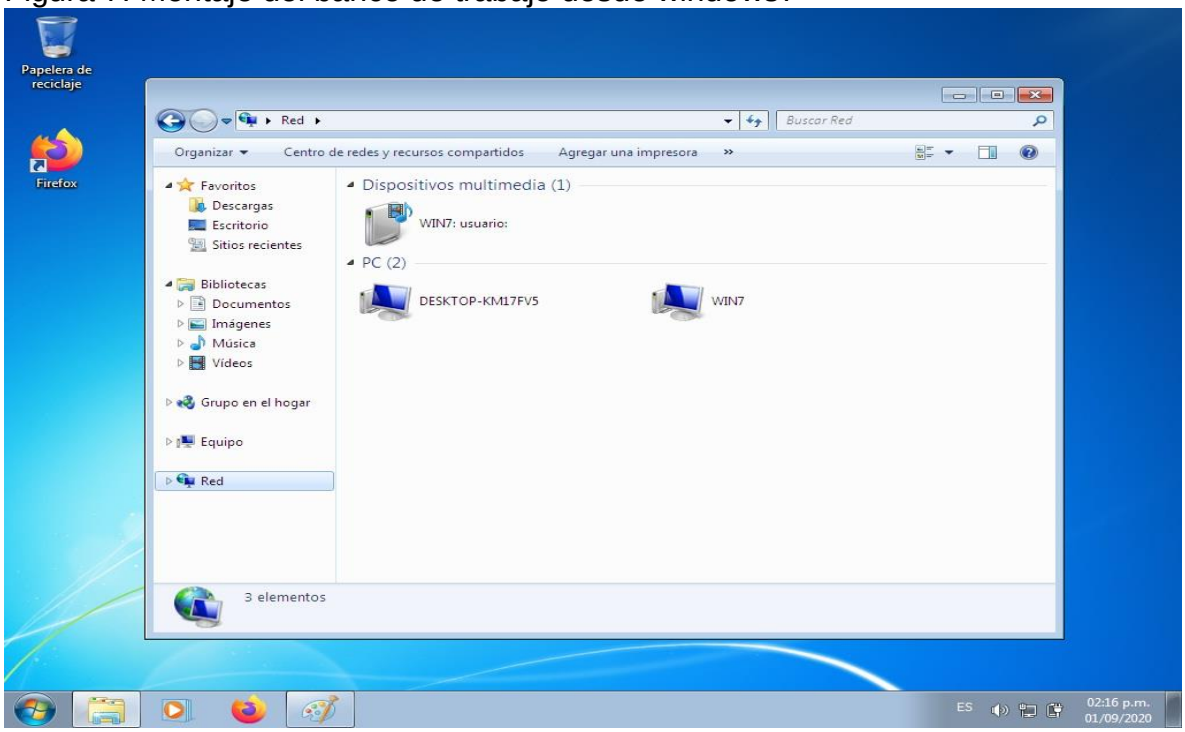
1.4.3 Paso C: Evidenciar el montaje del banco de trabajo y explicar cómo se encuentra desplegado. En cada una de las tres máquinas virtuales se selecciona la conexión adaptador puente y desde mi equipo se puede visualizar que tengo acceso a las máquinas virtuales.

Figura 6. Montaje del banco de trabajo desde Windows 7 X64



Fuente: Autor

Figura 7. Montaje del banco de trabajo desde windows7



Fuente: Autor

2. ETAPA ACTUACIÓN ÉTICA Y LEGAL

2.1 ANÁLISIS DESDE EL PUNTO DE VISTA LEGAL Y NO ÉTICO DEL ESCENARIO 2 Y DEL ACUERDO

2.1.1 Anexo 2 - Escenario 2: La empresa WhiteHouse Security reconocida mundialmente por apoyar procesos de Ciberseguridad a grandes gobiernos presenta los siguientes procesos ilegales y no éticos:

Contrato diseñado por un abogado que fue despedido por darse cuenta de procesos ilícitos
Cuando lo debería redactar un abogado que estuviera vinculado actualmente a la empresa, para mí es un actuar sospechoso

La alta gerencia no revisa ningún contrato sobre el personal
Siendo ésta una de las principales funciones de la gerencia y así no ser implicado en investigaciones

2.1.2 Anexo 3 – Acuerdo: Acuerdo de confidencialidad

CLÁUSULAS donde se evidencia proceso ilegal o no ético

Primera: Los procesos ilegales no se podrán divulgar
En este caso ya estaría en contra del código de ética y la dignidad de las profesiones ya que me están solicitando no reportar de encontrar algo ilegal

Segunda: Se considera como información confidencial datos secretos como chuzadas, interceptación de información o acceso abusivos a sistemas de información
Estos ítems no entrarían en la definición de datos confidenciales ya que se consideran ilegales ante la ley

Cuarta:
No denunciar actividades sospechosas como espionaje donde se apropie información de terceros
Como ingeniera de sistemas y futura especialista estaría actuando en contra de mi código de ética y buen nombre al realizar estas acciones

No se podrá publicar ni denunciar información ilegal que resulten de reuniones
Al ser la información ilegal también estaría actuando ilícitamente y violando las leyes que ejercen en el país

Ser responsable por el mal uso de la información confidencial que le dan los representantes
Hay que revisar muy bien lo que se firma ya que como profesionales deberíamos responder por la información que almacenan nuestros sistemas y saber la finalidad de su uso dentro de la misma empresa

No revelar ni divulgar información ilegal sin el consentimiento de la empresa
Toda información ilegal encontrada debe ser reportada de inmediato ante los entes ya que de lo contrario actuaría en contra de la ley y entraría en el proceso de investigación

Octava: Responder ante las autoridades en caso de haber allanamiento por la información ilegal encontrada, contratar un abogado privado y dejar exenta a la empresa
Encierra el buen o mal actuar profesional de mi parte pero mediante esta cláusula se libran de sus actos y toda la culpa recaería en el contratado, lo ideal sería que la empresa me respaldará en dado caso ya que me encuentro trabajando para esta.

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

Según la ley 1273 el acuerdo vulnera los siguientes artículos:

Artículo 269A: El abuso al acceder a información sea protegida o no **al no poder publicar ni denunciar información ilegal que resulten de reuniones**

Artículo 269B: Impedir el normal funcionamiento de un sistema o red **al no divulgar los procesos ilegales que se realizan en la empresa**

Artículo 269C: Cuando sin orden judicial se acceda a datos de un sistema **al considerar como información confidencial datos secretos como chuzadas, interceptación de información o acceso abusivos a sistemas de información**

Artículo 269D: Destruir, eliminar o alterar datos de un sistema informático **al ser responsable por el mal uso de la información confidencial que le dan los representantes**

Artículo 269F: Manipular de alguna manera datos personales alojados en bases de datos y demás para beneficio propio o de un tercero **al no denunciar actividades sospechosas como espionaje donde se apropie información de terceros y de ser responsable por el mal uso de la información confidencial que le dan los representantes**

Artículo 269H: Se ampliarán las penas si realiza: Sobre sistemas estatales u oficiales, sector financiero, nacionales o extranjeros, si es servidor Público, si se presenta abuso de confianza, si se da información para perjudicar a otro, para beneficio propio o de un tercero, con intención terrorista, manipulando una tercera persona y si el que incurrir en los delitos es el responsable de administrar la información se le inhabilitará de sus funciones **al no revelar ni divulgar información ilegal sin el consentimiento de la empresa y al tener que responder ante las autoridades en caso de haber allanamiento por la información ilegal encontrada y dejar exenta a la empresa que serían los más responsables**

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

Como estudiante de la especialización de seguridad informática, esta propuesta de trabajo se hace muy atractiva por el sueldo de $15.000.000 M/CTE mensuales y que el contrato es de por vida ya que son dos aspectos que hoy en día las empresas no ofrecen pues los contratos son en su mayoría por prestación de servicios, por corto tiempo y el sueldo es muy mal pago; además sería mi primer trabajo en ésta rama y en el primero que aplicaría mis conocimientos sobre seguridad informática, la verdad estaría muy emocionada de aspirar a este cargo; pero revisando las cláusulas del contrato una por una detenidamente se puede evidenciar hasta donde pueden llegar **las acciones que se manifiestan en el acuerdo ya que en su mayoría estas acciones no son legales y por ética no podría realizar todo lo que se plasma en el contrato siendo las siguientes las que irían en contra de mi ética profesional: no poder publicar ni denunciar información ilegal que resulten de reuniones, no divulgar los procesos ilegales que se realizan en la empresa, considerar como información confidencial datos secretos como chuzadas, interceptación de información o acceso abusivos a sistemas de información, responder por el mal uso de la información confidencial que le dan los representantes, no denunciar actividades sospechosas como espionaje donde se apropie información de terceros, no revelar ni divulgar información ilegal sin el consentimiento de la empresa y al tener que responder ante las autoridades en caso de haber allanamiento por la información ilegal encontrada, dejar exenta a la empresa que serían los más responsables y de quien se esperaría el total apoyo así como uno de profesional responde por los resultados de los trabajos realizados.**

Teniendo en cuenta lo anterior no aplicaría a este trabajo ya que dispongo de valores éticos fundados de casa que me definen como una persona que sabe que está bien y que está mal en el actuar frente a ciertas situaciones que se presentan en la vida diaria y que al igual aplicarían a esta situación. Leyendo el código de ética profesional que Copnia en sus tres capítulos (Disposiciones especiales- Los deberes, obligaciones y prohibiciones - Inhabilidades e incompatibilidades) tiene dispuesto para Ingeniería de sistemas y a fines **se establecen las conductas profesionales que se exigen, se prohíben o simplemente se inhabilitan, ante la ley se da a conocer si el actuar del profesional es el correcto o no y se puede establecer que de llegar a violar este código podría llegar a la suspensión o cancelación de la matricula profesional y en el caso de una falta simple conlleva a una amonestación escrita**. Este código de ética siempre velará por el buen nombre de nuestra profesión

Concluyendo así que el contrato que ofrece la empresa WhiteHouse Security conllevaría a **obligaciones que van en contra del reglamento ético y legal de**

mi profesión en varios aspectos por ejemplo: la utilización indebida de información, el ocultamiento de procesos ilegales, el celebrar contratos que vayan en contra de las leyes vigentes y cualquier otra violación que establezca el código de ética y la ley 842 de 2003.

2.4 ANÁLISIS DESDE MI PUNTO DE VISTA Y LOS ASPECTOS LEGALES Y ÉTICOS DE LA NOTICIA DEL CASO “OPERACIÓN ANDROMEDA BUGGLY”

A continuación daré a conocer las implicaciones legales y éticas que pudo haber generado este caso:

Todo empezó con la idea de construir una comunidad de seguridad informática donde a los interesados en ser parte tenían que realizar retos con el ánimo según ellos de compartir sus conocimientos aunque no fueran muy avanzados, su deseo era hacer parte de una comunidad grande y de reconocimiento, este lugar funcionaba con todo lo de ley y lo que se exige en el marco legal para su funcionamiento. Pero en verdad lo que se hacía era **reclutar a los hackers más técnicos sin saber que se trataba de una operación militar donde se realizaba espionaje y violación de datos personales mediante software de interceptación de uso exclusivo del gobierno o conseguido en el mercado negro**

En febrero de 2014 se dieron a conocer las primeras noticias sobre este caso donde se daba a conocer que en el barrio galerías de Bogotá **funcionaba un restaurante como fachada para realizar interceptaciones y espionajes ilegales por medio de sistemas operativos, celulares y computadores a integrantes del dialogo de paz en la Habana obviamente sin orden judicial, estas acciones eran realizadas por delincuentes informáticos mal llamados “hackers” los cuales eran supuestamente pagos con dineros del ejercito pero sin saber a ciencia cierta para quien realizaban estos actos delictivos.**

En enero de 2016 fue allanado este lugar donde el gobierno de ese entonces estableció que **estos actos se habían realizado para conveniencia de terceros y no por órdenes del sistema de inteligencia Colombiano**, el gobierno para defenderse se basa a la ley 1621 de 2013 donde asegura crear un plan Nacional de inteligencia para identificar supuestas amenazas contra el estado donde indican que se deben **desarrollar “productos de inteligencia que permitan al Gobierno identificar las situaciones, los problemas y los peligros que puedan afectar el proceso de negociación de la paz o sus implicaciones frente a la seguridad nacional**” el cual fue a probado por el consejo de seguridad Nacional

Este caso provoco fueran relevados de sus cargos 30 militares, la captura de Andrés Sepúlveda y **pone en evidencia las falencias en el proceso de inteligencia, fallas operativas e inconsistencias de los sistemas utilizados.**

3. ETAPA EJECUCIÓN PRUEBAS DE INTRUSIÓN

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

Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Red team. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

3.1.1 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.

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

3.1.3 Mestaspolit: Proyecto de código abierto y gratuito el cual da a conocer las debilidades de seguridad en un sistema y también asiste en las etapas de penetración con el fin de protegerlo. Permite utilizar otras herramientas como Nessus y Nmap

Para iniciar el proceso desactivare el firewall, update y antivirus en ambas máquinas identificadas así: Windows 7 y Windows 7x64

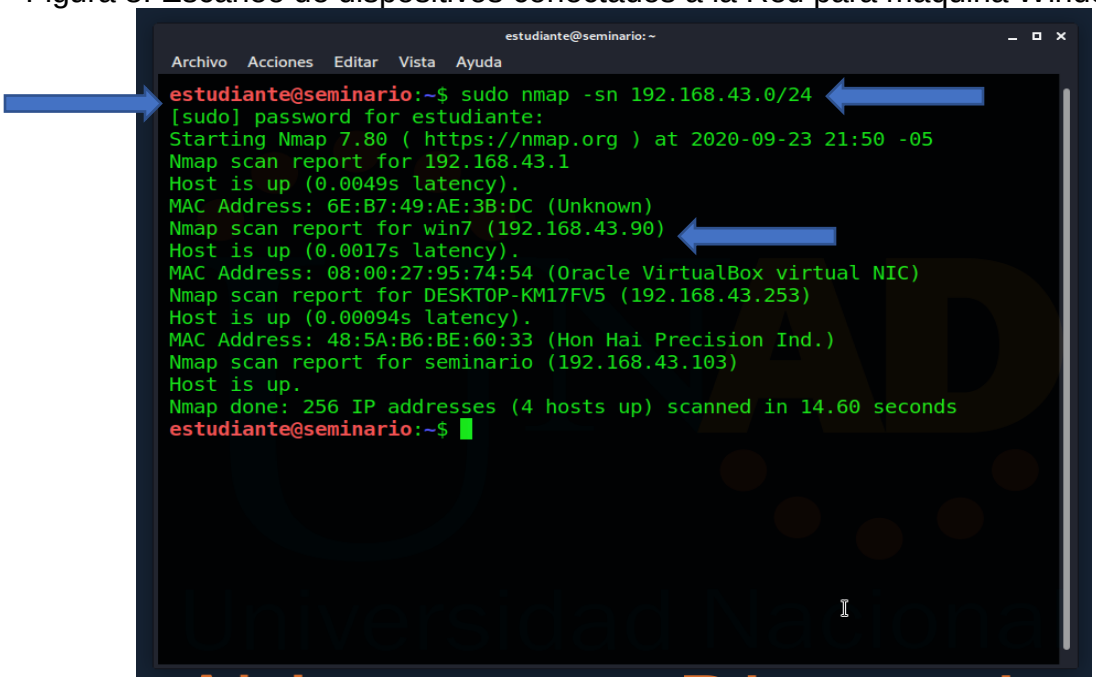
3.2 INFORME CON ANÁLISIS DEL CASO DE RED TEAM, QUE PERMITIÓ DAR SOLUCIÓN AL FALLO IDENTIFICADO

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca constantemente las dos máquinas con Windows 7 X86 y Windows 7 X64.
-Los equipos sospechosos cuentan con Windows 7 X86 y X64
-Los equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque no es compatible con otros sistemas operativos.
-Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y archivos dentro de la red.
-Al momento de la fuga de información (10 de junio de 2020) los S.O. no se encontraban actualizados
-Su última actualización fue el 05 de febrero de 2017
-Fallo de seguridad con identificador CVE-2017-0144
-Los equipos de cómputo no tienen instalada la actualización MS17-010.

3.2.1 Recopilación de información

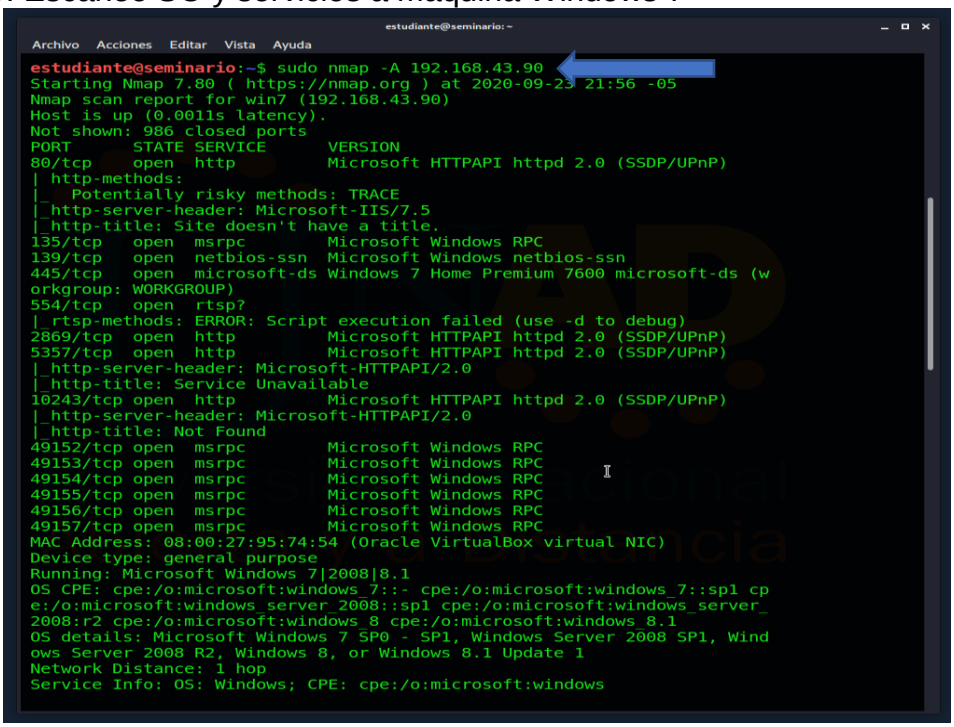
Conocer y disponer de la mayor cantidad de información del sistema que nos permita llevar a cabo nuestro objetivo, en esta etapa utilizaré la herramienta Nmap y así verificar la seguridad por medio de los puertos y los servicios.

Figura 8. Escaneo de dispositivos conectados a la Red para máquina Windows 7



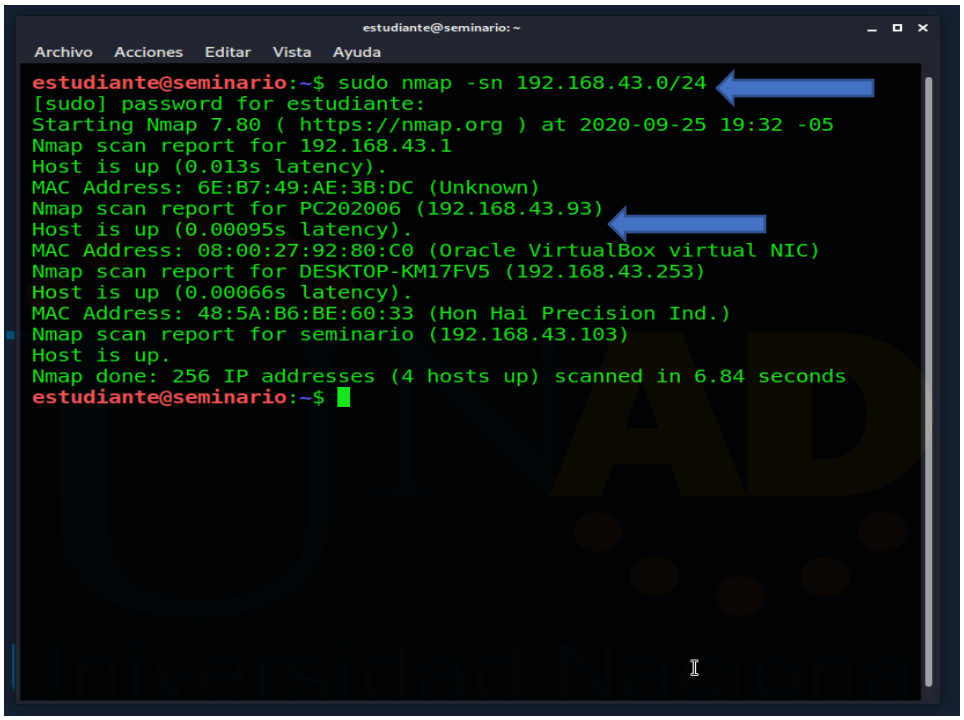
Fuente: Autor

Figura 9. Escaneo SO y servicios a máquina Windows 7



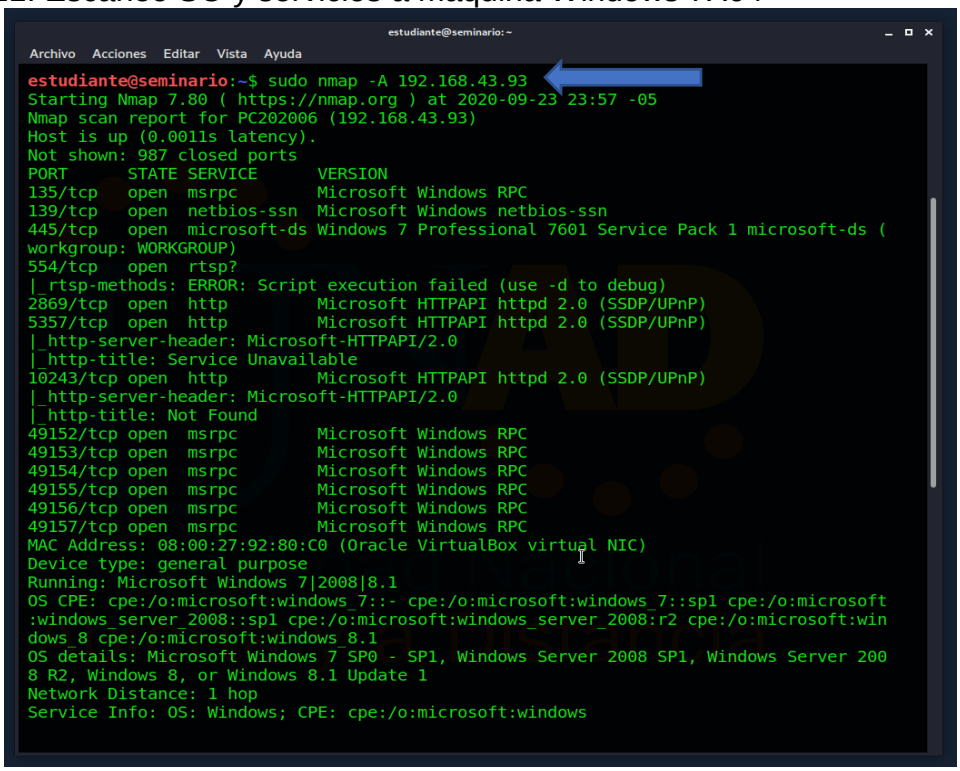
Fuente: Autor

Figura 10. Escaneo de dispositivos conectados a la Red para máquina Windows 7X64



Fuente: Autor

Figura 11. Escaneo SO y servicios a máquina Windows 7X64



Fuente: Autor

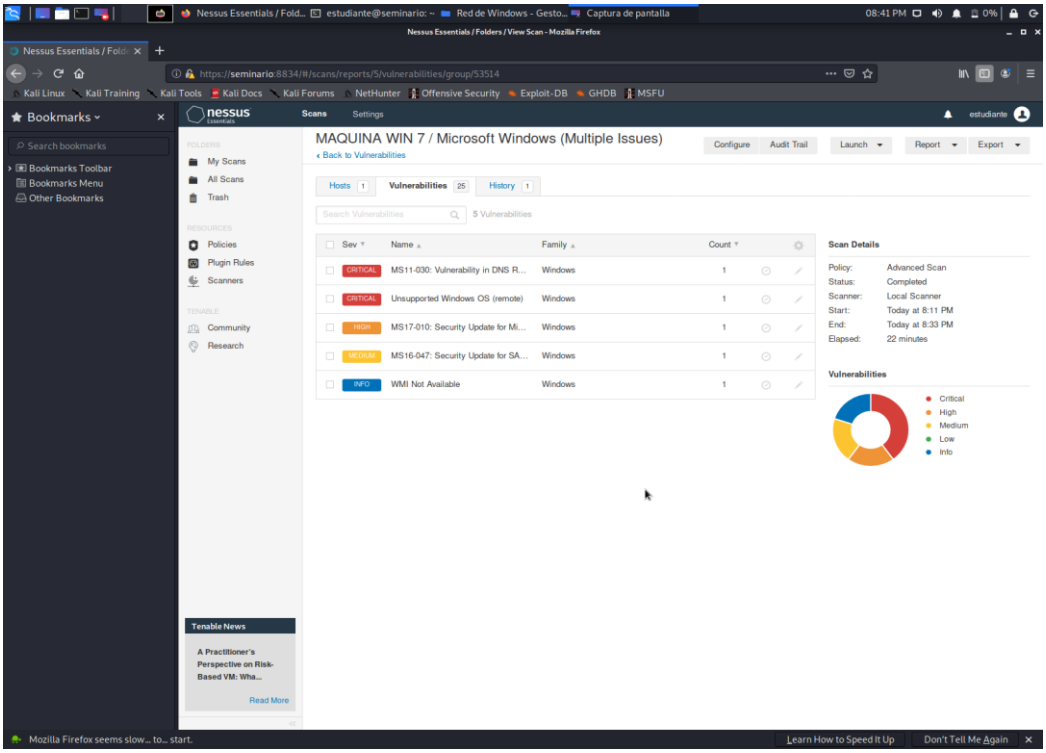
3.3 INFORME DE HERRAMIENTAS UTILIZADAS PARA DAR IDENTIFICAR FALLOS EN EL ESCENARIO PROPUESTO

¿Qué herramienta utilizó para poder identificar los fallos a nivel de sistema operativo “máquinas Windows 7”?

3.3.1 Búsqueda de vulnerabilidades

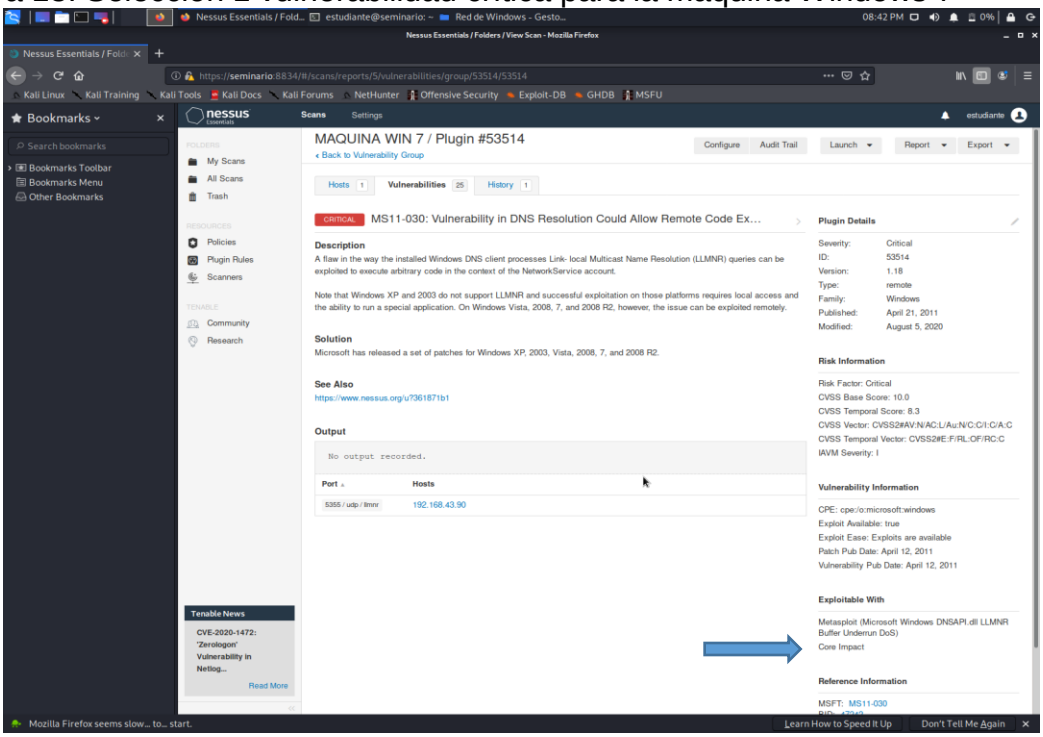
Se analiza la información recolectada en búsqueda de amenazas, utilizaré la herramienta Nessus

Figura 12. Vista de las vulnerabilidades críticas escaneo Nessus para la máquina Windows 7



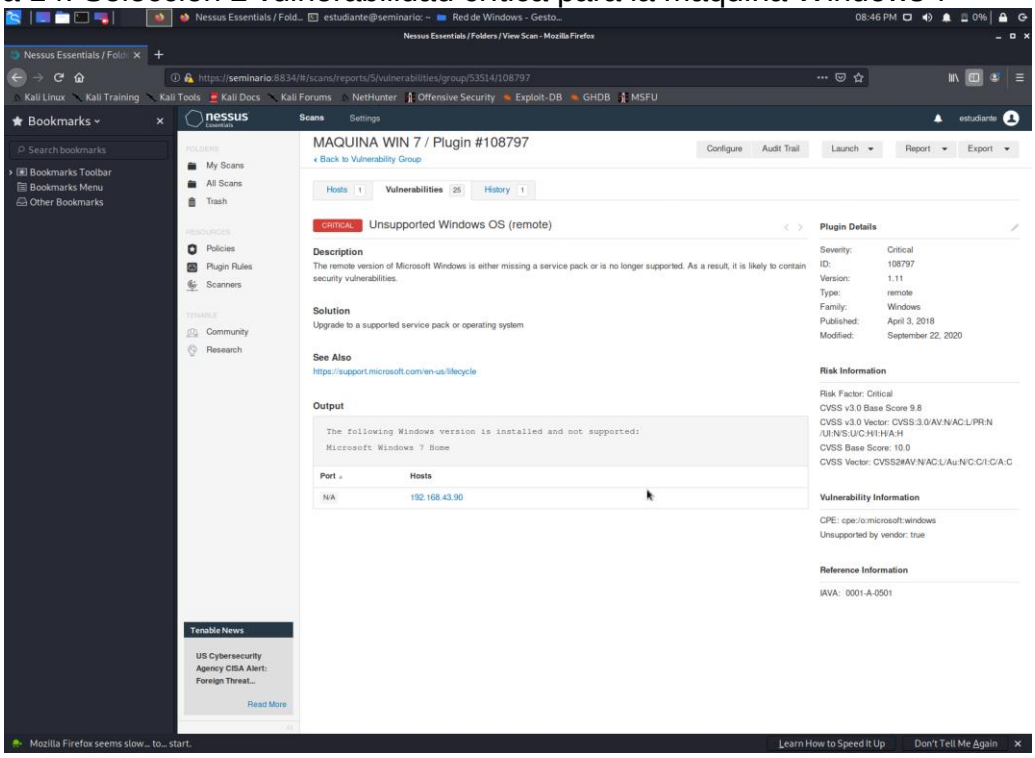
Fuente: Autor

Figura 13. Selección 1 vulnerabilidad crítica para la máquina Windows 7



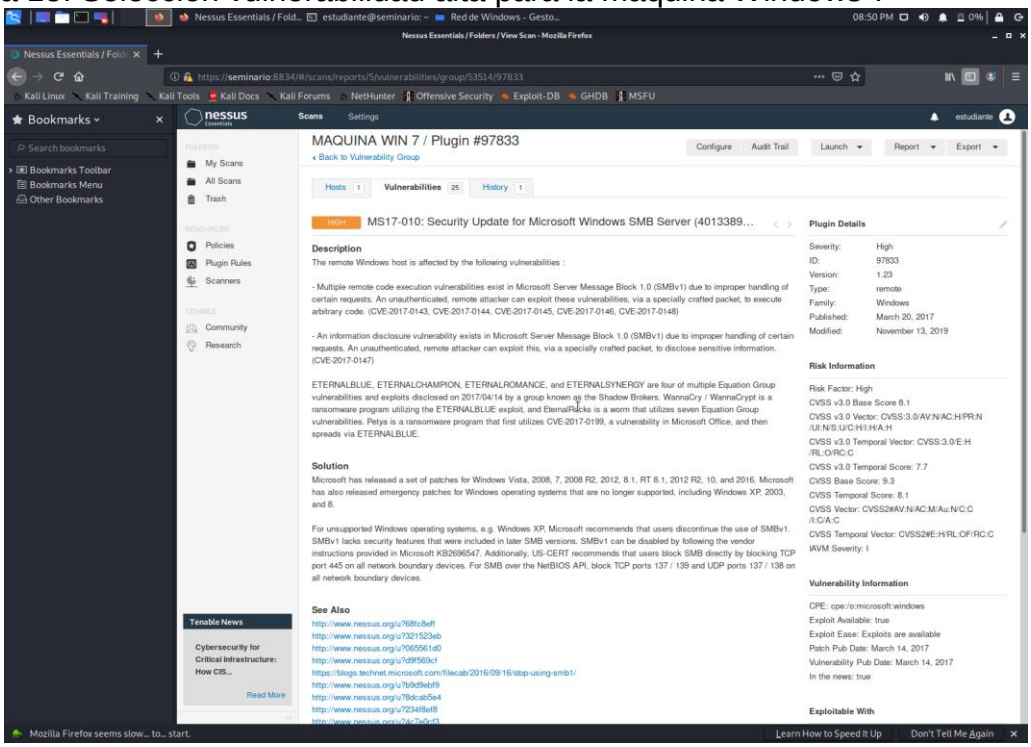
Fuente: Autor

Figura 14. Selección 2 vulnerabilidad crítica para la máquina Windows 7



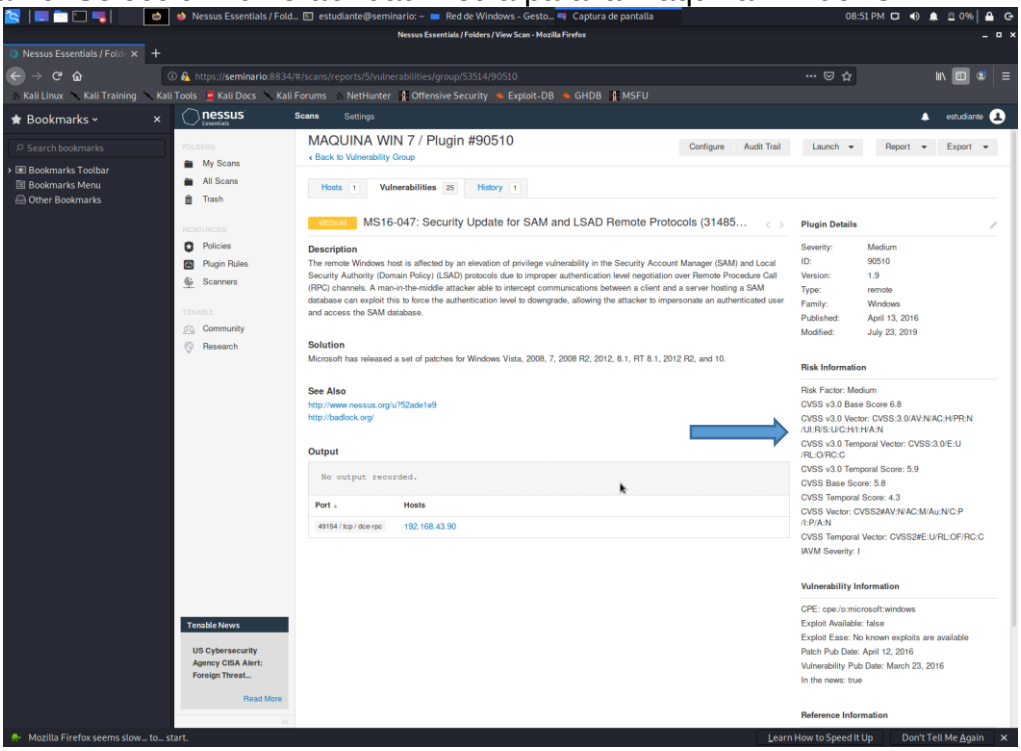
Fuente: Autor

Figura 15. Selección vulnerabilidad alta para la máquina Windows 7



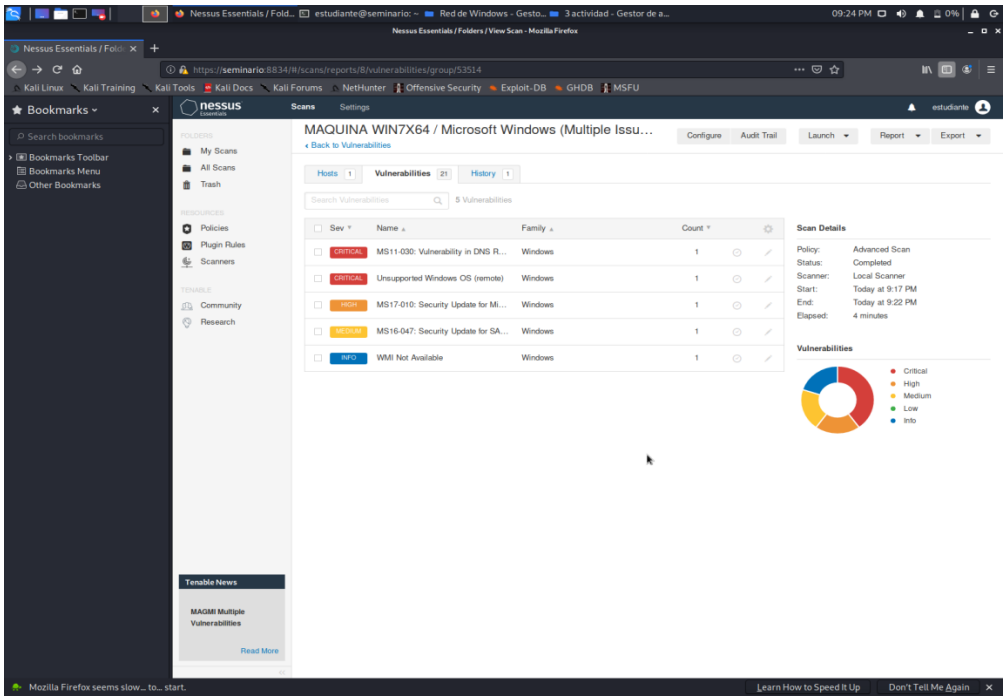
Fuente: Autor

Figura 16. Selección vulnerabilidad media para la máquina Windows 7



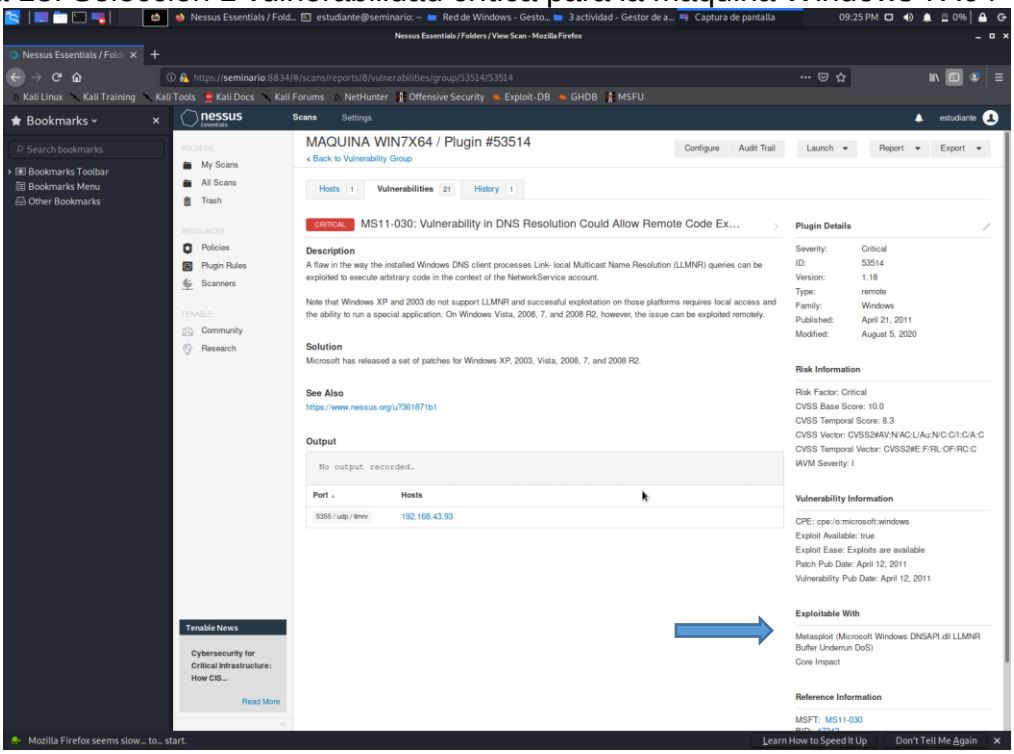
Fuente: Autor

Figura 17. Vista de las vulnerabilidades críticas escaneo Nessus para la máquina Windows 7X64



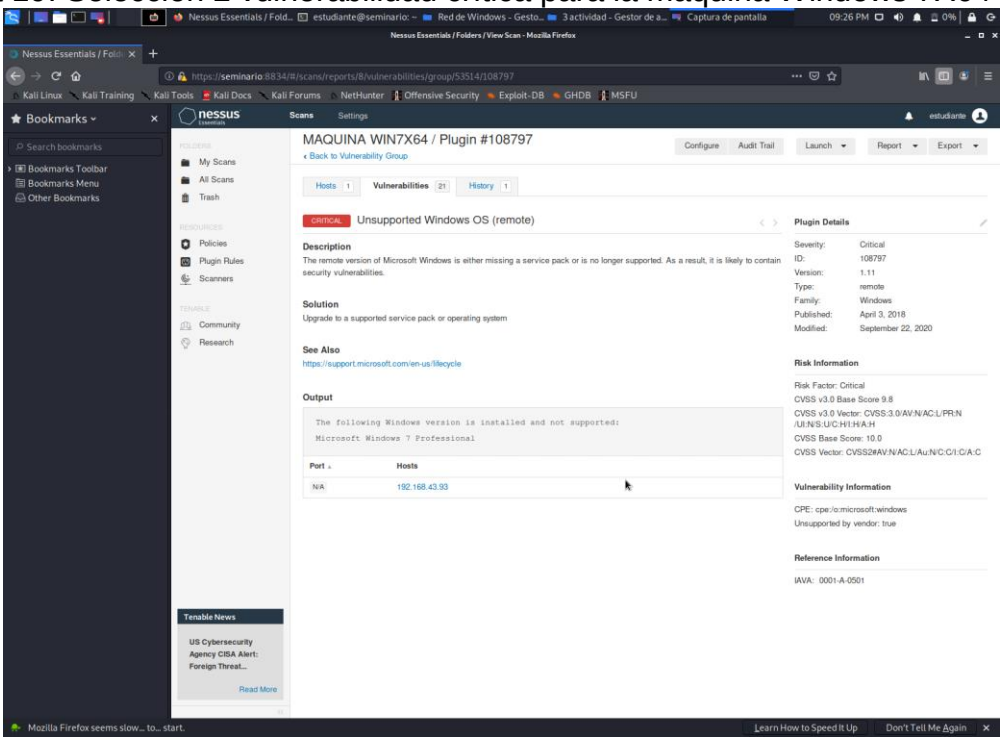
Fuente: Autor

Figura 18. Selección 1 vulnerabilidad crítica para la máquina Windows 7X64



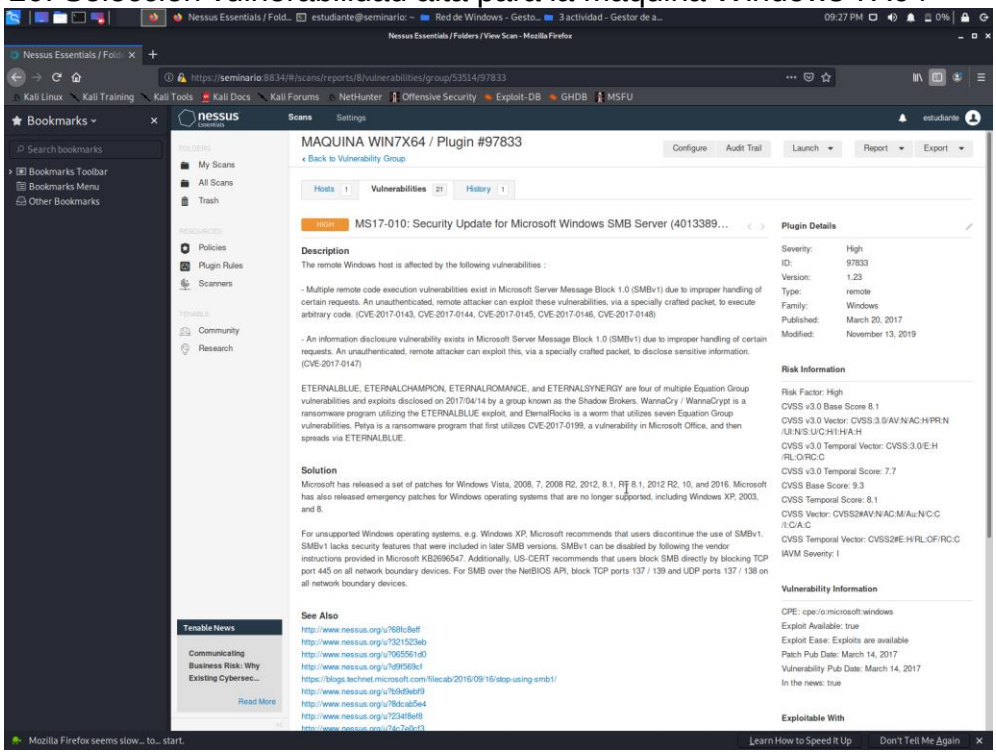
Fuente: Autor

Figura 19. Selección 2 vulnerabilidad crítica para la máquina Windows 7X64



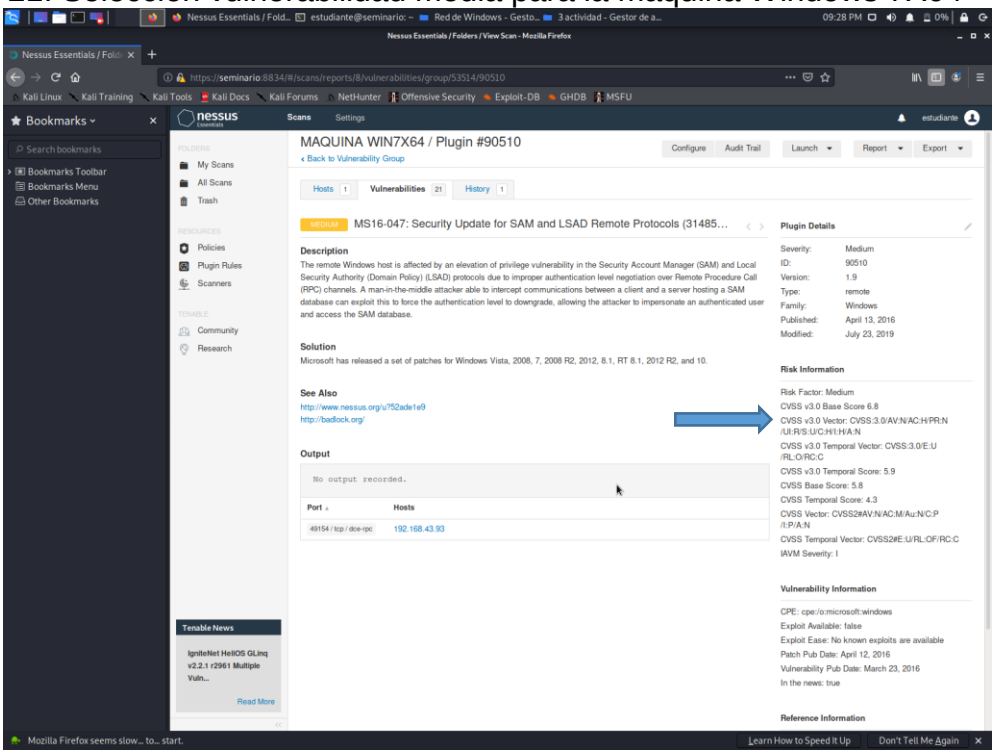
Fuente: Autor

Figura 20. Selección vulnerabilidad alta para la máquina Windows 7X64



Fuente: Autor

Figura 21. Selección vulnerabilidad media para la máquina Windows 7X64



Fuente: Autor

Tabla 1. Fallos de seguridad

Categoría	Descripción	Detalles
Critical MS11-030	Una falla en la forma en que los procesos del cliente DNS de Windows instalados vinculan las consultas de resolución de nombres de multidifusión local se pueden aprovechar para ejecutar código arbitrario en el contexto de la cuenta de servicio de red	ID 53514 Versión 1.18 Type Remote Family Wimdows Published 21/04/11 Modified 5/08/20
Critical UNSUPPORTED WINDOWS OS (REMOTE)	La versión remota de Microsoft Windows no es compatible, posiblemente contenga vulnerabilidades de seguridad	ID 108797 Versión 1.11 Type Remote Family Wimdows Published 3/4/18 Modified 22/9/20
High MS17-010	Existen vulnerabilidades de ejecución remota de código en el bloque de mensajes del servidor de Microsoft 1.0 (MSBv1) debido al mal manejo de ciertas solicitudes. Un atacante puede aprovecharse de estas vulnerabilidades, a través de un paquete especialmente diseñado para ejecutar código ilegal. CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148. También existe una vulnerabilidad de divulgación de información en el mismo bloque de mensajes donde se puede aprovechar de esta a través de un paquete especialmente diseñado para divulgar información confidencial CVE-2017-0148	ID 97833 Versión 1.23 Type Remote Family Wimdows Published 20/3/17 Modified 13/11/19
Medium MS16-047	El host de Windows remoto se ve afectado por una vulnerabilidad de privilegios de elevación en el administrador de cuentas de seguridad (SAM) y la autoridad de seguridad local (política de dominio) (LSAD) se debe a la autenticación incorrecta en los canales de llamada a procedimientos remotos donde se puede interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM, puede explotar esto para forzar la degradación del nivel de autenticación, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la base de datos SAM	ID: 90510 Versión: 1.9 Type: Remote Family: Wimdows Published: 13/4/16 Modified: 23/7/19

Fuente: Autor

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

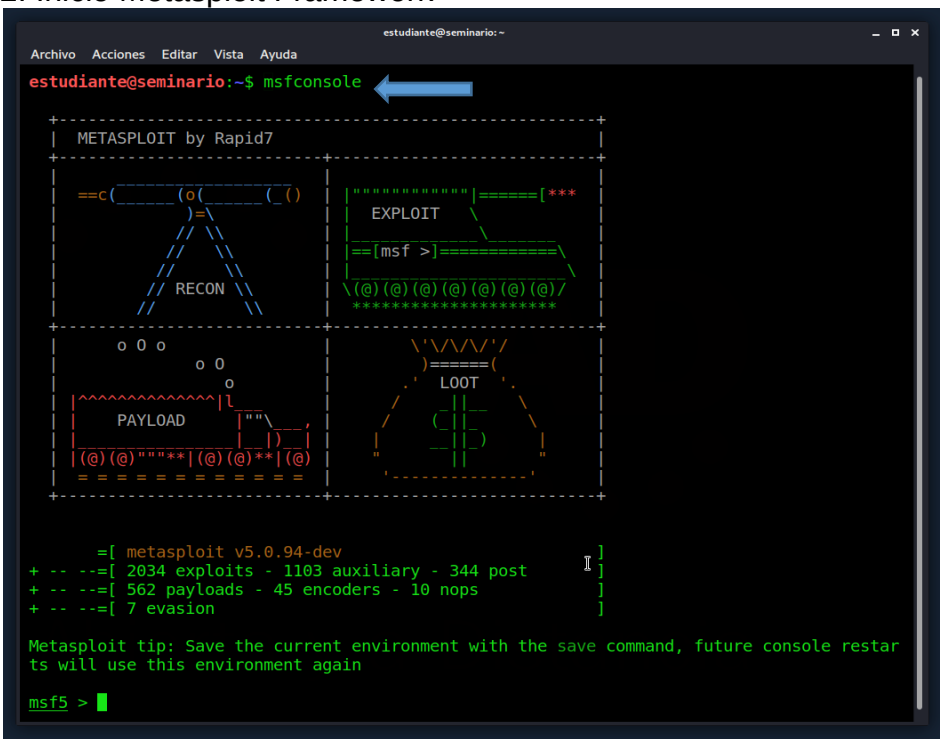
Explique con sus palabras y de manera específica cómo afecta el ataque a cada una de las máquinas (Windows 7 y Windows 7 X64).

Mediante las pruebas de penetración se identifican las debilidades, carencias de programas y vulnerabilidades, también permite simular métodos que un atacante puede utilizar para tener acceso a una organización. En Windows las vulnerabilidades son explotadas por los puertos en este caso el 445 siendo fácil de explotar con un exploit y un payload para conseguir una Shell remota conociendo únicamente su IP. Para el ataque se utiliza Metasploit ya que proporciona una infraestructura para automatizar tareas rutinarias y complejas permitiendo la identificación de fallas dentro de una organización. El modo consola de Metasploit Msfconsole para ejecutar los exploits maneja una base de datos que contiene todos los exploits permitiéndonos explotar cada una de las vulnerabilidades encontradas

3.4.1 Explotación de vulnerabilidades

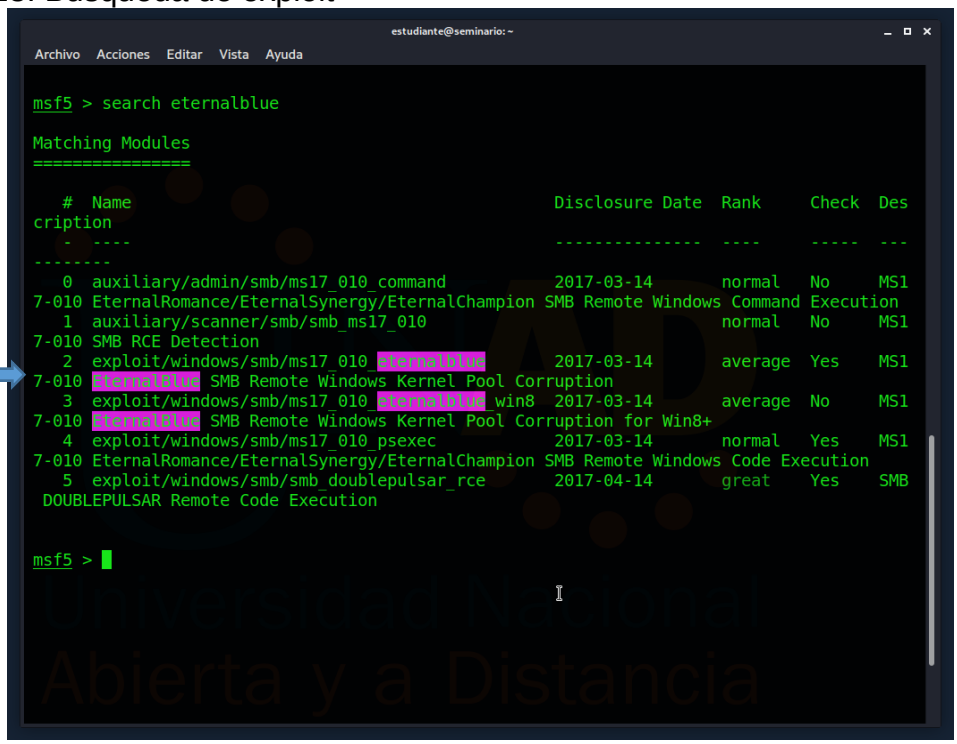
Una vez identificadas las vulnerabilidades se definirá como aprovecharlas y así comprometer el sistema, la herramienta a utilizar es Metasploit se utilizan los siguientes comandos:
msfconsole: Da inicio al Metasploit Framework
search eternalblue: Busca el Exploit (MS17-010 Eternalblue SMB Remote Windows Kernel Pool Corruption)
exploit: Lanzar ataque, me permitirá tomar ventaja de las fallas en el sistema, aplicación y/o servicio
payload es un código o virus que genera un efecto dentro del sistema atacado.
sysinfo: Muestra las características del equipo
getuid: Muestra que el nivel de acceso es de administrador
pwd: Muestra en que parte me encuentro
ps: Muestra los procesos del sistema

Figura 22. Inicio Metasploit Framework



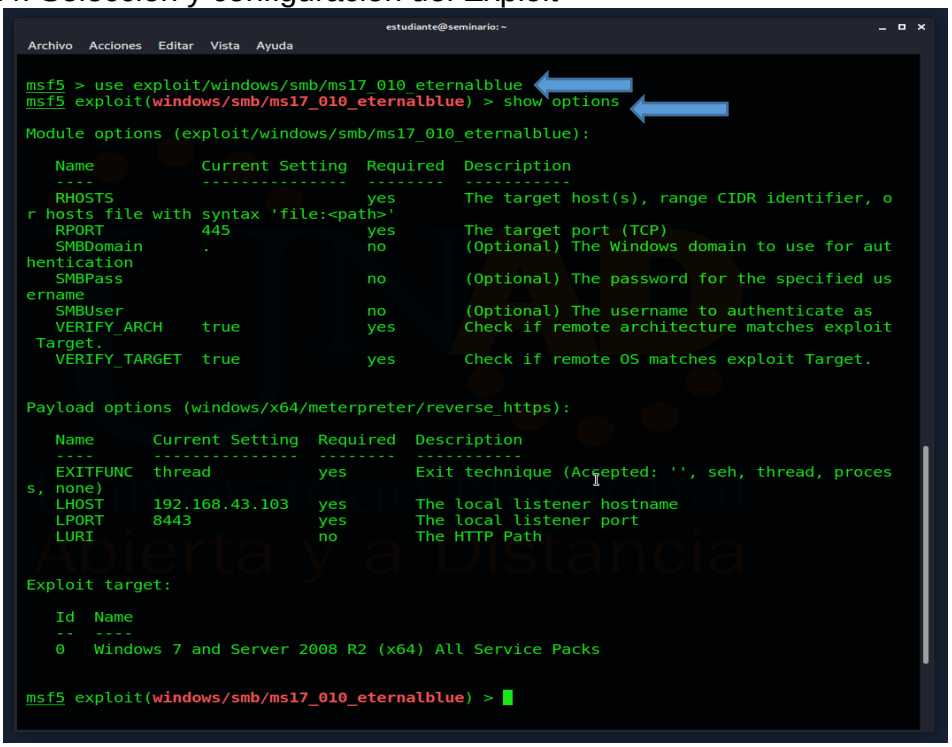
Fuente: Autor

Figura 23. Búsqueda de exploit



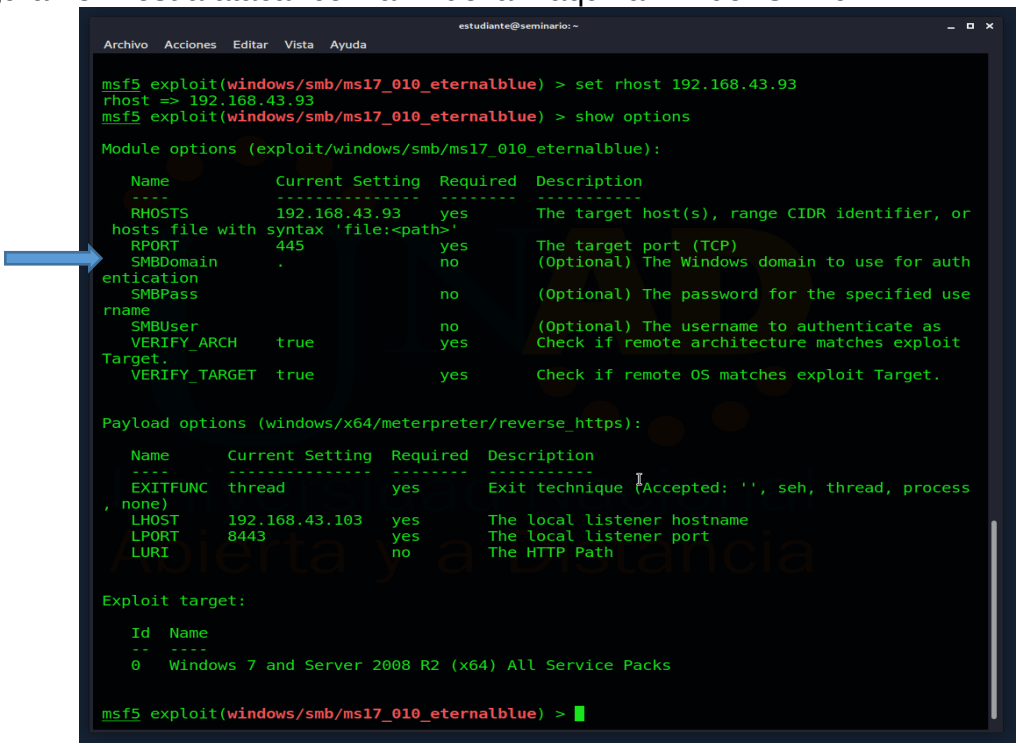
Fuente: Autor

Figura 24. Selección y configuración del Exploit



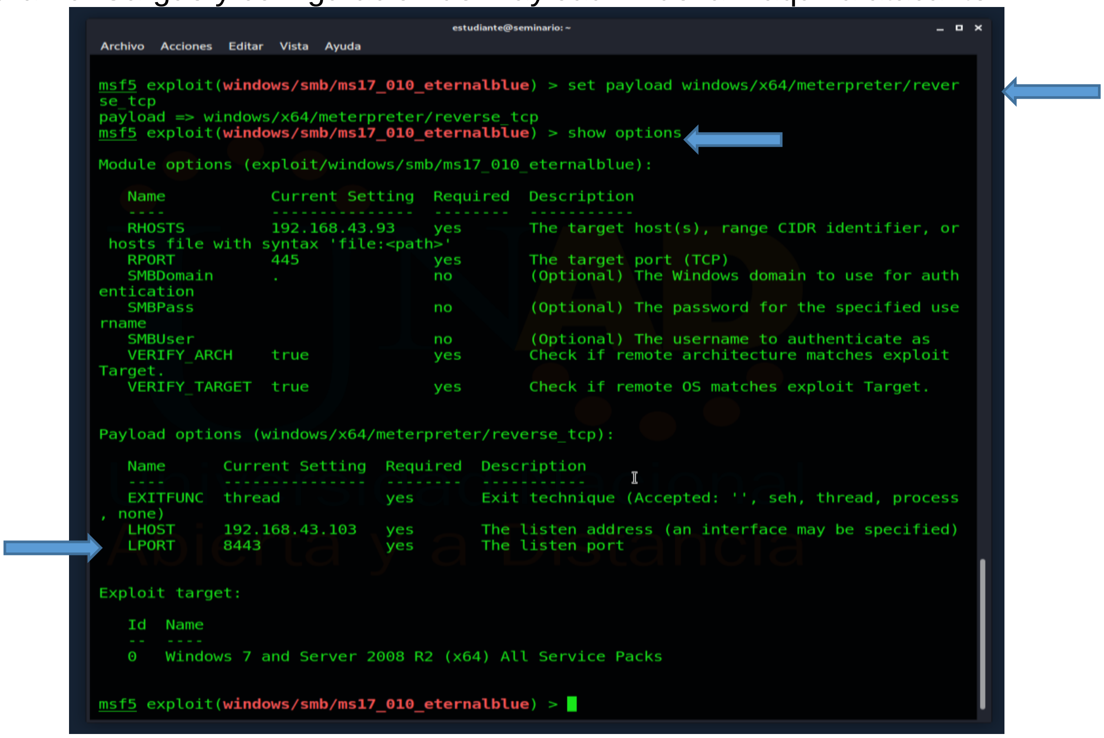
Fuente: Autor

Figura 25. Host a atacar con la IP de la máquina Windows 7X64



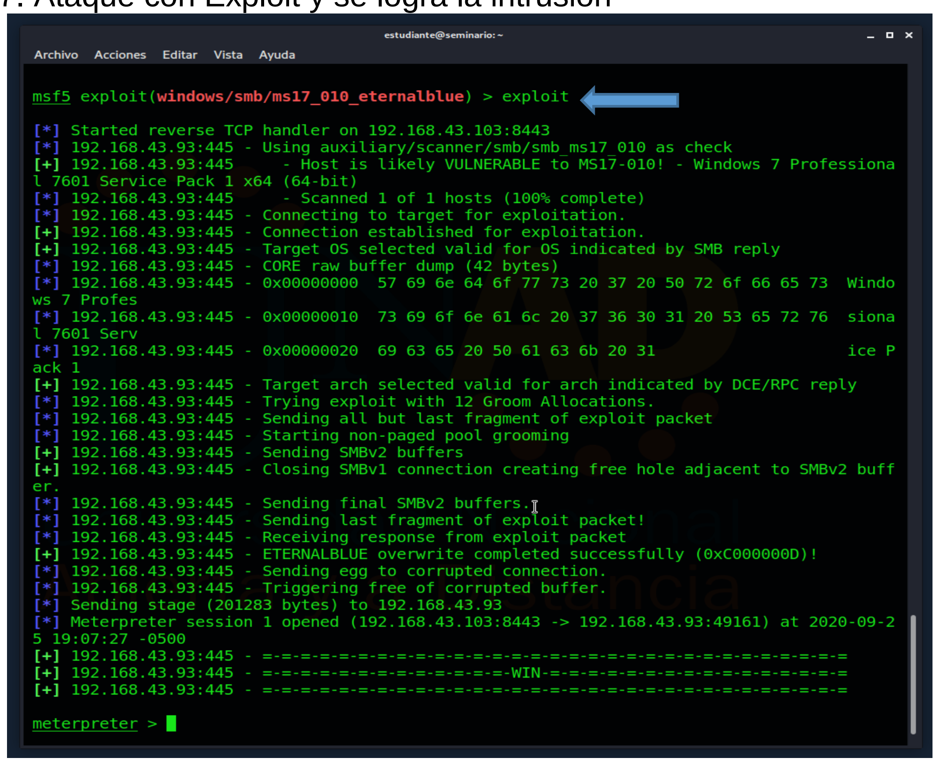
Fuente: Autor

Figura 26. Cargue y configuración del Payload-IP de la máquina atacante



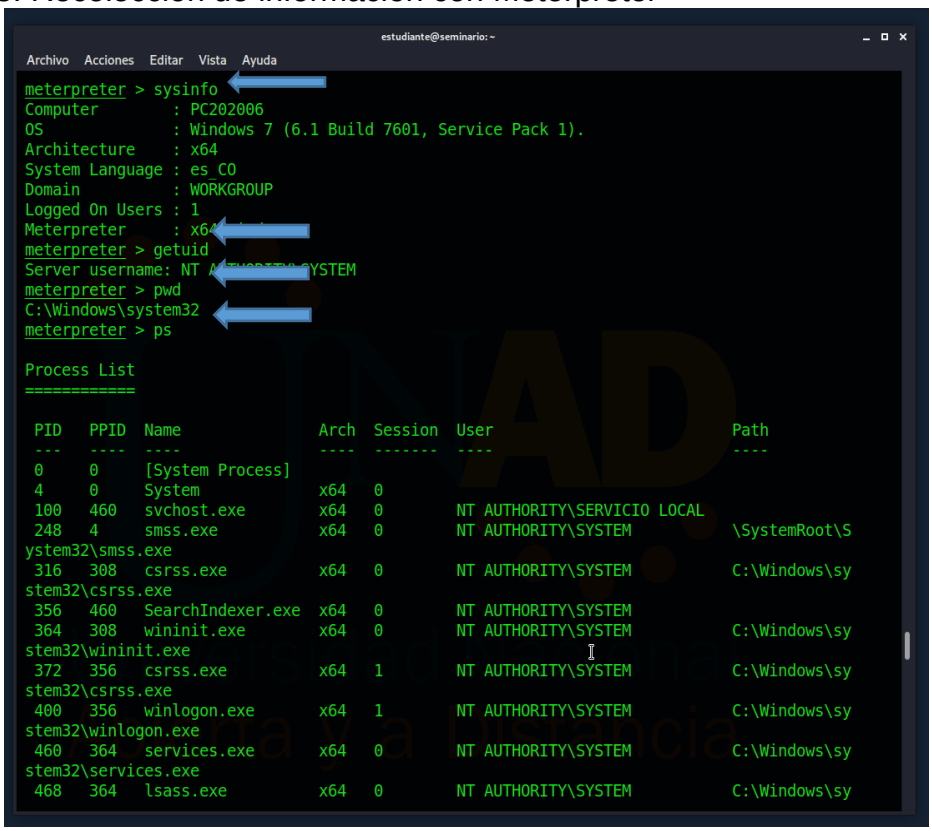
Fuente: Autor

Figura 27. Ataque con Exploit y se logra la intrusión



Fuente: Autor

Figura 28. Recolección de información con Meterpreter

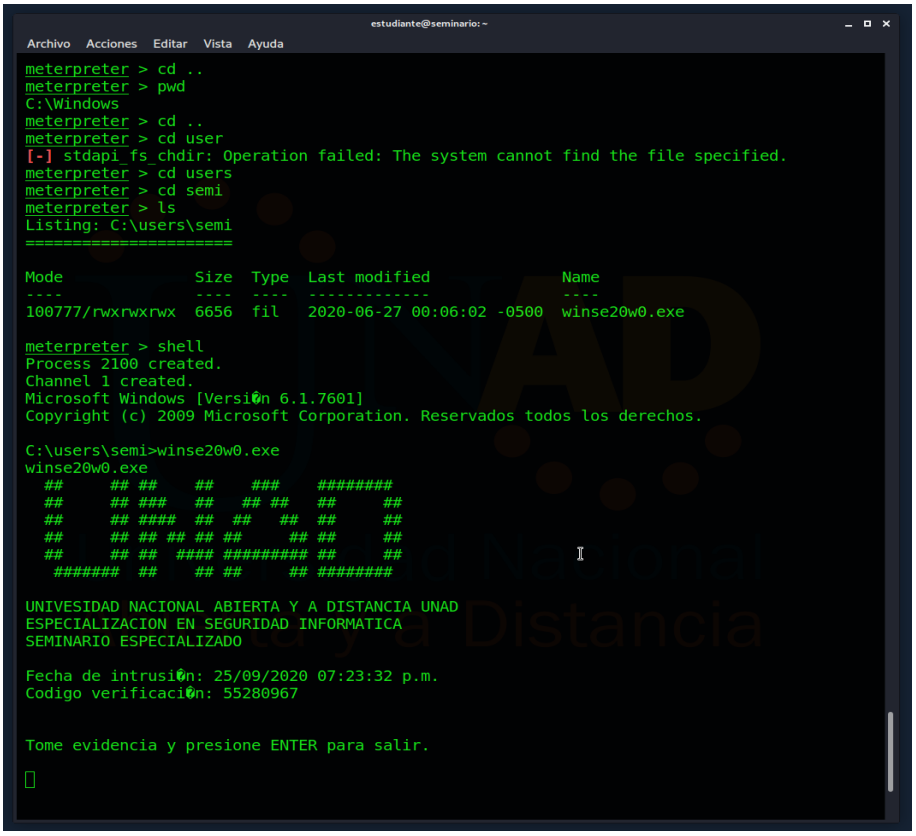


Fuente: Autor

3.5 EVIDENCIA DE LA EXPLOTACIÓN DE LA VULNERABILIDAD QUE IDENTIFICO

Adjunte un printscreen con la evidencia generada por el archivo winse20w0.exe el cual podrá ejecutar y visualizar una vez irrumpa en la máquina víctima.

Figura 29. Printscreen de evidencia



Fuente: Autor

Se realizaron varios ataques a la máquina Win7 (Win7-SE2020-X86), los ataques son tan fuertes con Eternalblue que lo que produce un volcado de memoria por la incompatibilidad en la estructura de X64 a X86 o definitivamente se deniegan dichos ataques.

4. CONTENCIÓN DE ATAQUES INFORMÁTICOS

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

Al encontrarme frente a un ataque en tiempo real tendría en cuenta los siguientes pasos en su orden:

4.1.1 Paso 1 Prevención:

Definir procedimientos preventivos, reunir la mayor cantidad de información, establecer comunicación y sensibilizar al cliente. En este paso abordaría las siguientes medidas:

Copias de seguridad y aislarlas
Mantener actualizado tanto el software como el equipo
Instalación, actualización de antivirus y análisis de equipo constantemente
No abrir correos desconocidos y mucho menos descargar archivos
Tener protegido el sistema por medio de contraseñas seguras
Limitar el acceso a la red
Bloquear las direcciones IP que no se utilizan
Cerrar los servicios no utilizados en los sistemas de destino así se previene el escaneo de puertos

4.1.2 Paso 2 Detección:

Averiguar el tipo de ataque, su alcance mediante monitoreo e incluir a las partes apropiadas en el dado caso que yo no esté facultada para tomar decisiones y crearía una copia de toda la evidencia reunida donde se dará a conocer los procedimientos de recuperación, las personas involucradas y en detalle los datos que fueron recuperados. Los tipos de ataques más comunes son:

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
Phising: Cuando por medio de comunicación electrónica simula ser una empresa y accede a datos personales
Denegación de servicios DoS: Cuando el atacante evita que los usuarios accedan a información y servicios

4.1.3 Paso 3 Recuperación

En este paso se buscan 3 objetivos:
Mitigar las consecuencias del ataque sobre el entorno objetivo por medio de una herramienta de contención que sea la más apropiada limitando así el impacto y consecuencias del ataque
Utilizar medidas 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 borrado de datos etc.
Volver a la etapa normal de funcionamiento teniendo en cuenta los detalles del ataque, ajustar los planes para responder al ataque más rápidamente, implantando medidas como backups y copias de seguridad

4.1.4 Paso 4 Respuesta

Al presentarse este hecho dentro de una organización el paso final a seguir es dar a conocer la información de lo acontecido a los interesados como puede ser: los clientes, trabajadores y a los respectivos entes para denunciarlo, dando a conocer las consecuencias del ataque, las medidas adoptadas después del daño ocasionado y la disposición de nuestra parte para responder dudas que puedan surgir

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

Por Hardenización entiendo que es asegurar un sistema de información reduciendo las vulnerabilidades eliminando servicios, usuarios, funciones u otros que no son necesarios llevando a endurecer la seguridad. Lo que propondría para que este ataque no se repita se describe a continuación:

Autenticación mediante llaves SSH lo que permitirá que se cuente con una secreta y una para compartir con otros usuarios sin ninguna restricción

Cortafuegos el cual inspecciona que servicios exponer en la red teniendo en cuenta que hay servicios públicos que son aquellos a los cuales no tienen ninguna restricción, disponibles para todos como por ejemplo el servidor web, están también los servicios privados a los cuales solo tiene acceso un grupo seleccionado en este caso sería ejemplo el panel de control y por ultimo tenemos los servicios internos donde solo se accede desde el servidor que solo permita conexiones locales

VPN y redes privadas: Se pueden crear conexiones remotas disponibles exclusivamente para ciertos usuarios/servidores.

Auditoria de servicio: 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.

Auditoria de archivos: Se realiza la comparación del sistema actual con uno que se encuentre en los archivos revisando actividades no usuales o no autorizadas o simplemente para revisar si el sistema ha tenido algún cambio y brinda la certeza de no haber sido alterado.

Aislar procesos: Donde cualquier servidor individual se ejecuta en su propio espacio dedicado creando un aislamiento, dependiendo de las características de la aplicación y de las condiciones en que se encuentre la infraestructura limitando así el acceso a intrusos

Protección de Hardware: Para el arranque de la máquina establecer contraseñas complejas, denegar el encendido del sistema a menos que se realice desde el disco duro, deshabilitar la entrada de cualquier dispositivo de almacenamiento externo

Instalación correcta sistema operativo: Se recomienda crear dos particiones la primera para alojar el sistema operativo y la segunda para almacenar en resto de

información creada evitando instalar componentes innecesarios para su correcto funcionamiento

Instalar programas de seguridad: Antivirus, Antispyware y Antispam

Configuración de la política local del sistema: Busca que se cumpla con los requisitos de complejidad de contraseñas, deshabilitación de las cuentas administrador e invitado y limitar los privilegios de los usuarios

Los respaldos manejarlos vía internet o almacenarlos en lugar diferente al que las originó

Configurar las opciones de seguridad en cuanto a navegadores, email y cuentas en portales web

Un correcto check list de permisos al abrir cualquier archivo ayuda bastante a evitar el acceso mal intencionado

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

A continuación relaciono las diferencias entre los equipos a estudiar:

Tabla 2. Diferencia entre los equipos

Equipo Blue team	**Equipo de respuesta a incidentes informáticos**
Este equipo se basa en la seguridad defensiva	El equipo de respuesta se enfoca en las incidencias de seguridad informática
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)
Ataque: amenaza, riesgo	Incidencia: hecho sospechoso o real
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
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
Rastrea incidentes de Ciberseguridad	Gestión de incidentes
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
Verifica la efectividad de las medidas de seguridad	Respuesta rápida y efectiva, lo cual le permitirá a la organización operar con total normalidad
Instalación software IDS e IPS como esquema para su protección	

Fuente: Autor

4.4 ANÁLISIS SOBRE LA PERTINENCIA DE TRABAJAR CON CIS “CENTER FOR INTERNET SECURITY” COMO PROPUESTA DE ASEGURAMIENTO POR PARTE DE UN EQUIPO DE BLUE TEAM.

El objetivo principal del Centro para la seguridad de internet es identificar, ejecutar, validar y mantener soluciones para ciberdefensa basándose en la ardua experiencia de los profesionales en esta rama. CIS cuenta con controles que permiten la configuración segura de un sistema los cuales se ajustan a normas establecidas.

El CIS lo utilizaría ya que es reconocido como un estándar de seguridad contra ciberataques y pueden llegar a controlar cuando el atacante:
Espera la oportunidad de que se conecten a la red equipos desprotegidos
Compromete el sistema explorando remotamente o cuando por medio de la red distribuye material malicioso
Aprovecha los avisos de seguridad
Aprovecha el mal uso de privilegios como por ejemplo ser engañados para abrir un archivo malicioso o ingresar a páginas que permiten ala atacante acceder al sistema
Explota ciertas vulnerabilidades como puertos abiertos, contraseñas/cuentas inseguras o predeterminadas y preinstalación de software que no es necesario
Aprovecha de las inconsistencias en el registro para ocultar su ubicación, software malicioso y actividades a ejecutar en las maquinas victimas pasa prácticamente desapercibido
Engaña a los usuarios permitiendo la perdida de datos importantes y la introducción de código malicioso
Busca servicios mal configurados, contraseñas predeterminadas para aprovecharse y explotarlos
Comprometen los sistemas al alterar la configuración, el software e información almacenada
Aprovecha que la información confidencial esta guardada con la misma seguridad que la información común
Aprovecha la conexión inalámbrica para tener acceso a largo plazo de la organización objeto
Descubre y explota cuentas de usuario que por diferentes motivos ya no se utilizan pero son legítimas y así suplantarlas lo que le permite no ser descubierto
Aprovechan las vulnerabilidades de software como errores de programación, de lógica, y gestión de memoria deficiente

4.5 ANÁLISIS SOBRE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM

La informática SIEM Seguridad de Información y Gestión de eventos tiene como función principal detectar amenazas potenciales y resolverlas con eficacia en el menor tiempo posible.

4.5.1 Funciones:

Presenta en tiempo real análisis de ataques de seguridad tanto hardware como software alertando dependiendo el progreso de las mismas
Preventivamente detecta amenazas, ataques, mal funcionamiento, mal uso pudiendo precisar cuáles son de mayor riesgo
Resuelve de una manera rápida y eficaz la respuesta ante amenazas
Centraliza el almacenamiento en un solo punto
Acorta los tiempos de actuación
Visión global de la seguridad de la tecnología de la información

4.5.2 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.

4.6 INFORME DE ELECCIÓN DE 3 HERRAMIENTAS QUE PERMITAN CONTENER ATAQUES INFORMÁTICOS.

Teniendo en cuenta la observación descrita en el anexo 5 Escenario 4 me permito seleccionar 3 herramientas que permitan contener ataques y que sean de licencia GPL

4.6.1 Snort 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 trafico coincide con alguna de las regla de ser así rechazará el trafico permitiendo así bloquear al atacante.

4.6.2 Openwips-ng 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

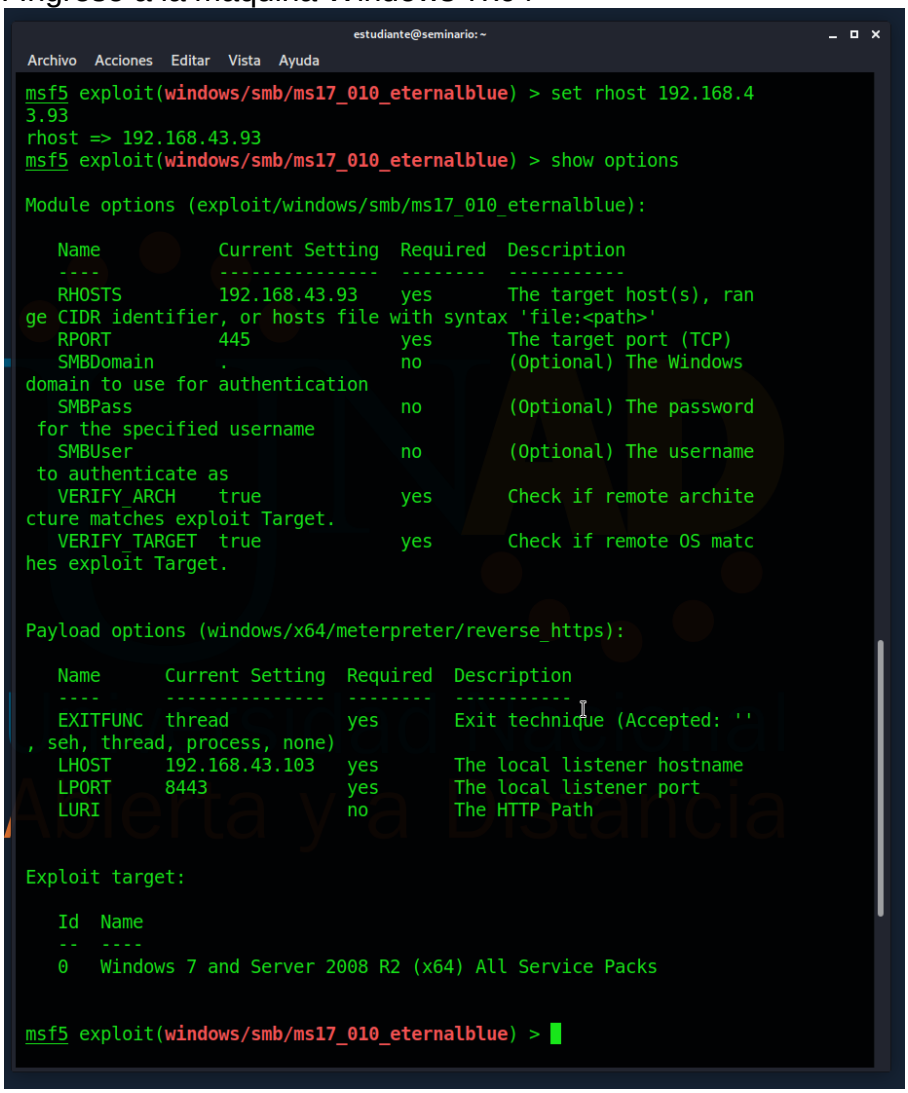
4.6.3 Ossec es una herramienta gratuita:
Permite realizar análisis de registro
Detección de rootkit
Verificación de integridad e información de alertas
Permite administrar y llevar fácilmente el monitoreo de varios sistemas
Lleva el registro de varios dispositivos y formatos gracias a que cuenta con un motor de análisis
Puede realizar la detección de ataques para casi todos los sistemas operativos

4.7 PASOS PARA RESPONDER AL ATAQUE

Para iniciar el proceso activaré el firewall, update y antivirus en la máquina Windows 7x64

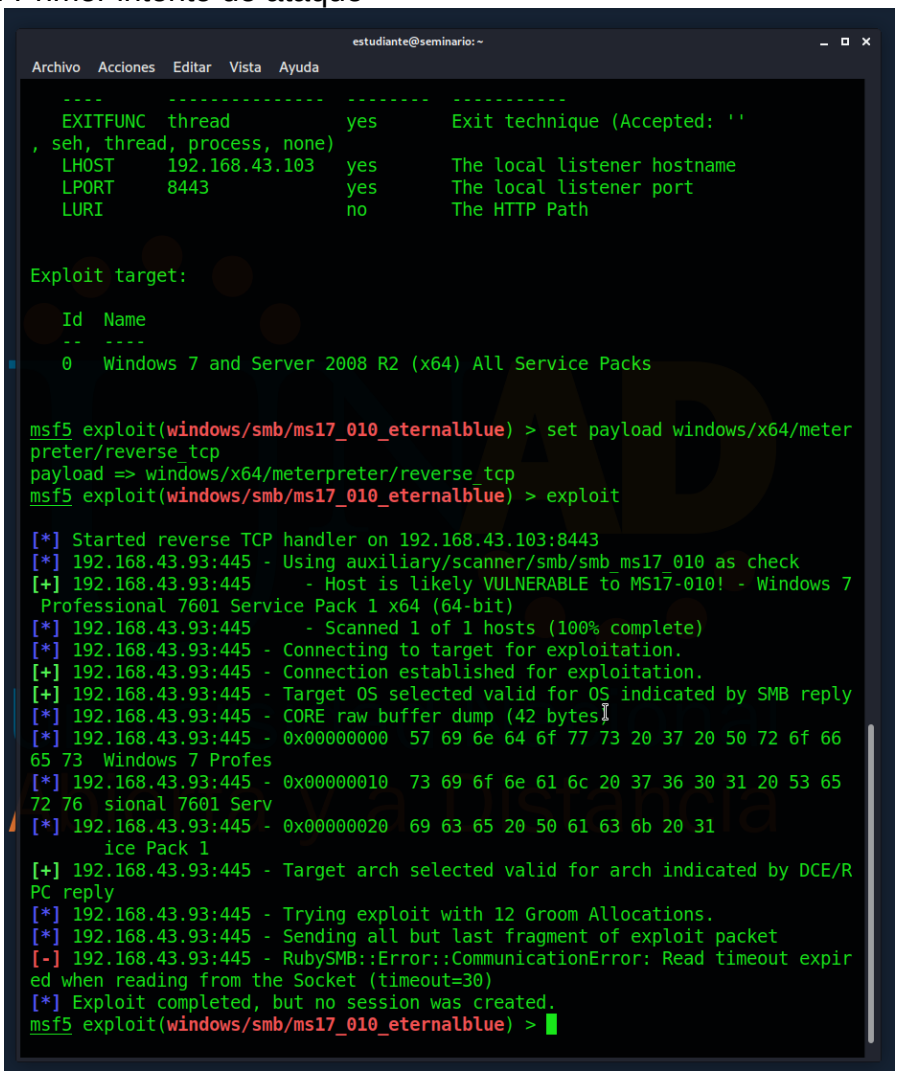
Luego se procede a atacar varias veces el equipo donde se evidencia que el Firewall cumple con no permitir la intrusión de igual forma quedo pendiente la actualización del parche MS17-010 para que al momento del ataque la vulnerabilidad no sea efectiva.

Figura 30. Ingreso a la máquina Windows 7x64



Fuente: Autor

Figura 31. Primer intento de ataque



Fuente: Autor

Figura 32. Segundo intento de ataque

Fuente: Autor

CONCLUSIONES

Es de suma importancia mantenerme muy bien informada de las leyes que rigen en Colombia sobre la protección de la información, de los datos personales y de todos los riesgos que corre esta información al estar en las manos de un tercero o expuesta a una mala administración.

Como se dio a conocer en este trabajo es de vital trascendencia saber que estoy amparada por un código de ética al momento de firmar un contrato laboral que además de indicarme los alcances de las acciones como profesionales también indica lo que conllevaría si llegase a fallar en alguna de las leyes y que dependiendo de la falta podría llegar hasta la cancelación de mi matricula profesional. Concluí que por más atractiva que se vea una oferta de trabajo y donde son muchos los beneficios que voy a recibir en cuanto a dinero y experiencia no debo dejar de lado las leyes y ética que me gobiernan ya que serán las que hablen de mí actuar ante otros posibles trabajos.

El proceso de penetración cuanta con 4 etapas definidas donde paso a paso se analiza un sistema de información en busca de vulnerabilidades y permite presentar un informe concreto de los hallazgos y la explotación realizada a esas vulnerabilidades. Durante el desarrollo del informe se tienen en cuenta las 4 etapas dando a conocer cada una de las herramientas utilizadas y su funcionalidad. Al realizar este proceso me permitió identificar las debilidades, carencias de programas y las vulnerabilidades a aprovechar para realizar el ataque y así obtener información valiosa del objetivo, se utiliza Nmap y Metasploit para automatizar la detección.

Para explotar las vulnerabilidades se utilizó Metasploit porque simplifica la detección de redes, permite concentrarse en aspectos específicos en las pruebas de penetración y además aumenta la eficacia de los escaneos de vulnerabilidad, hoy en día las organizaciones se centran más en detectar amenazas y responder a las mismas que en revisar su capacidad de contener un ataque ya sea por presupuesto, planes estratégicos, exceso de herramientas que se utilizan en la organización, la falta de planes de respuesta etc., llevando a que las probabilidades de experimentar un ataque sean altas.

Al momento de seleccionar una herramienta de contención siempre se debe tener en cuenta múltiples factores del sistema y lo más importante la capacidad de respuesta ante incidencias presentadas en tiempo real, en este momento es donde realmente se evalúa la capacidad tanto del profesional como de la herramienta seleccionada.

RECOMENDACIONES

Disponer de la activación y actualización constante del software de seguridad, sistema operativo y programas ya que del buen funcionamiento de estos dependerá en gran parte la respuesta a los ataques

Estar informados en cuanto a las normas y leyes que rigen en nuestra país sobre la protección de datos personales y tener en cuenta además el código de ética que nos rige como profesionales en la rama de la ingeniería

Estar actualizado en el manejo de cada una de las herramientas diseñadas para la detección de vulnerabilidades, explotación y contención de ataques

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”

HACKING PARA NOVATOS “Fases de una auditoria (pentesting)”. Internet: (https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/)

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/)

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

WIKIPEDIA “Nmap”. Internet: (https://es.wikipedia.org/wiki/Nmap)

WIKIPEDIA “Nmap”. Internet: (https://es.wikipedia.org/wiki/Nmap)

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)

3DJUEGOS “¿Qué es CVE? Ocho siglas relacionadas con las vulnerabilidades”. Internet: (https://www.3djuegos.com/comunidad-foros/tema/48444082/0/articulo-que-es-cve-ocho-siglas-relacionadas-con-las-vulnerabilidades/)

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.

HACKING PARA NOVATOS “Fases de una auditoria (pentesting)”. Internet: (https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/)

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)

WIKIPEDIA “Nmap”. Internet: (https://es.wikipedia.org/wiki/Nmap)

WIKIPEDIA “Nmap”. Internet: (https://es.wikipedia.org/wiki/Nmap)

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)

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

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

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.)

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

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

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

Este Anexo lo puede encontrar en el siguiente Link:

https://drive.google.com/file/d/1Zz6XEC8y36IUqDlOf-GAHc07Vna_1pJf/view?usp=sharing

ANEXO B. VÍDEO SUSTENTACIÓN INFORME TÉCNICO

Este Anexo lo puede encontrar en el siguiente Link:

Drive
https://drive.google.com/file/d/155C4oTHPVgcB6rKQ7uzHHSkDhvbOSiPa/view?usp=sharing

YouTube
https://youtu.be/6d1xdN74mbo