SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

CESAR AUGUSTO FERNANDEZ QUILINDO

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

Director curso.

M.Sc. Jhon Freddy Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Vicerrectoría Académica y de Investigación
Popayán
2021

RESUMEN

En el presente documento, se relaciona el informe técnico final donde se plantearon y estructuraron estrategias de seguridad informática relacionadas con actividades propuestas en el seminario especializado en seguridad informática equipos estratégicos en ciberseguridad: red team & blue team, donde se proponen una serie de casos estudio enfocados con la seguridad de la empresa The WhiteHose Security.

El contenido del informe técnico se estructura basado en el desarrollo de 4 etapas: Etapa 1 - Conceptos equipos de Seguridad, Etapa 2 - Actuación ética y legal, Etapa 3 - Ejecución pruebas de intrusión y Etapa 4 - Contención de ataques informáticos. En la primera etapa se identifica y caracteriza el problema y se realiza el despliegue de infraestructura necesaria para dicho proceso. En la segunda etapa se presenta el caso de análisis de contratación relacionado con personal que se requiere vincular al equipo red team & blue team de la empresa The WhiteHose Security. En la tercera etapa se analizan metodologías de pruebas para la penetración de la seguridad informática, utilizando herramientas especializadas; se hace la explotación del sistema y se identifica las vulnerabilidades que tiene la organización con respecto a su seguridad. En la cuarta etapa se realiza un estudio minucioso de las vulnerabilidades y se genera plan de mejora de la seguridad de la empresa.

Con el desarrollo de las actividades anteriormente mencionadas el informe técnico finaliza realizando recomendaciones y conclusiones en relación con las estrategias y actividades desarrolladas por el equipo red team & blue team de la empresa The WhiteHose Security.

CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

Pág.

GLOSARIO

METASPLOIT: Es una herramienta pentest, la cual permite desarrollar y ejecutar procesos exploits, en el cual identifica los diferentes tipos de vulnerabilidades y es en una ayuda muy precisa en la prueba de penetración. Este tipo de herramienta la podemos encontrar disponibles en sistemas operativos como Unix, Linux, MAC, BSD y en las 3 versiones de sistemas operativos de Windows.

NMAP: Es una herramienta de código abierto que permite la exploración de redes y auditoria de seguridad. Su diseño permite el análisis, ejecutar proceso y procedimientos en grandes redes, aunque también funciona con equipos individuales.

OPENVAS: Es una herramienta de uso libre, que permite identificar vulnerabilidades logrando realizar correcciones de fallas de seguridad. Este framework que su base de operación son servicios y herramientas para poder evaluar vulnerabilidades, se puede utilizar de forma individual o e manera conjunta con otras herramientas de seguridad.

EXPLOITDB: Este tipo de herramienta permite realizar una copia de seguridad del proceso realizado en la web exploitdb, permitiéndonos realizar una búsqueda más de talladas de la información fuera de línea de a través de un proceso de copia local. Este tipo de herramienta es muy útil en los procesos que evaluación de seguridad de una red que no cuente con la posibilidad de ingreso a internet.

CVE: Tipo de herramienta cuya característica son las vulnerabilidades y exposiciones comunes, en las bases de datos. El uso de esta herramienta se enmarca en generar un listado de información donde se tienen las vulnerabilidades o fallas de los sitios oficiales de la CVE, este tipo de listas se encuentran disponibles al público.

NESSUS: Esta herramienta utiliza procesos de escaneo, búsqueda de algún tipo de vulnerabilidad en la red y sus posibles soluciones; permite emitir resultados en un informe final desde donde se clasifica cada uno de los análisis realizados.

BLUETEAM: Equipo azul, grupo de personas que realizan análisis de los sistemas informáticos, permitiendo garantizar la seguridad, identificar fallas de seguridad, verifica efectividad de las medidas adoptadas y se aseguran de que

las medidas de seguridad implementadas continúen siendo eficientes para la seguridad de la empresa.

REDTEAM: Equipo rojo, grupo de personas que ayuda a una organización a mejorar sus sistemas de seguridad a través de la utilización e implementación de ataques sectorizados algún objeto de la empresa, permitiendo el estudio de sus vulnerabilidades.

VULNERABILIDAD: Defecto que se puede presentar en un sistema informático, el cual puede provocar su desprotección ante cualquier atacante del sistema de una organización. También está asociada al conjunto de procedimientos que permita que la seguridad de una organización se encuentre expuesta ante una amenaza.

HARDENIZACION: Proceso de asegurar un sistema mediante la minimización o mitigación de vulnerabilidades en el mismo; permite eliminar software, servicios, usuarios, entre otros; innecesarios en el sistema y de la misma manera puertos que no estén en uso.

PENTESTING: Practica que se realiza para poner a prueba la seguridad de un sistema informático, aplicación web o una red, en donde se establecen las posibles vulnerabilidades que un atacante podría explotar.

INTRODUCCIÓN

En el siguiente informe técnico se presentan las acciones relevantes, realizadas por el equipo Red team y Blue team de la empresa The WhiteHose Security, correspondientes al marco de los criterios éticos y legales de los procesos de seguridad informática, análisis e implementación de herramientas para realizar pruebas de penetración y herramientas de ciberseguridad.

Se planteará en detalle los procesos y procedimientos realizados en las diferentes etapas del pentesting, las herramientas utilizadas en cada una de estas etapas y sus respectivos análisis en el sistema indagado. Se caracterizará los factores de vulnerabilidad a partir del análisis de riesgos de seguridad en el sistema informático de la empresa, dando a conocer las respectivas acciones para minimizar o mitigar ataques que se realicen en tiempo real; teniendo en cuenta funciones y características de la informática SIEM.

En los procesos de ciberseguridad cada día se generan nuevas amenazas y vulnerabilidades, que parten en suplantar herramientas ya existentes que tiene alterado su contexto y en vez de ser una herramienta para nuestra seguridad, se convierte en un elemento que logra vulnerar nuestro sistema conociendo información importante de la empresa: por esto es de suma importancia saber qué tipo de herramienta de contención vamos a emplear, respondiendo eficientemente a las amenazas que se presenten.

OBJETIVOS

Objetivo general.

Socializar informe técnico sobre los procedimientos de seguridad informática desarrollados con el equipo Red team y Blue team de la empresa The WhiteHose Security, cumpliendo normas y procedimientos de seguridad establecidos por la empresa.

Objetivos específicos.

- Analizar los requerimientos del cliente y la normatividad sobre procesos de seguridad informática.
- Implementar acciones metodológicas de seguridad planteadas por el equipo Red team y Blue team de la empresa The WhiteHose Security.
- Establecer conclusiones y recomendaciones a mejorar en las estrategias usadas por el equipo Red team y Blue team de la empresa The WhiteHose Security.

DESARROLLO DEL INFORME TÉCNICO

1. Etapa 1: Conceptos equipos de Seguridad

- ✓ Anexo 1 – Escenario 1.

Situación problema: Montaje banco de trabajo.

The Whitehouse Security requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de The WhiteHouse Security. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.

De manera simultánea The WhiteHouse security requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

1.1 Normativas sobre delitos informáticos.

Procesos fundamentales relacionados con las leyes 1273 de 2009 y 1581 de 2012.

1.1.1 Ley 1273 de 2009.

Ley Colombiana que permite realizar modificaciones al código penal, en cual se crea un bien jurídico tutelado que se identifica con el nombre “de la protección de la información y de los datos”.[1]

Características artículos que está compuesta esta ley:

- **Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.**
- **Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.**
- **Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.**
- **Artículo 269D. DAÑO INFORMÁTICO.**
- **Artículo 269E. USO DE SOFTWARE MALICIOSO.**
- **Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.**

[1] Ley 1273 2009. (5 de enero 2009) Normatividad – Leyes. Obtenido. Dirección de apropiación de las TIC . ministerio de las tecnologías de la información y comunicaciones: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- **Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.**
- **Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.**
- **Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.**
- **Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.**

1.1.2 Ley 1581 de 2012.

"Ley que permite la protección de datos personales que se encuentren registrados en cualquier base de datos".[2]

Principios característicos de la ley:

- **Principio de legalidad en materia de Tratamiento de datos:**
  Es una ley que esta reglamentada y que está sujeta a lo establecido en ella y que en lo que la desarrolle.
- **Principio de finalidad:**
  Debe obedecer el tratamiento a una finalidad legitima y que este acorde a la constitución y la ley.
- **Principio de libertad:**
  Este tratamiento solo puede ejercerse con el consentimiento del titular y los datos personales no podrán ser obtenidos o divulgados sin algún tipo de autorización.
- **Principio de veracidad o calidad:**
  La información en tratamiento debe ser completa, exacta, comprobable y comprensible.
- **Principio de transparencia:**
  Es preciso determinar que la información en tratamiento debe garantizar el derecho del titular a conocer en cualquier momento.
- **Principio de acceso y circulación restringida:**
  La información que se encuentre en tratamiento se debe regir a los límites que derivan de la naturaleza de los diferentes datos personales, de la ley y constitución.
- **Principio de seguridad:**
  Se debe manejar la información sujeta a tratamiento con todas las técnicas necesarias tanto administrativas como humanas.
- **Principio de confidencialidad:**
  Se debe garantizar la reserva de la información tratada, inclusive después de realizar el respectivo trabajo de tratamiento.

[2] Ley estatutaria 1581 del 2012 (octubre 17 de 2012). Senado de la república de Colombia. Obtenido Diario Oficial No. 48.587: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

1.2 Herramientas utilizadas para la prueba de penetración.

1.2.1 Fase 1: Recolección de información.

En esta fase nos dedicamos a recolectar toda la información posible que la empresa tenga disponible identificando los sistemas y programas en funcionamiento que ella tiene.

Herramienta: scanner y arañas que permiten la recolección total de la información.

1.2.2 Fase 3: Análisis de vulnerabilidades.

En esta fase se valoran los casos exitosos de nuestras estrategias de penetración a través del análisis y proactividad de vulnerabilidades.

Herramientas: NESSUS, Nmap, CVE.

1.2.3 Fase 4: Explotación.

En esta fase se inicia el proceso de intentar conseguir los accesos a los diferentes sistemas objeto de nuestra prueba de penetración.

Herramientas: Metasploit, exploitdb.

1.2.4 Fase 5: Informe.

En esta fase final es donde se presenta el resultado de la prueba de penetración, donde se identifica con claridad los riesgos que se pueden presentar según las vulnerabilidades encontradas.

Herramientas: Sistemas ofimáticos para entrega de los respectivos informes.

1.3 Herramientas utilizadas en procesos de Ciberseguridad.

1.3.1 Metasploit.

Es una herramienta pentest, la cual permite desarrollar y ejecutar procesos exploits, en el cual identifica los diferentes tipos de vulnerabilidades y es en una ayuda muy precisa en la prueba de penetración.

En la característica de uso de esta herramienta encontramos 3 acciones importantes de referenciar:

- Metasploit Framework.
- Metasploit Express 4.0.
- Metasploit Pro-3.5.

1.3.2 Nmap.

Es una herramienta de código abierto que permite la exploración de redes y auditoria de seguridad. Su diseño permite el análisis, ejecutar proceso y procedimientos en grandes redes, aunque también funciona con equipos individuales.

1.3.3 OpenVas.

Es una herramienta de uso libre, que permite identificar vulnerabilidades logrando realizar correcciones de fallas de seguridad.

1.3.4 ExploitDB.

Este tipo de herramienta permite realizar una copia de seguridad del proceso realizado en la web exploitdb, permitiéndonos realizar una búsqueda más de talladas de la información fuera de línea de a través de un proceso de copia local.

1.3.5 CVE.

Tipo de herramienta cuya característica son las vulnerabilidades y exposiciones comunes, en las bases de datos.

1.4 Instalación banco de trabajo.

1.4.1 Prueba de conectividad entre maquinas “win 7 – SE2020-X64” y maquina “win 7 – SE2020”

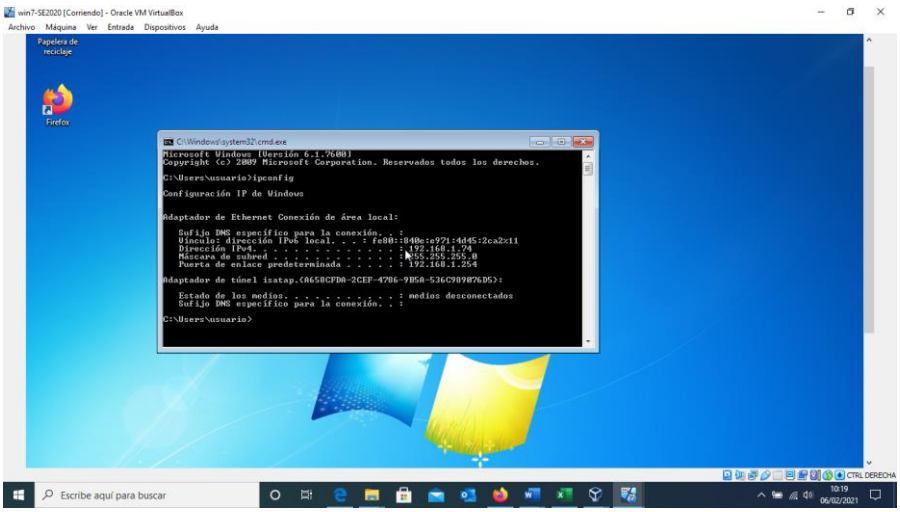
Paso 1: Encendemos las dos máquinas correspondientes de prueba.

Figura 1 Entorno máquina Virtual win 7 x64 y x86.

Fuente: Autor

Paso 2: Identificamos la dirección IP asignada a la maquina “win 7 – SE2020”. IP: 192.168.1.74 MODO RED: Adaptador Puente.

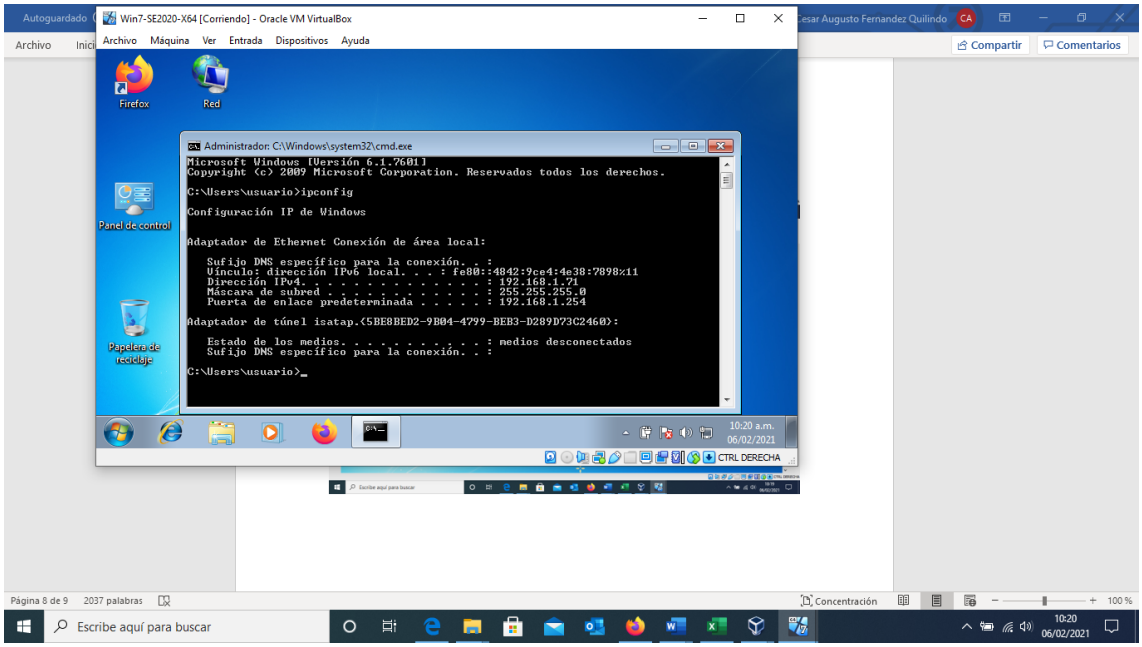
Figura 2 Dirección IP win 7 se2020.



Fuente: Autor

Paso 3: Identificamos la dirección IP asignada a la maquina “win 7 – SE2020-64”. IP: 192.168.1.71 MODO RED: Adaptador Puente.

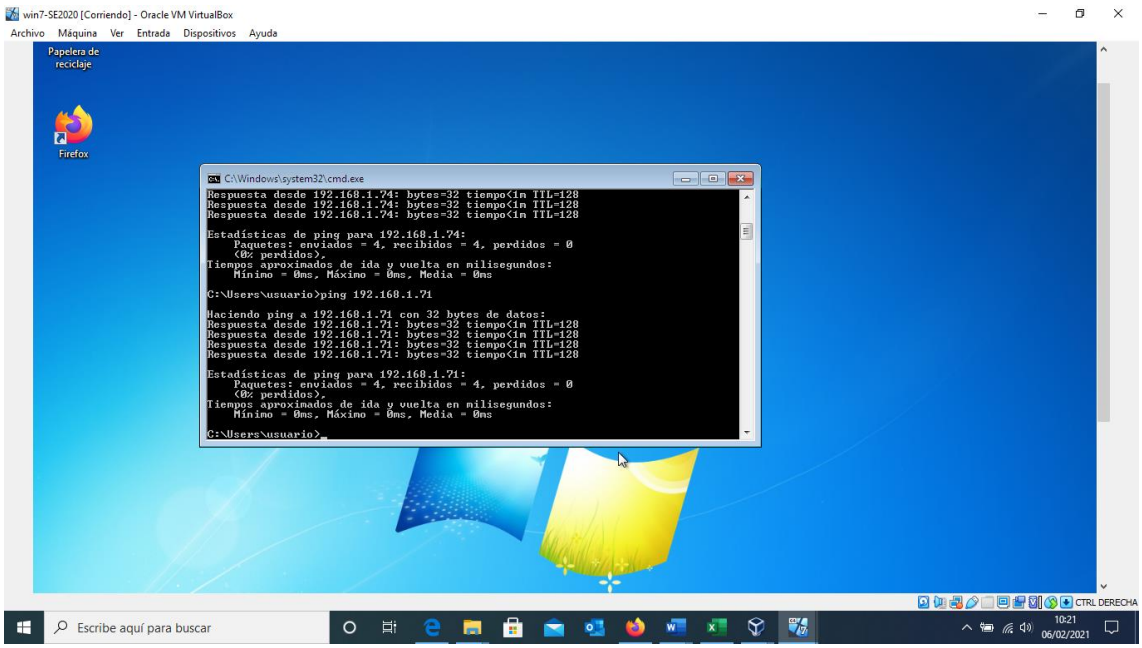
Figura 3 Dirección IP win7 SE2020 x64.



Fuente: Autor

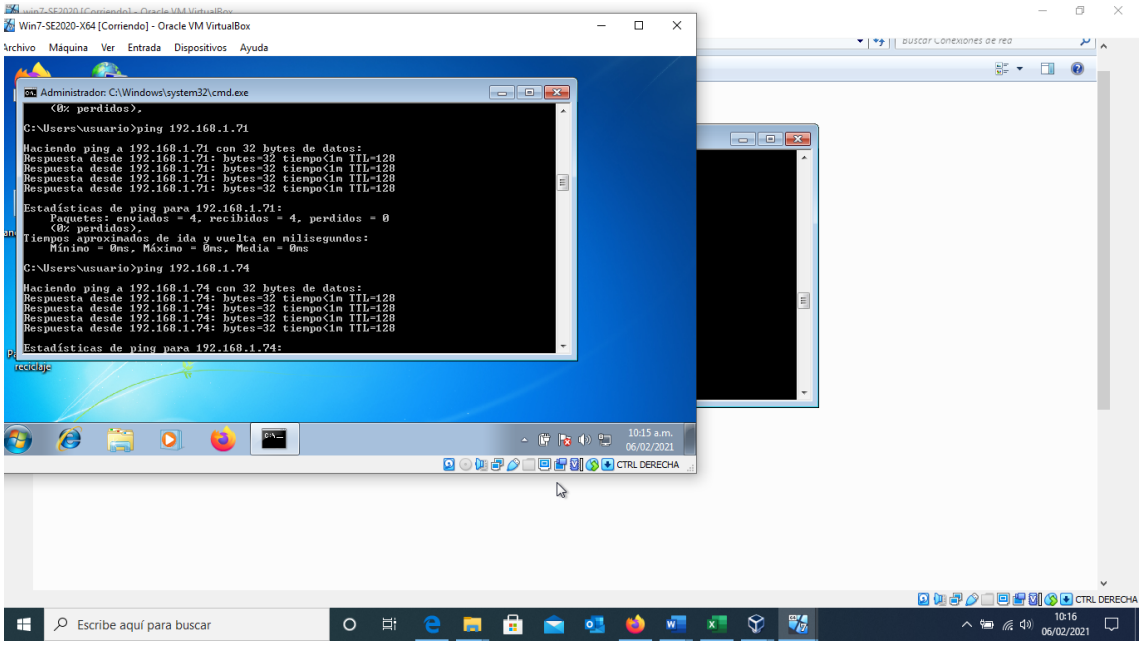
Paso 4: Verificamos conectividad entre las máquinas virtuales.

Figura 4 Verificación conectividad win 7 SE 2020.



Fuente: Autor

Figura 5 Verificación conectividad win 7 SE2020 x64.



Fuente: Autor

1.4.2 Prueba de conectividad entre maquinas “Kali - seminario” y maquina “win 7 – SE2020”

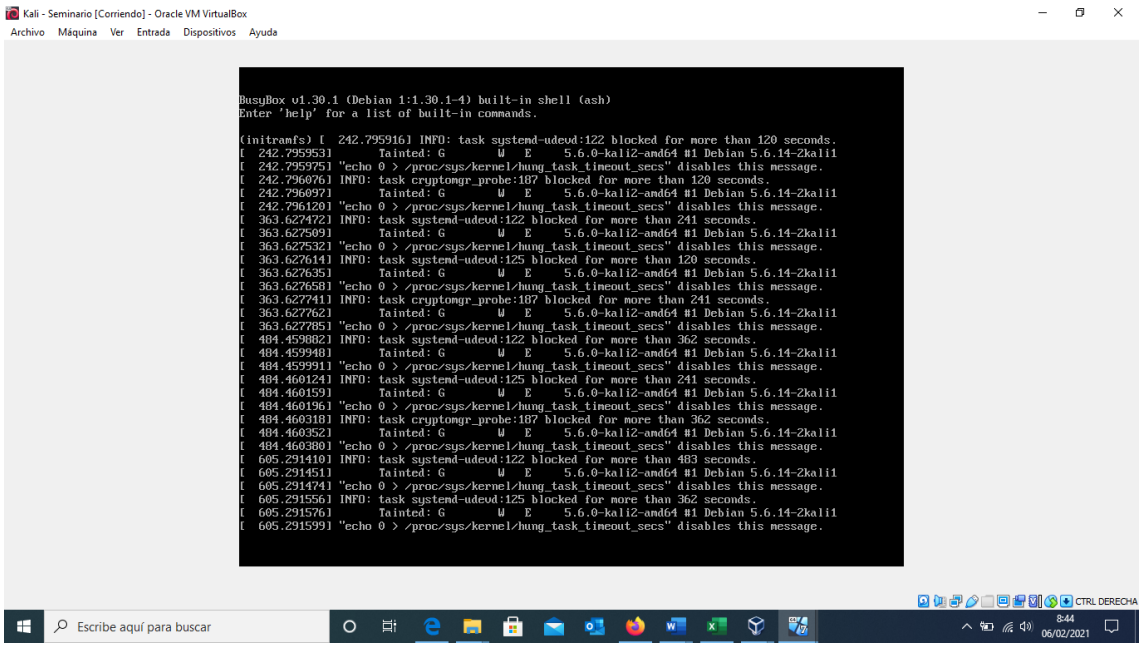
Paso 1: Encendemos las dos máquinas correspondientes de prueba.

Figura 6 Entorno máquinas virtuales win 7 SE 2020 y Kali seminario.

Fuente: Autor

Paso 2: Cargamos los archivos de Kali – seminario.

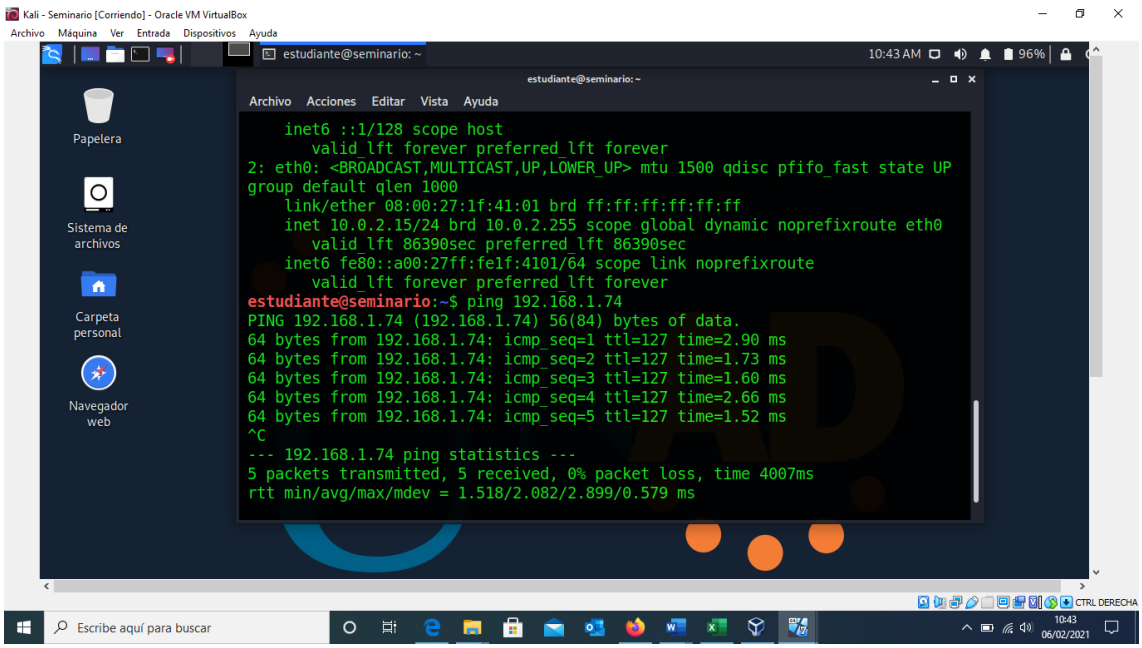
Figura 7 Cargue archivos Kali - seminario.



Fuente: Autor

Paso 3: El ping es exitoso desde la máquina de Kali – seminario a la maquina win 7 – SE2020

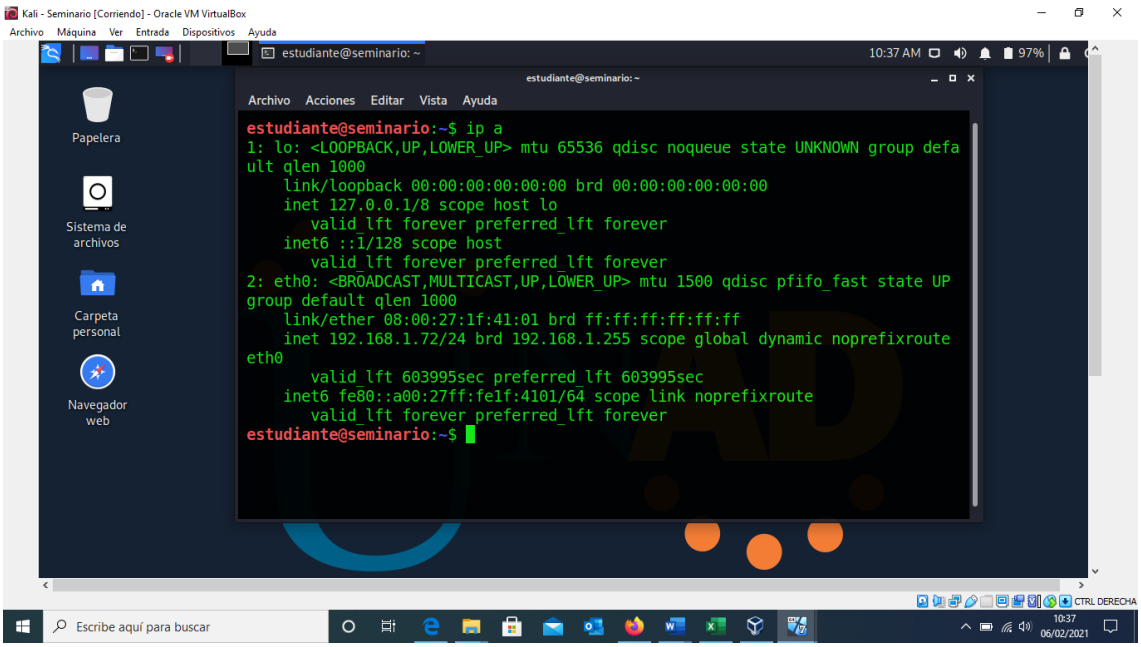
Figura 8 Conectividad entre Kali seminario y win 7 SE 2020.



Fuente: Autor

Paso 4: Configuración MODO Adaptador Puente. IP 192.168.1.72

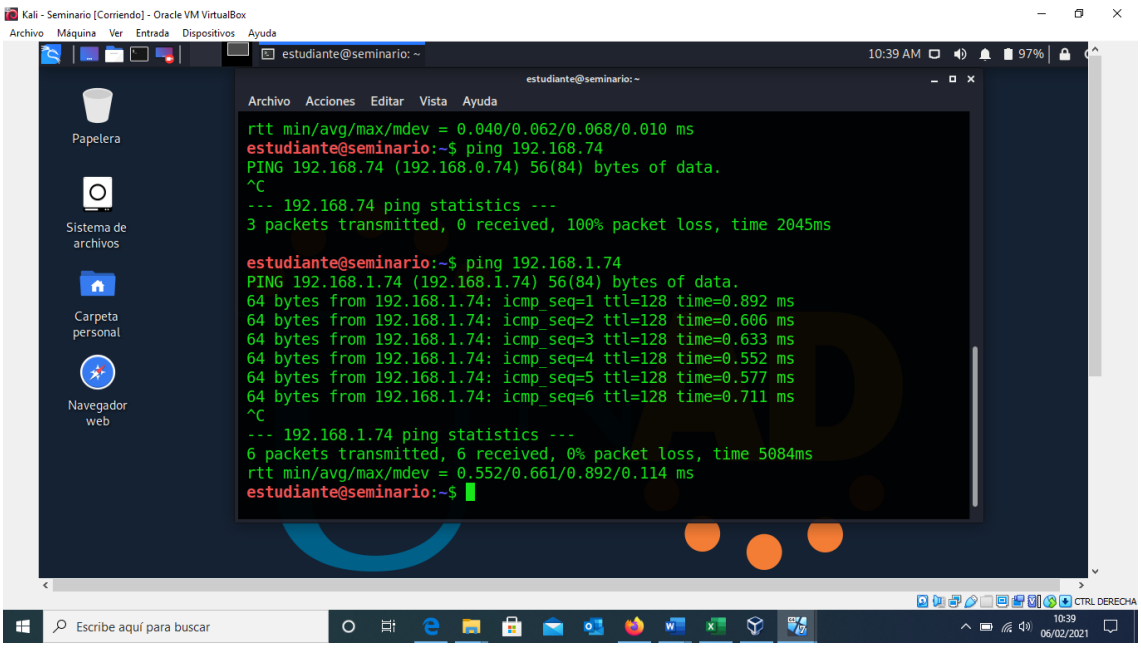
Figura 9 Dirección IP Kali seminario.



Fuente: Autor

Paso 5: Ping éxitos con la maquina win 7 – SE2020.

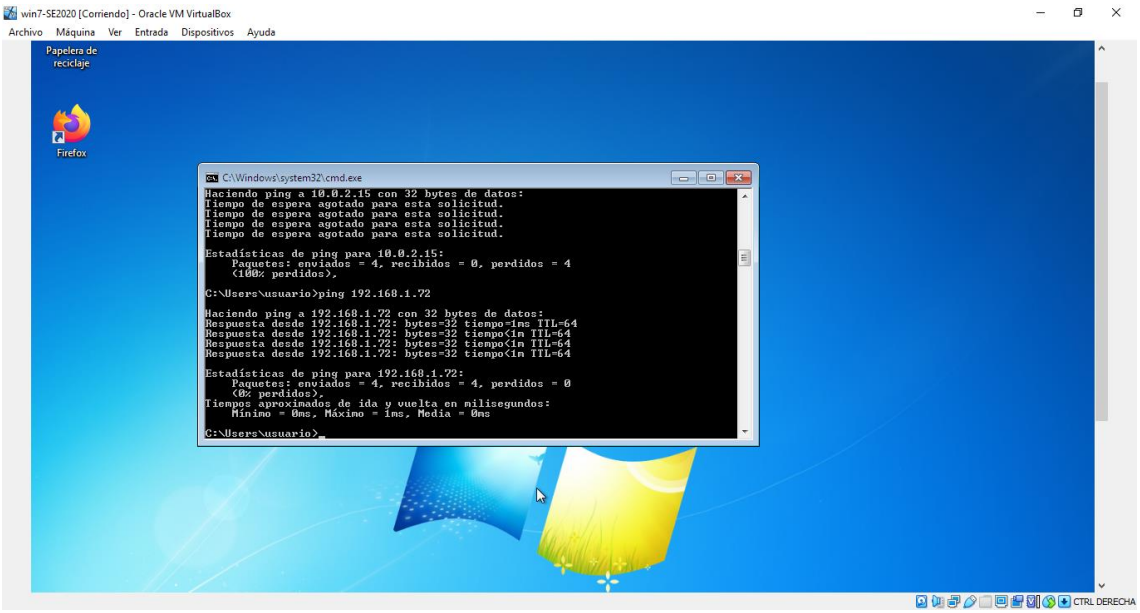
Figura 10 Conectividad win 7 SE 2020.



Fuente: Autor

Paso 6: Ping éxitos con la maquina Kali – seminario.

Figura 11 Conectividad Kali seminario.



Fuente: Autor

1.4.3 Prueba de conectividad entre maquinas “Kali - seminario” y maquina “win 7 – SE2020X64”

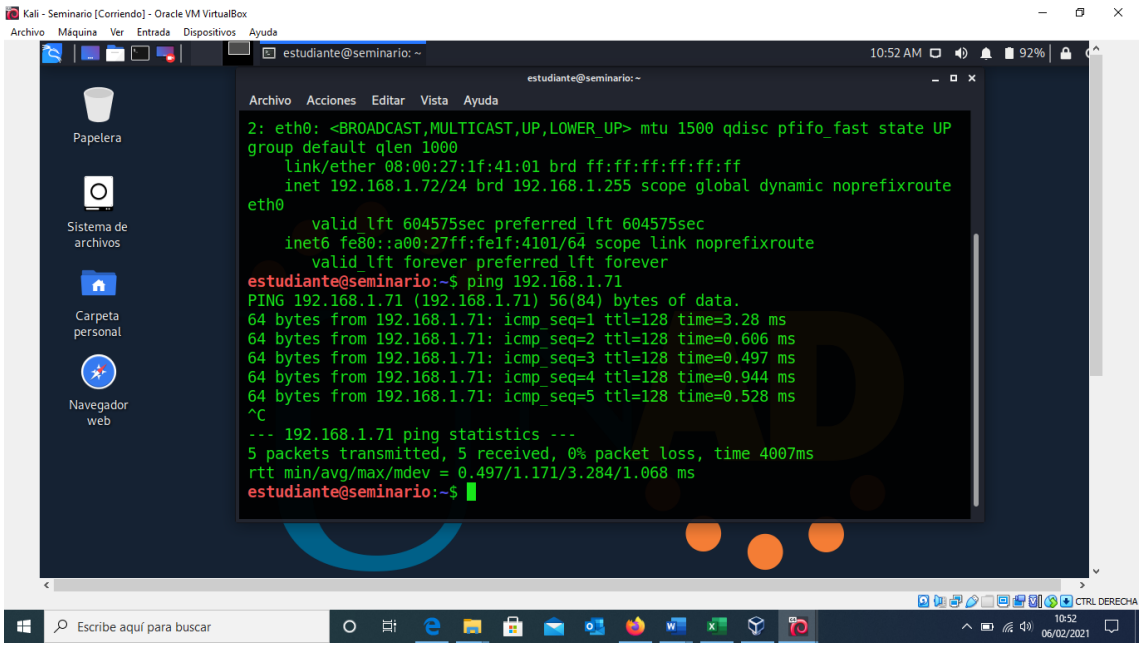
Paso 1: Encendemos las dos máquinas correspondientes de prueba.

Figura 12 Entorno máquinas virtuales.

Fuente: Autor

Paso 2: Realizamos las pruebas de conectividad desde la maquina Kali – seminario hacia la maquina win 7 – SE2020X64. Exitoso.

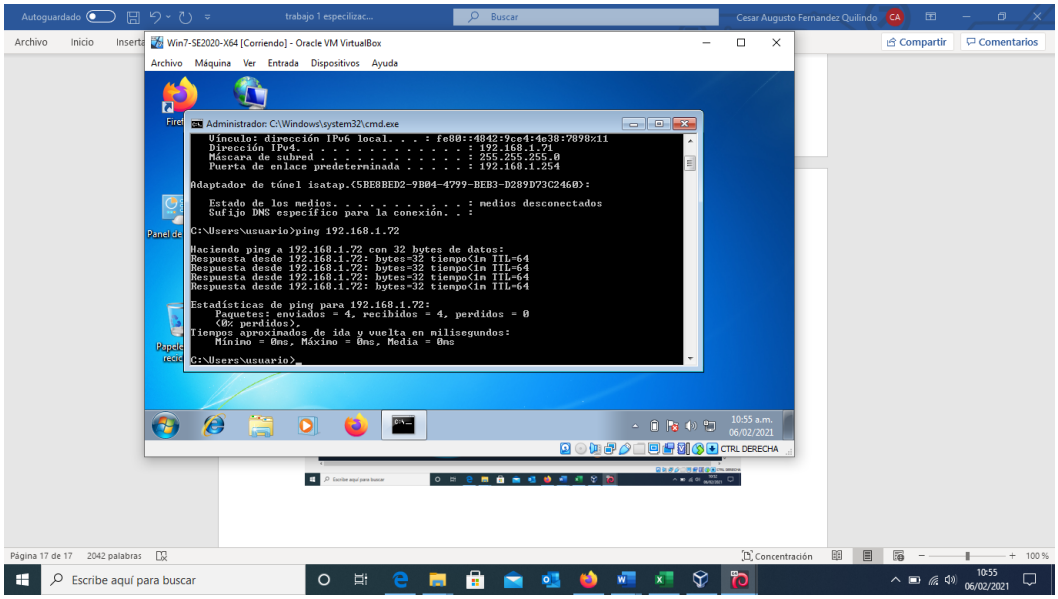
Figura 13 Conectividad win 7 SE 2020 x 64.



Fuente: Autor

Paso 3: Realizamos las pruebas de conectividad desde la maquina win 7 – SE2020X64 hacia la maquina Kali – seminario. Exitoso.

Figura 14 Conectividad Kali seminario.



Fuente: Autor

2. Etapa 2 Actuación ética y legal.

- ✓ Anexo 2 – Escenario 2

Situación problema: Análisis legal.

La organización WhiteHouse Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.

Para dar inicio, la organización WhiteHouse Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión “característica” de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

- ✓ Anexo 3 – Acuerdo

Situación problema: Análisis legal.

ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y WHITEHOUSE SECURITY.

2.1 Análisis acuerdo legal contrato, proceso legal y no ético del escenario 2 – acuerdo.

2.1.1 Clausula primera.

“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”.

Los fragmentos resaltados “autoridades legales” y “sobre procesos ilegales dentro de whitehouse Security no podrán ser divulgados”, permite omitir información sobre el proceso realizado, ocasionando perdida de confidencialidad del tratamiento de la información de la empresa. Con este proceso se limita las acciones de denuncia ante autoridades competentes, dentro de las posibilidades de sospechas de algún tipo de espionaje o cualquier tipo de proceso por el cual intervenga terceros con respecto a la apropiación de la información de la empresa.

2.1.2 Clausula segunda.

“Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la parte receptora con ocasión del proceso de selección de personal.

2. 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”. Parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones”.

La parte resaltada “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”, en este apartado se presenta un procedimiento no ético al suministrar u otorgar información de manera ilegal, sabiendo cuales son los debidos procesos y procedimientos legales que existen para poder tratar la información de la organización. Es preciso que las autoridades tratantes de la información respondan por el mal uso de estos procesos.

2.1.3 Clausula 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.

La parte resaltada “independiente de su fuente o soporte”, se denota que a pesar de que la cláusula es clara de donde proviene la diferente información a tratar, no precisa las respectivas formas, procedimientos fuentes o soportes que se van a tener en cuenta para lograr su adquisición, incurriendo en procesos ilegales los cuales las leyes de nuestro país la denominan como delitos.

2.1.4 Clausula cuarta.

Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la información confidencial segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la información confidencial, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de

la misma Whitehouse Security, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

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

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

5. Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

6. Mantener la información confidencial en reserva hasta tanto adquiera el carácter de pública.

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

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

9. 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.

Parágrafo: Cualquier divulgación autorizada de la información confidencial a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente Acuerdo y la parte receptora deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

La parte resaltada “3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros”, hacia este proceso en donde no se denuncie actividades que provoquen sospechas de delitos asociados a espionajes u otra actividad asociadas, se pude identificar que muchas de las anteriores actividades de mencionamos están relacionadas con extorciones, algún tipo de secuestro y hasta actos mortales, y por lo cual el no denunciar este tipo de actos te puede volver cómplice de estos delitos.

La parte resaltada “4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas”, Con este proceso se limita las acciones de denuncia ante autoridades competentes, dentro de las posibilidades de sospechas de algún tipo de manipulación, cambio, modificación, o cualquier tipo de proceso por el cual intervenga terceros con respecto a tratamiento de la información de la empresa.

La parte resaltada “7. Responder por el mal uso que le den sus representantes a la información confidencial”, esta cláusula es muy particular pues en el momento de presentarse algún tipo de problema legal, las responsabilidades de procesos y procedimientos efectuados, también recae sobre el empleado y como consecuencia de este tipo de actos es la detención inmediata, según lo estipule la ley según la falta cometida, llegando con este proceso hasta perder el derecho de ejercer la profesión.

La parte resaltada “9. 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”, en este inciso se habla claramente de información confidencial o **“ILEGAL”**, por lo anterior la empresa u organización si es conocedora de que se incurre sobre procesos ilegales en la información que se maneja y que así se va a evidenciar cuando se le requieran.

2.1.5 Clausula 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 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.

La parte resaltada “En caso 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”, es preciso identificar que dentro de los proceso y procedimientos legales que se desarrollen en el tratamiento de la información de la organización, se cuenta con abogados propios de la empresa, contratados para tratar los aspectos de irregularidad y/o proceso legales correspondientes a la información de la organización.

2.2 Análisis ilegalidad según proceso establecido en la ley 1273 sobre el acuerdo.

- **Clausula primera:**

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.

Este artículo se aplica para el caso de ingreso sin autorización o sin ningún tipo de acuerdo establecido por la parte de seguridad, a la totalidad de la información o parcialmente al sistema informático.

- **Clausula segunda:**

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.

Artículo que se aplica en casos donde se interceptan información de origen, destino o en el interior de un sistema informático, sin ningún tipo de orden judicial que soporte esta acción realizada.

- **Clausula tercera:**

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.

Este tiene aplicación en el caso en donde tiene como objetivo ilícito y sin estar facultado para realizar estas acciones, diseñe, desarrolle, trafique, venda o envié páginas electrónicas, enlaces o ventanas emergentes.

- **Clausula cuarta:**

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.

Caso en el cual el personal sin estar facultado para realizar dichas acciones, con algún tipo de interés propio o de terceros, obtenga, sustraiga, venda, intercambie, divulgue o modifique datos personales contenido en un fichero, archivo y/o bases de datos.

Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.

Proceso que aplica para personal que, superando medidas de seguridad informáticas, realice manipulación de la información.

- **Clausula octava:**

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.

Proceso que se aplica a la persona que, sin estar facultada para desarrollar dicha acción, obstaculice o interfiera el normal funcionamiento de los sistemas informáticos, en sus datos de información ahí contenidos o no permita el acceso correcto a las redes de telecomunicaciones.

2.3 Análisis propuesta laboral – Punto de vista legal y ético.

- ✓ ¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? usted como experto en ciberseguridad aplicaría a este trabajo en The White House, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.

Como profesional y como experto en procesos de ciberseguridad, no aplicaría para este trabajo, ya que en las diferentes clausulas y acuerdos suscritos en el contrato, no se especifica de manera clara, concreta y detallada; las formas de cómo se va a desarrollar los diferentes procesos y procedimientos para el caso de tratar la información. Lo anterior genera un alto grado de desconfianza ya que se puede en algún momento estar incurriendo en delitos que la ley puede identificar como irregulares al debido proceso de la confidencialidad, integralidad, disponibilidad de los datos y de los sistemas informáticos, descritos en la ley 1273 de 2009.

También se debe tener en cuenta que, para tomar esta decisión, contamos con una herramienta fundamental que permite desarrollar de manera correcta y eficiente los procesos de tratamiento de la información y que se encuentra consignado en el código de ética de COPNIA, donde se establece del deber ser del ejercicio de la ingeniería.

Se enuncian algunos artículos de este código de ética COPNIA, que se deben tener en cuenta:

- **ARTICULO 31.**
  DEBERES GENERALES DE LOS PROFESIONALES.
- **ARTÍCULO 35.**
  DEBERES DE LOS PROFESIONALES PARA CON LADIGNIDAD DE SUS PROFESIONES.
- **ARTÍCULO 37.**
  DEBERES DE LOS PROFESIONALES PARA CON SUS COLEGAS Y DEMÁS PROFESIONALES.
- **ARTÍCULO 39.**
  DEBERES DE LOS PROFESIONALES PARA CON SUSCLIENTES Y EL PÚBLICO EN GENERAL".

2.4 Análisis de mi punto de vista sobre la noticia del caso "OPERACIÓN ANDROMEDA BUGGLY" en la ciudad de Bogotá.

Desde mi punto de vista teniendo como fundamento los proceso legales y éticos que se pueden analizar en el caso "OPERACIÓN ANDROMEDA BUGGLY" el cual de desarrollo en la ciudad de Bogotá, se pueden establecer varios puntos de estudio, partiendo que todo se desarrolla en un ámbito colaborativo donde se establecen sistemas de conocimiento con personas expertas en sus áreas de profesión, que a su vez buscan un trabajo en equipo para poder aprender cosas nuevas de cada uno de sus integrantes, en síntesis podemos estar hablando de un hackerspace (espacio de hackers), en donde su objetivo principal era hacerlo parecer una comunidad que se dedica a la seguridad informática y lo lograron. En el proceso de desarrollo de esta comunidad se presentaron algunos hallazgos que colocaron en duda su correcto funcionamiento, en este caso estamos hablando de la parte económica y de financiación de esta comunidad para soportar este tipo de proyectos; y en consecuencia con esto, también se analizaba el tipo de flexibilidad que se tenía para ingresar a este proyecto sin tener algún tipo de complicación para su vinculación.

Puedo entender con lo anterior que "BUGGLY", no era un lugar u organización sencilla en su estructura o en resumen un lugar el cual no se desarrollara grandes cosas como lo hicieron creer a muchos.

En la operación Andrómeda, desarrollada por parte de la inteligencia técnica del ejército nacional y en la cual se enmarcaba como objetivo principal adquirir conocimientos sobre hacking ético en donde solo se busca realizar pruebas en redes para poder identificar tipos de vulnerabilidades y luego ser reportadas buscando planes de mejoras sobre estas; en este caso no se busca realizar algún tipo de daño sobre los analizado. En un apartado de este análisis se identifica que el lugar no solo era visitado por personas del común que solo querían realizar dichos procesos, sino que también asistían militares o funcionarios de las fuerzas armadas. Otro caso que se presenta en esta operación aplica para la infraestructura de telecomunicaciones, en donde se dice que desde este lugar (Buggly) se realizaban caracterización y monitoreo del espectro, en donde se empleaban algunos malware para obtener información de personas, logrando la interceptación de comunicaciones, también se utilizaron software especializados los cuales permitían espiar equipos terminales de red (computadores), teniendo absoluto control de la información que en ellos se contenía tanto de entrada como de salida y que en un caso particular se utilizaba con las guerrillas de las FARC y ELN grupos al margen de la ley en Colombia; también se puede detallar dentro de este estudio que en algún momento se realizó espionaje al proceso de paz que se venía adelantado entre el gobierno y la guerrilla.

Ahora desde la información entregada por el General Ernesto Maldonado, todo se desarrollaba en un entorno legal, cobijada por la Constitución Política de Colombia y por los respectivos reglamentos y manuales de manejo de las redes informáticas. En contra de lo anterior se denota que, tanto en parte de los militares como de los civiles, no se tenía un control o supervisión de estas acciones que se desarrollaban en dicho lugar; teniendo por consecuencia el rompimiento de sus propios códigos de ética, suscitado por la ambición y el poder que esto ejercía, el dinero que se obtenía era demasiado y por consiguiente terminaban vendiendo la información a terceros con fines lucrativos y generando un gran daño. Por acciones anteriormente mencionadas fue donde se dieron cuenta que desde Buggly se realizaba espionaje a el proceso de paz que se estaba desarrollando con el gobierno de Colombia.

Las investigaciones luego de ser descubierto estos procesos ilícitos, los implicados aceptaron la culpa en donde afirman que si hubo malos manejos y ejecución de procesos que allí se desarrollaban. Se realiza exhaustivamente los procesos de investigación y se determinan las sanciones y penas de acuerdo con lo establecido por la ley colombiana.

3. Etapa 3 Ejecución pruebas de intrusión.

- ✓ Anexo 4 – Escenario 3

Situación problema: Análisis Red team.

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Dentro de la investigación también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

3.1 Herramientas y procedimientos establecidos para dar solución al escenario Red team siguiendo las fases de penetración.

3.1.1 Herramientas software utilizadas.

- **NMAP:** Es una herramienta que se utiliza en múltiples plataformas para realizar exploraciones sobre la red, permitiendo identificar puertos abiertos, los servicios configurados, versión de sistema operativo.
- **NESSUS:** Esta herramienta utiliza procesos de escaneo, búsqueda de algún tipo de vulnerabilidad en la red y sus posibles soluciones; permite emitir resultados en un informe final desde donde se clasifica cada uno de los análisis realizados.
- **MESTASPOLIT:** Herramienta de código abierto y gratuito, permite conocer las debilidades de seguridad en un sistema y también realiza asistencia en las etapas de penetración con el fin de protegerlos.

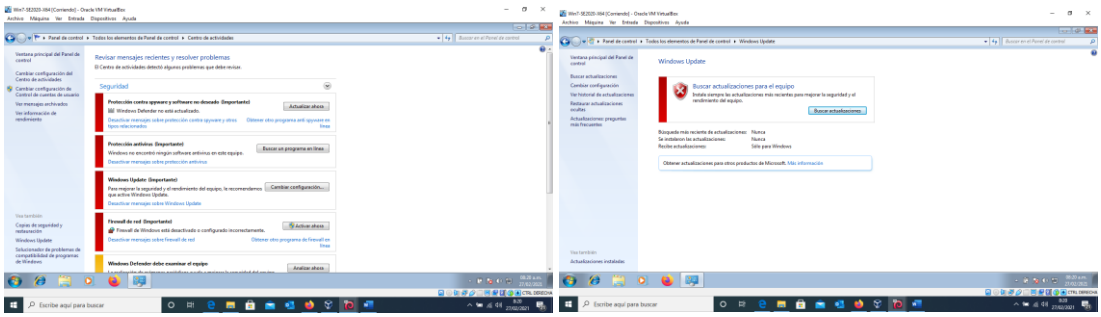
3.1.2 Fase recolección de información.

Para el desarrollo de esta fase, nos dedicamos a recolectar toda la información posible que la empresa tenga disponible identificando los sistemas y programas en funcionamiento que ella tiene. La herramienta que se emplea para recolección de información es NMAP donde me permite identificar puestos abiertos o cerrados dentro del procesos de operación y características propias de cada uno de ellos en servicios.

Además, se procede a desactivar le fireware de Windows para poder lograr las operaciones requeridas para análisis de vulnerabilidades que requiere la empresa y su respectivo análisis de operaciones en el sistema.

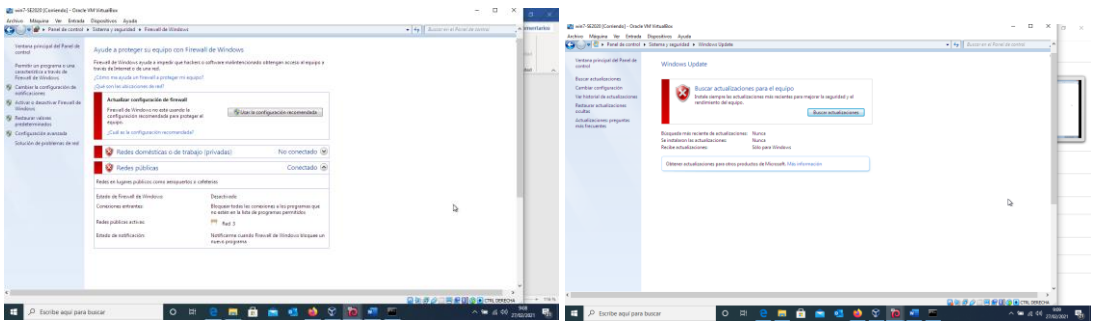
Paso 1: Desactivación de fireware de las maquinas virtuales.

Figura 15 Desactivar fireware y actualizaciones Win 7 x64.



Fuente: Autor

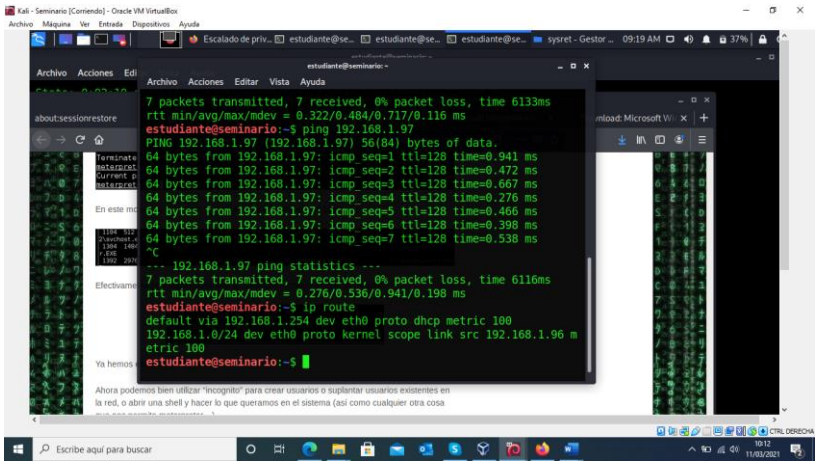
Figura 16 Desactivar fireware y actualizaciones Win 2020 x86.



Fuente: Autor

Paso 2: Identificación de enrutamiento.

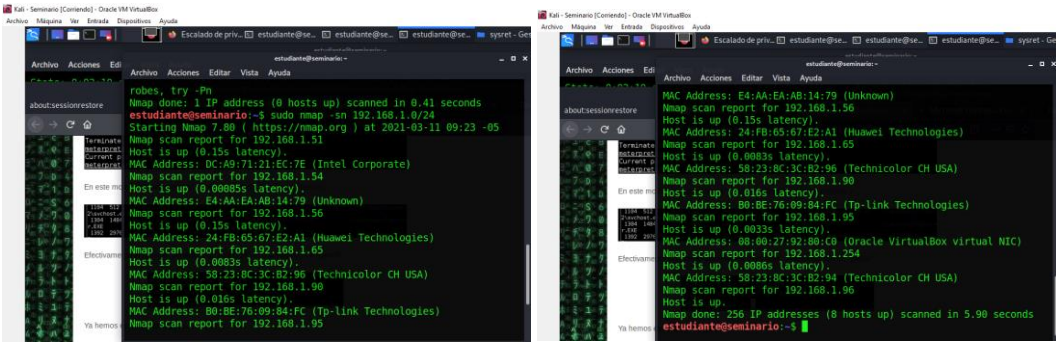
Figura 17 Identificación de enrutamiento.



Fuente: Autor

Paso 3: Que dispositivos están conectados a la red.

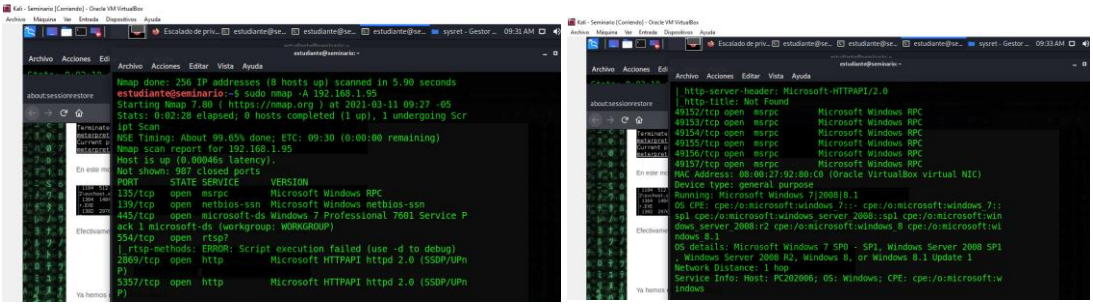
Figura 18 Dispositivos conectados a la red 192.168.1.0



Fuente: Autor

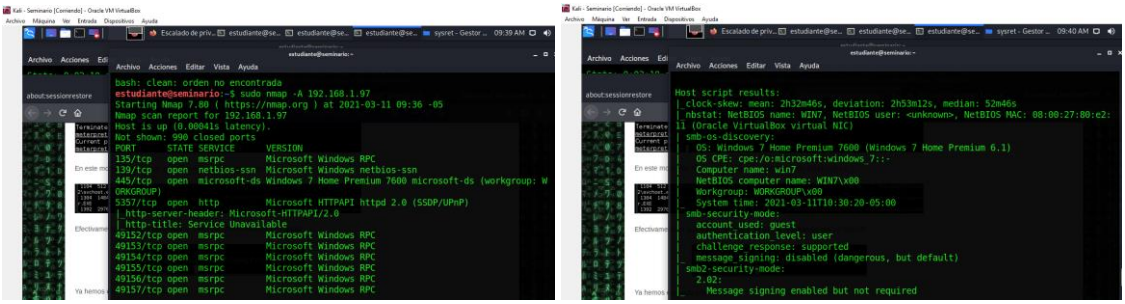
Paso 4: Identificación de puertos y servicios win7 x64.

Figura 19 Análisis de puertos y servicios Win 7 x 64.



Fuente: Autor

Figura 20 Análisis de puertos y servicios Win 7 x 86.



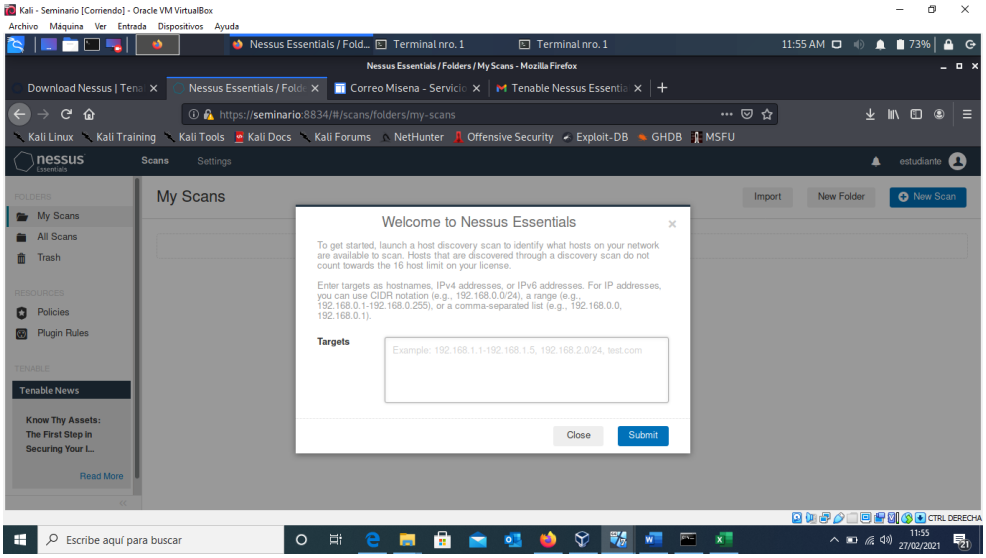
Fuente: Autor

3.1.3 Fase análisis de vulnerabilidad.

En esta fase se valoran los casos exitosos de nuestras estrategias de penetración a través del análisis y proactividad de vulnerabilidades. En este momento es cuando nos damos cuenta de si el proceso de penetración es eficiente y eficaz. Las herramientas que utilizamos para este proceso fue NESSUS – NMAP, las cuales me permiten identificar según el factor de vulnerabilidad las carateristicas de riesgos y estabilidad del sistema:

Paso 1: Entorno analisis de vulnerabilidades NESSUS.

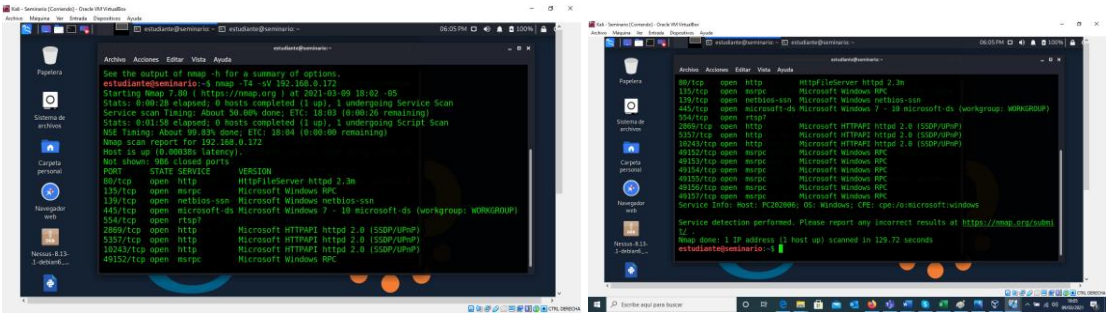
Figura 21 Entorno operación NESSUS.



Fuente: Autor

Paso 2: Nuevamente verificamos puertos y servicios para la utilizar la aplicación en los procesos de análisis de vulnerabilidad.

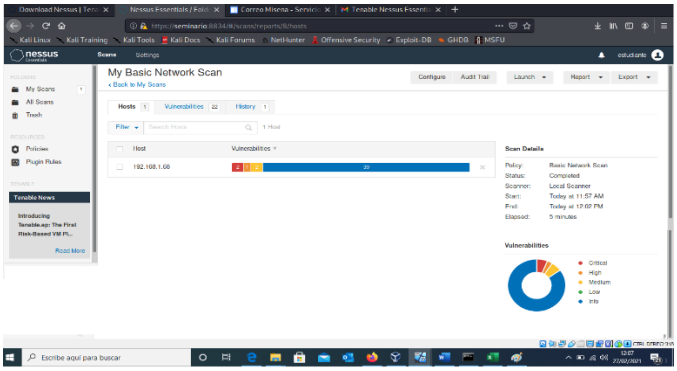
Figura 22 Análisis puertos y servicios.



Fuente: Autor

Paso 3: Ejecución de análisis de NESSUS.

Figura 23 Ejecución de NESSUS.

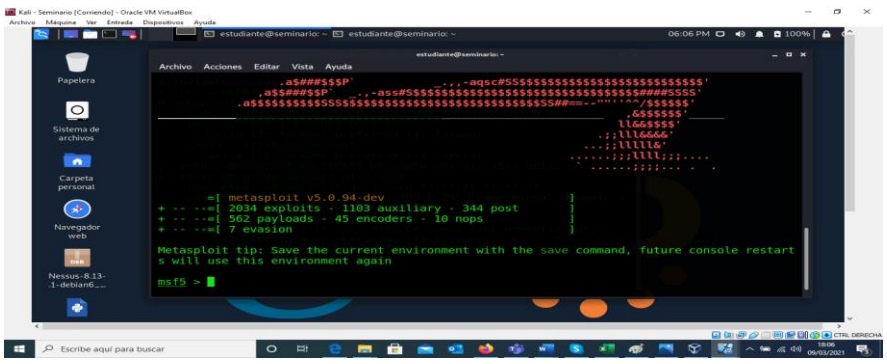


Fuente: Autor

3.1.4 Fase Explotación.

Paso 1: Ingreso desde la consola para realizar el exploit.

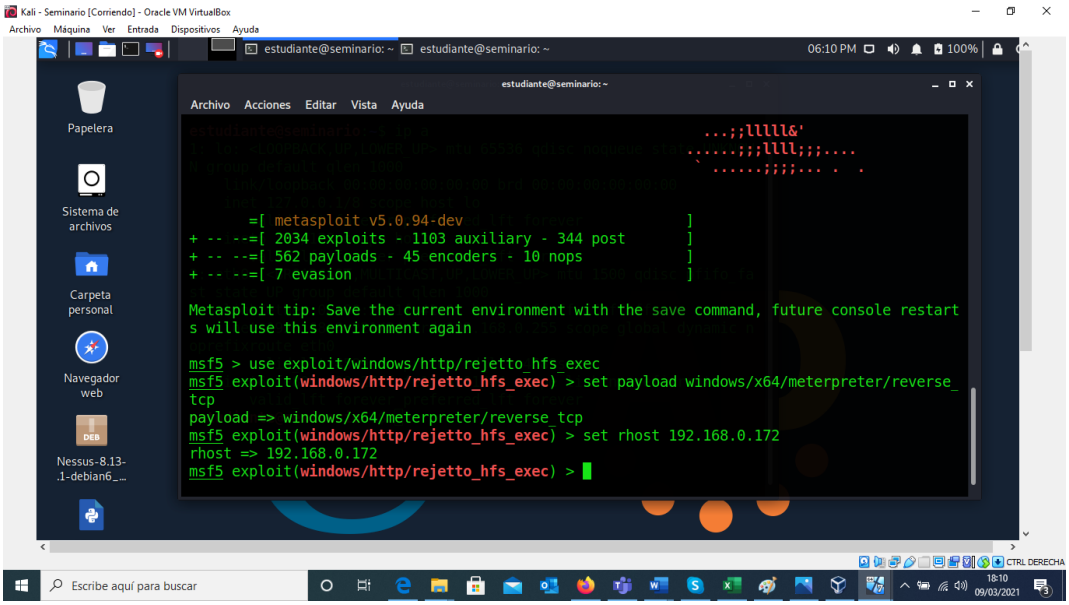
Figura 24 Consola msf exploit.



Fuente: Autor

Paso 2: Usamos el exploit rejetto 2.3, en este caso se procede a setear el payload: windows/x64/meterpreter/reverse_tcp. Posteriormente realizamos el seteo del rhost: 192.168.0.172

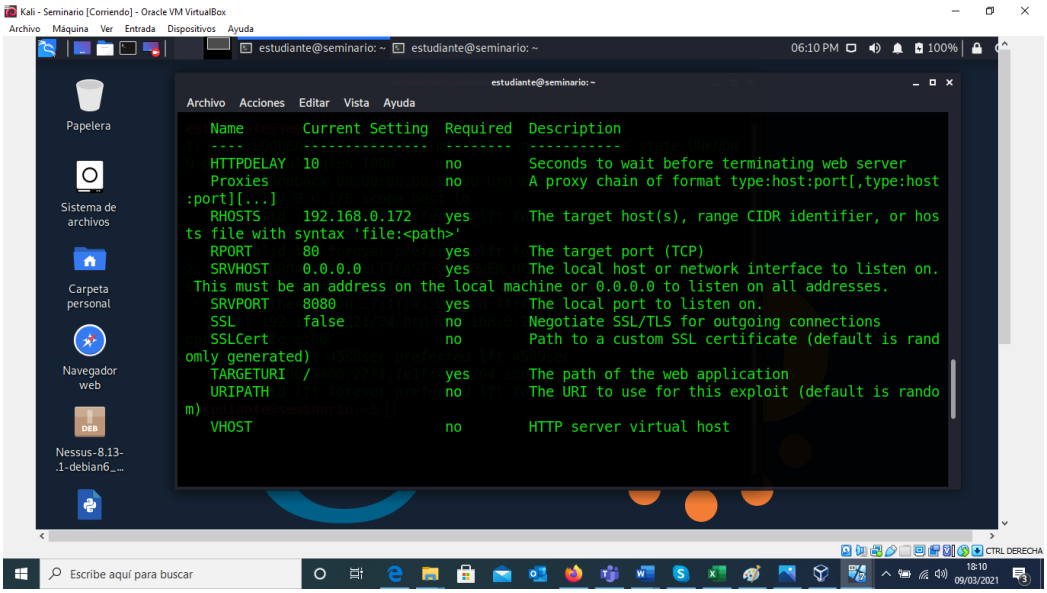
Figura 25 Exploit rejetto 2.3



Fuente: Autor

Paso 3: Verificamos que la configuración del set quedo acorde a lo establecido. Show options.

Figura 26 Estado de configuración SET.



Fuente: Autor

3.1.5 Fase Informe.

En esta fase final se hace entrega de la información relacionada con el análisis de vulnerabilidades caracterizadas en la prueba de penetración. Se identifica los puntos concretos en donde la seguridad se ha puesto de manera correcta y aquellos donde debe existir una corrección en la seguridad del sistema de información.

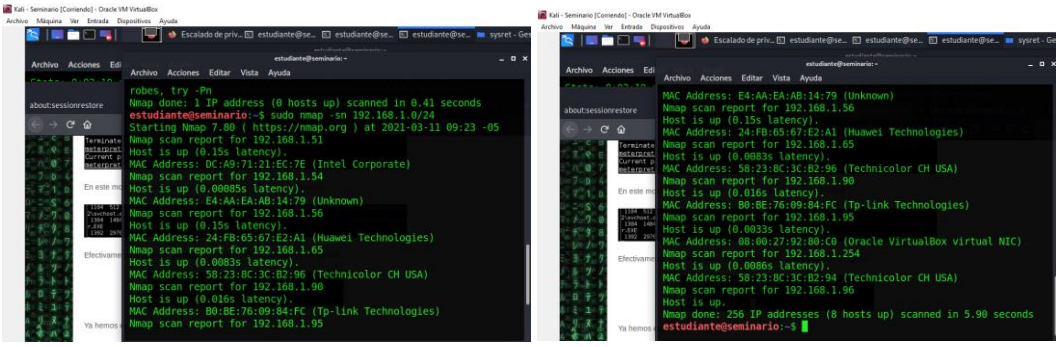
3.2 Análisis caso Red team – Identificación de fallos.

3.2.1 Caracterización de la información suministrada por el caso Red team.

a. Se identifica una aplicación llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64 en uno de los equipos de cómputo de la organización.
b. Se presenta un caso asociado a un exploit que puede ejecutar un Shell reversa.
c. Analizar la posibilidad de una sesión abierta de meterpreter.
d. Se identifica un escalamiento de privilegios, permite la creación de un usuario tipo administrador del sistema.

Paso 1: Identificamos los equipos que están conectados a la red.

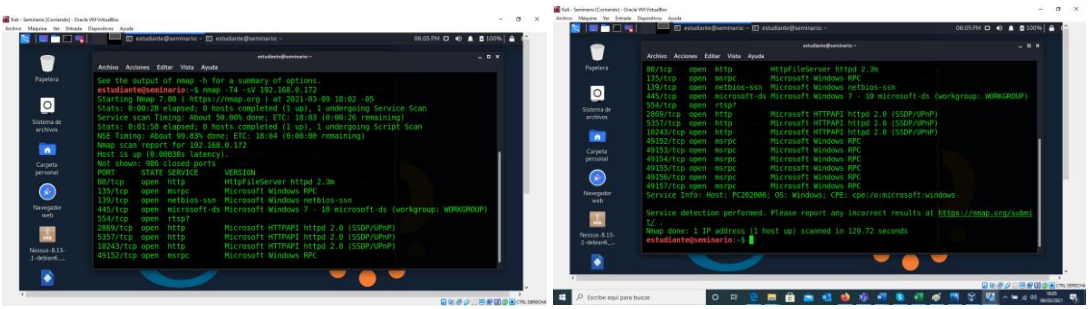
Figura 27 Identificación equipos conectados a la red.



Fuente: Autor

Paso 2: Realizamos escaneo al sistema operativo y servicios vinculados.

Figura 28 Escaneo de puertos y servicios.

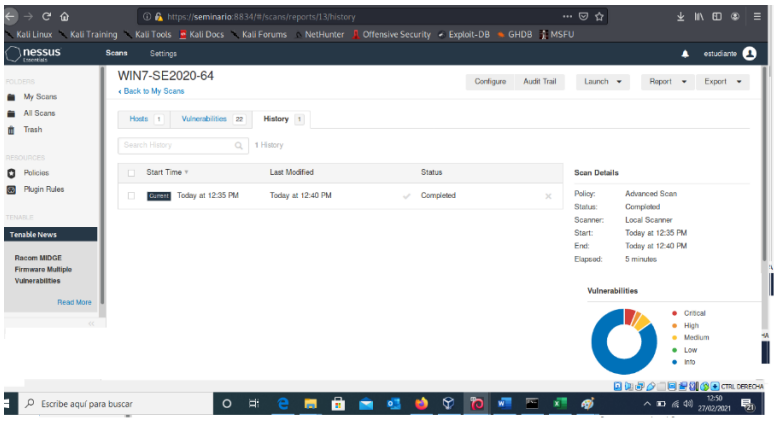


Fuente: Autor

3.3 Herramientas empleadas para identificación de fallos en la seguridad propuesto por el escenario Red team.

Paso 1: Análisis de vulnerabilidades NESSUS.

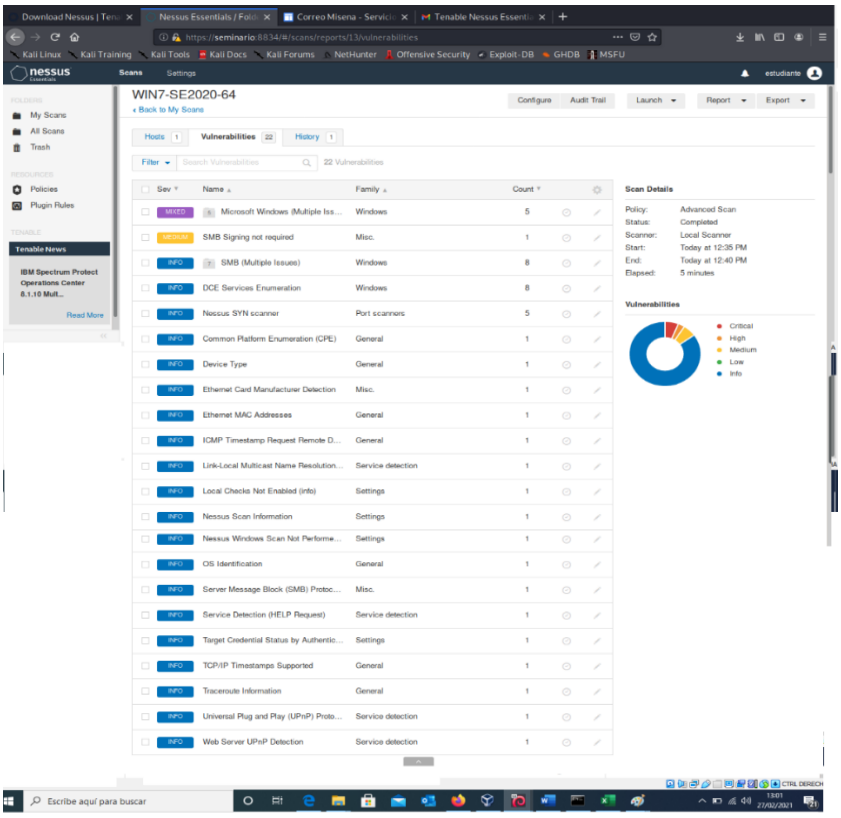
Figura 29 Entorno NESSUS.



Fuente: Autor

Paso 2: Caracterizar las vulnerabilidades encontradas en el proceso.

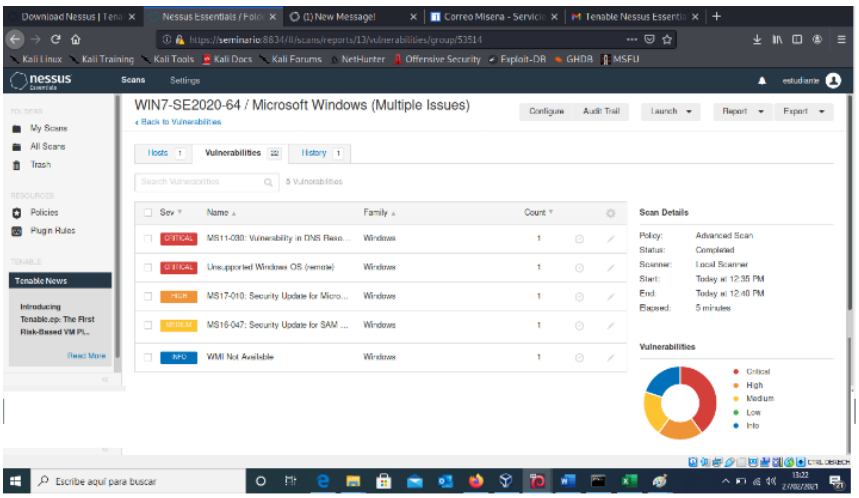
Figura 30 Caracterización de Vulnerabilidades.



Fuente: Autor

Paso 3: Vulnerabilidades críticas para tener encuenta en el proceso de exploit.

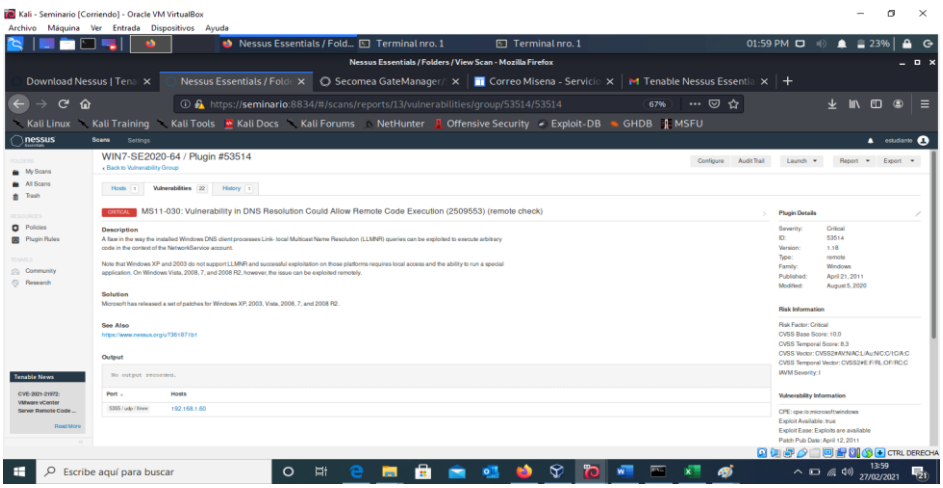
Figura 31 Vulnerabilidades identificadas.



Fuente: Autor

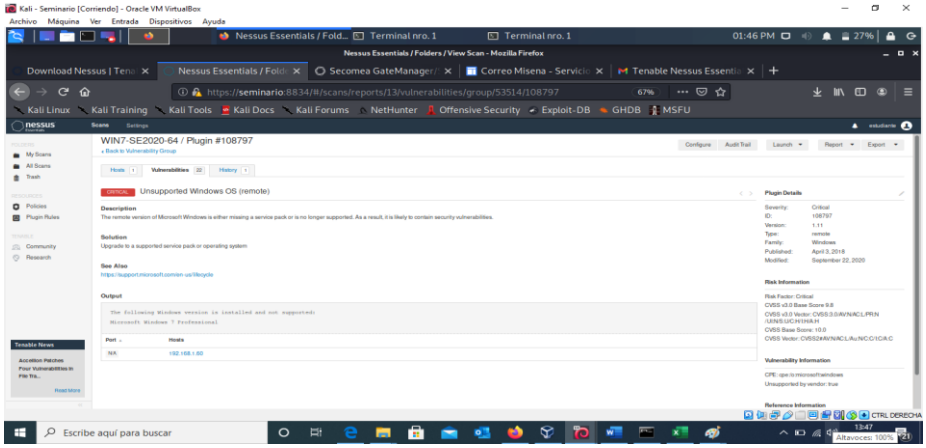
Paso 4: Análisis y caracterización de cada una de las vulnerabilidades encontradas.

Figura 32 Vulnerabilidad MS11-030.



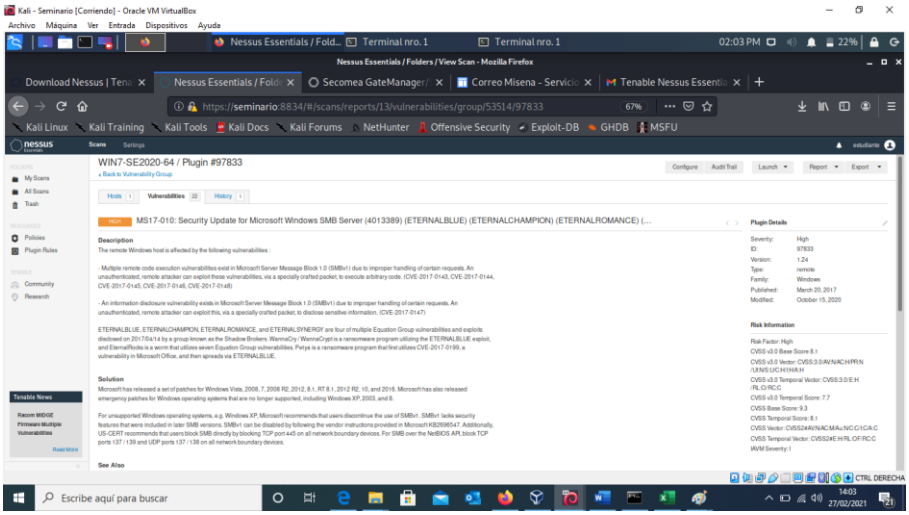
Fuente: Autor

Figura 33 Vulnerabilidad UNSUPPORTED WINDOWS OS (REMOTE).



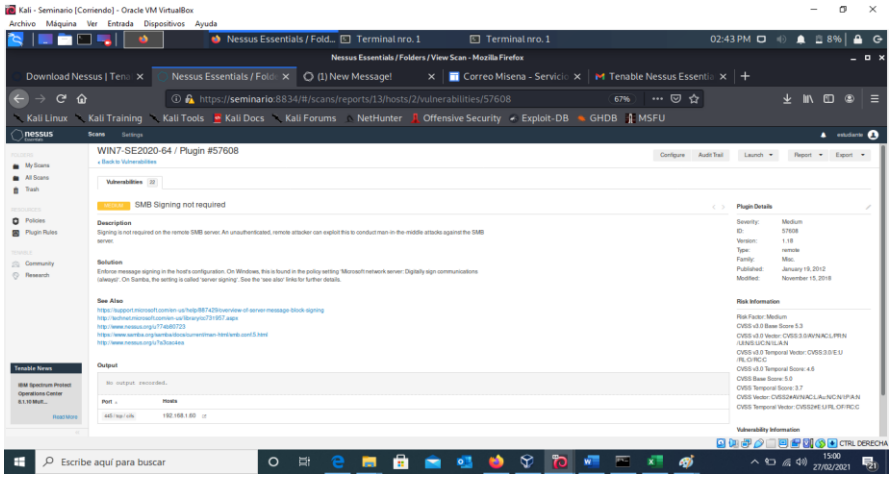
Fuente: Autor

Figura 34 Vulnerabilidad MS17-010.



Fuente: Autor

Figura 35 Vulnerabilidad MS16-047.



Fuente: Autor

Caracterización de los procesos anteriormente mecionados:

- MS11-030 (critical): Idéntica las fallas en la característica de forma del DNS de windows, permite realizar las consultas de resolución de nombres de multidifusión del enlace, los cuales se pueden aprovechar para ejecutar códigos arbitrarios en contextos de cuentas NetworkService.

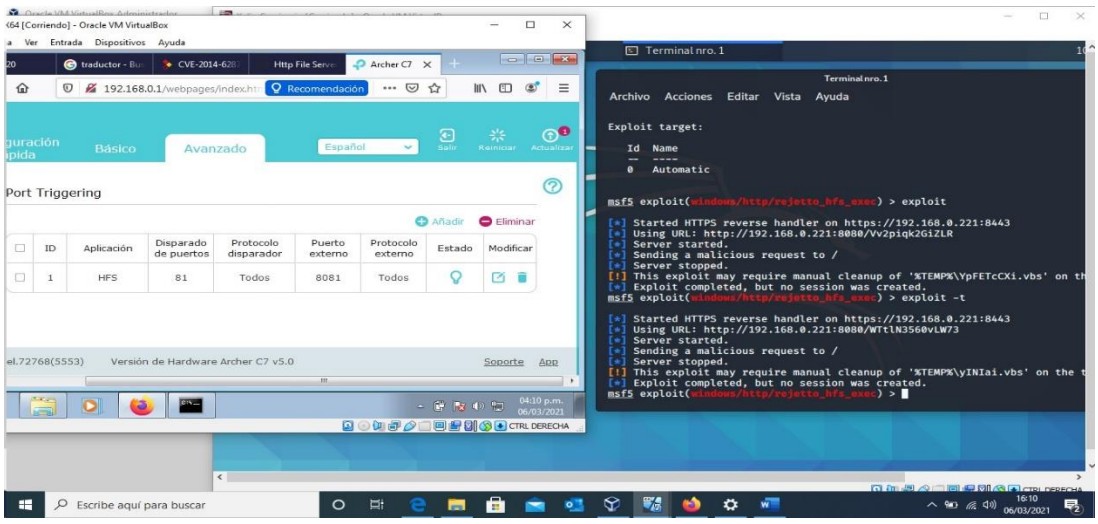
- UNSUPPORTED WINDOWS OS (REMOTE) (critical): Es una versión remota de Windows que permite identificar procesos de vulnerabilidades y su respectiva seguridad según procesos de intrusión y ruptura del código de seguridad

- MS17-010 (high): Diseñado para ejecutar códigos arbitrarios a partir de una ejecución remota de códigos de Microsoft Server Menssage Block, esto analiza los procesos inadecuados en ciertas solicitudes, pueden ser vulnerables al proceso de atacantes remotos no autenticados.

- MS16-047 (Medium): Permite identificar procesos de vulnerabilidad remota de elevación en los privilegios de protocolos del administrador de cuenta de seguridad, debido a una falla en la negociación en el nivel de autenticación en los canales de llamadas en procedimiento remoto; puede lograr una degradación en el nivel de autenticación.

Nota: se realiza cambion de router para poder identificar error en ejecucion de rejetto. Red 192.168.0.0

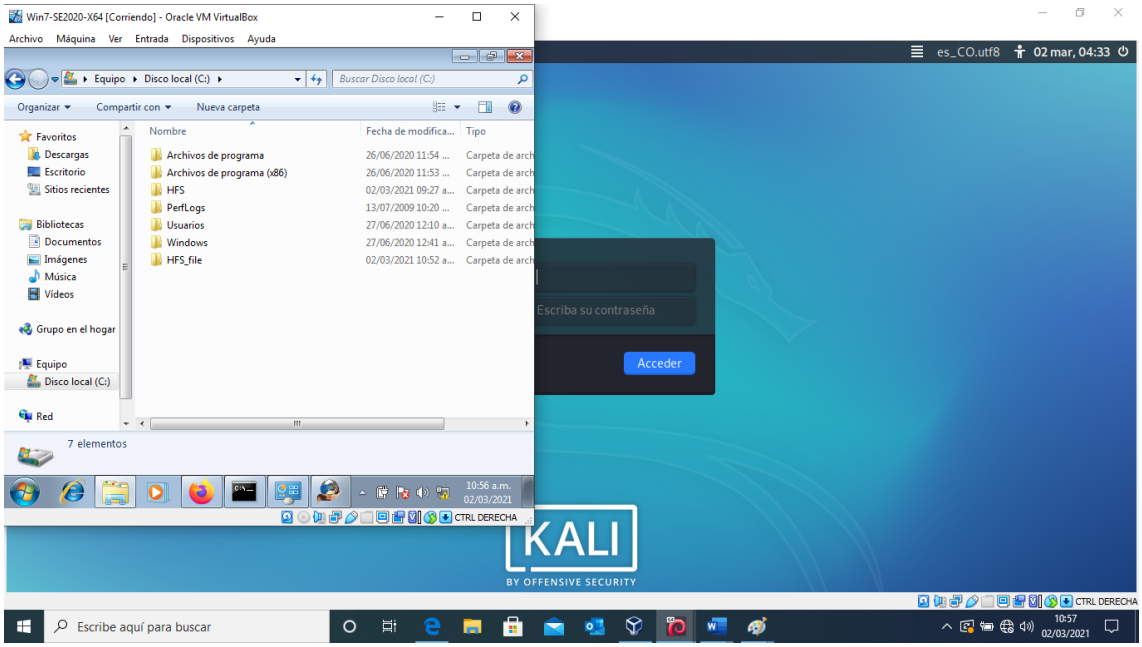
Figura 36 Cambio de Router.



Fuente: Autor

Paso 5: Instalación HFS maquina win 7 x 64.

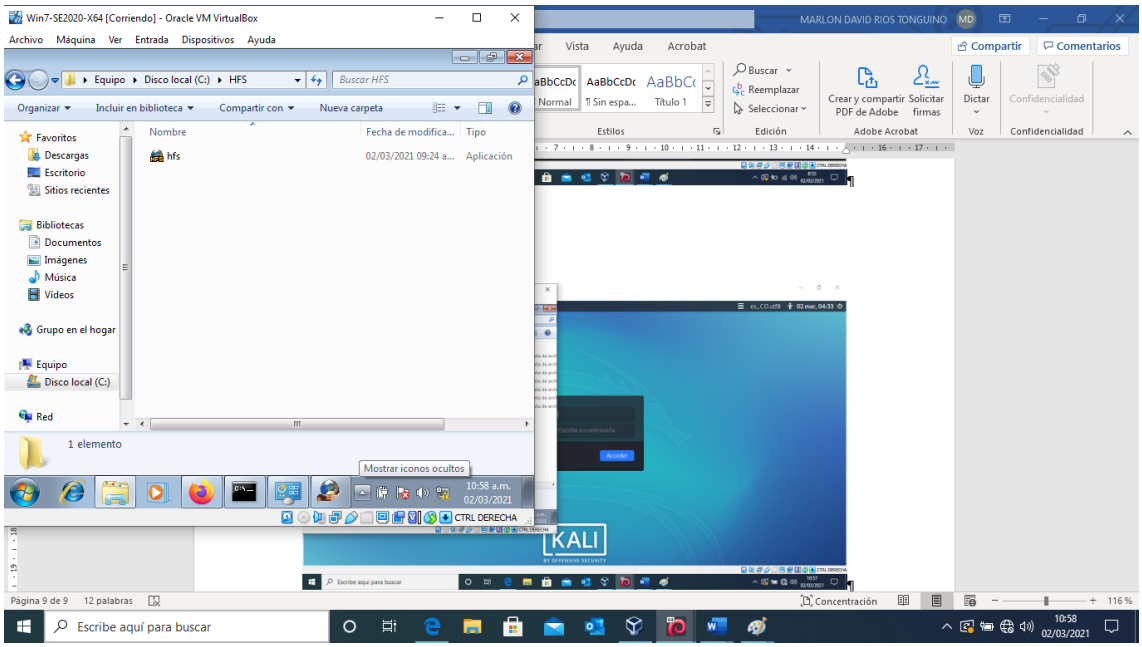
Figura 37 Instalación HFS.



Fuente: Autor

Paso 6: Ejecución programa HFS.

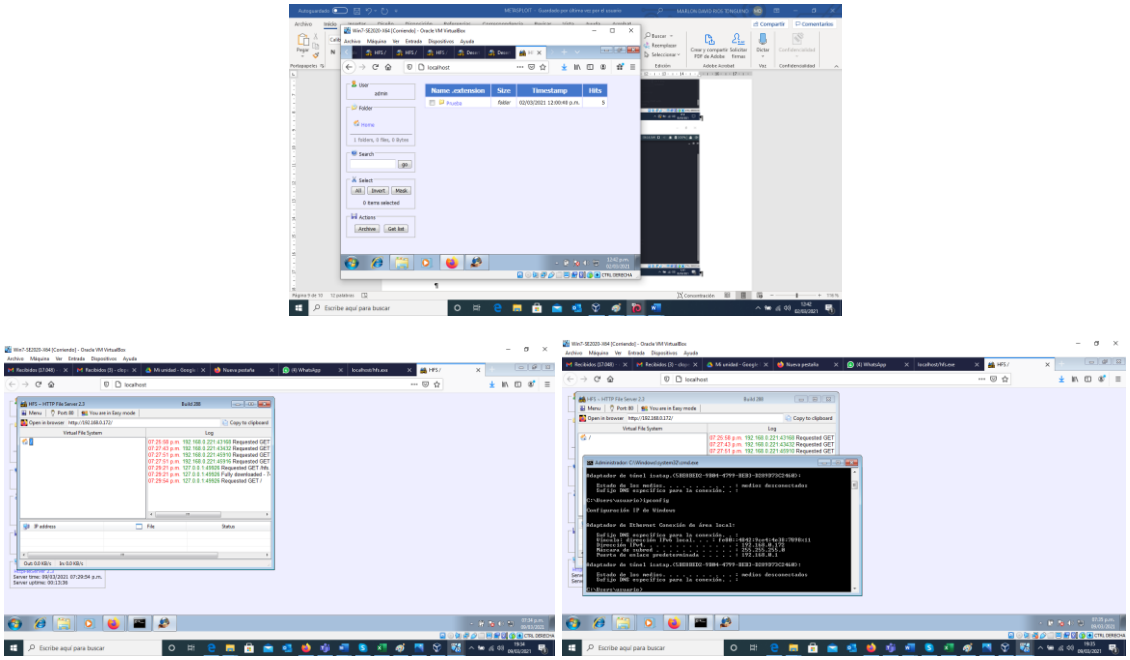
Figura 38 Ubicación HFS.



Fuente: Autor

Paso 7: Identificamos procesos de ejecución HFS en la maquina win 7 x 64.

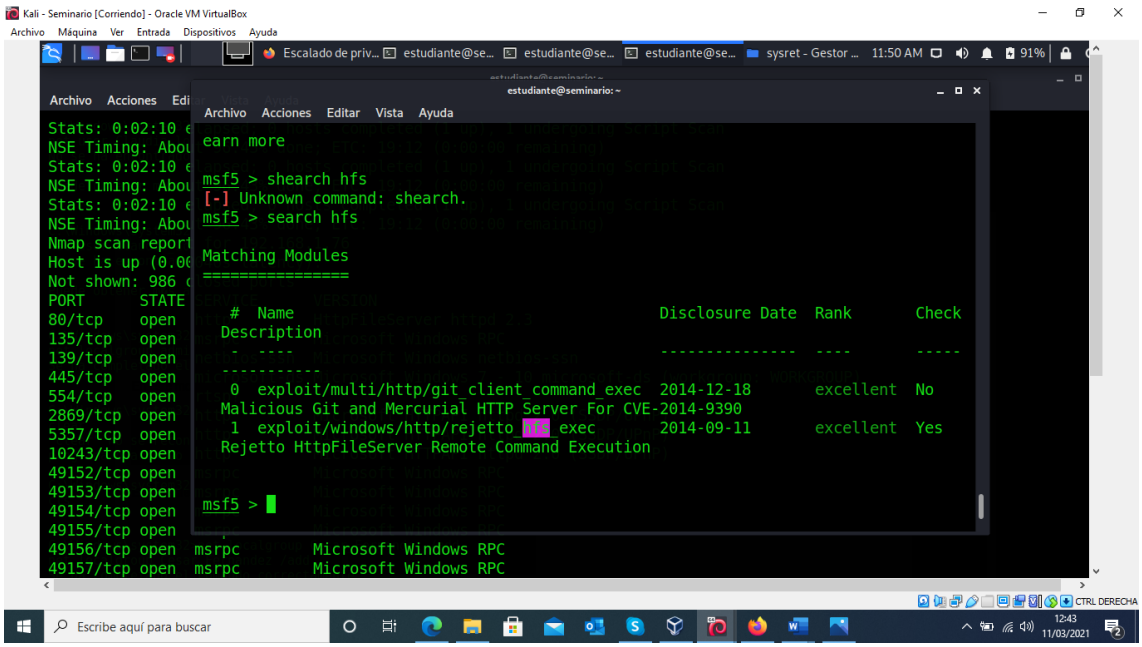
Figura 39 Procesos ejecutados HFS.



Fuente: Autor

Paso 8: Realizamos la búsqueda HFS. Search HFS.

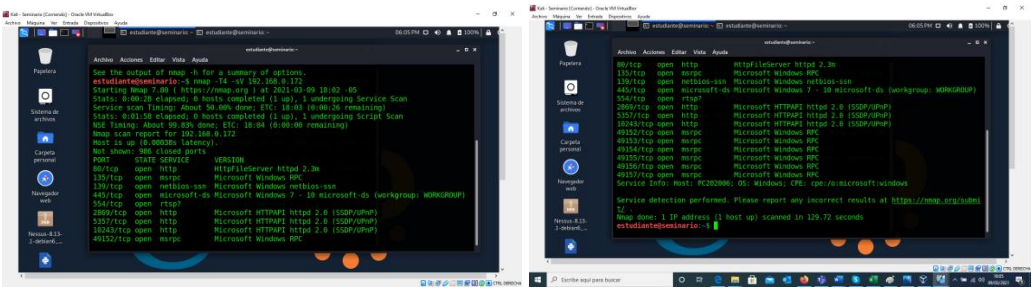
Figura 40 Búsqueda de HFS.



Fuente: Autor

Paso 9: Identificamos puertos para utilizar la herramienta rejetto.

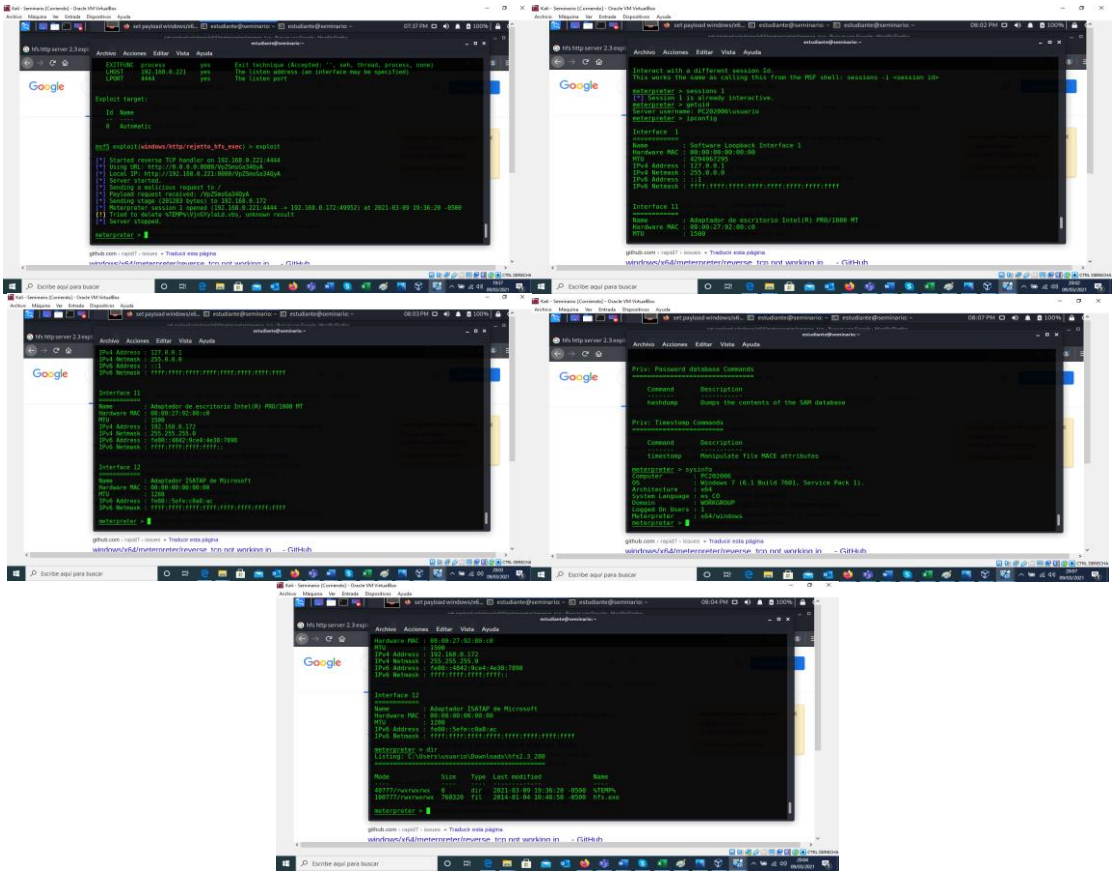
Figura 41 Identificación puertos.



Fuente: Autor

Paso 10: Realizamos el proceso de exploit con rejetto.

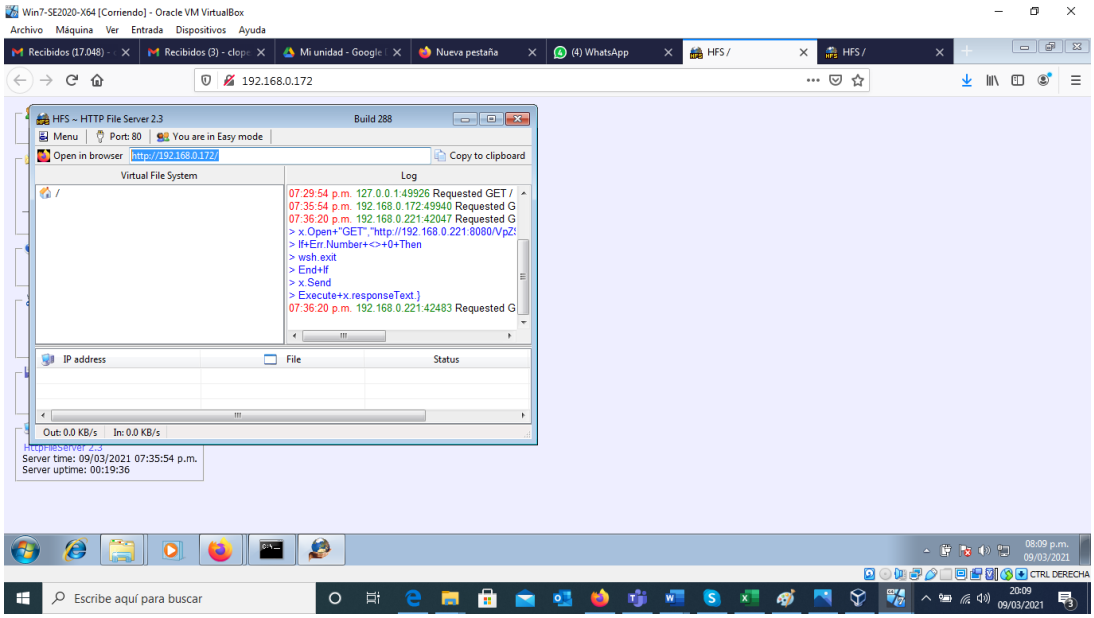
Figura 42 Proceso ejecutado rejetto.



Fuente: Autor

Paso 11: Ejecución proceso en análisis con rejetto 2.3.

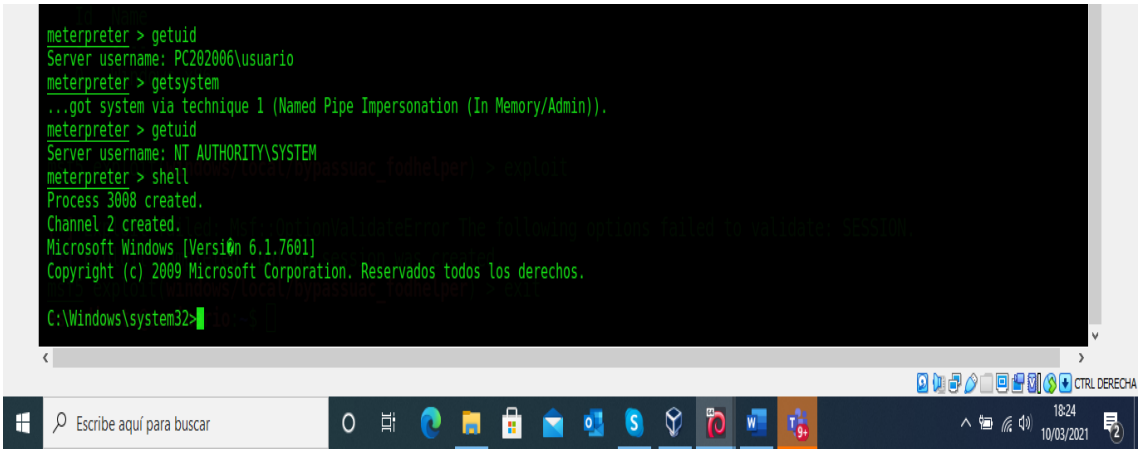
Figura 43 Ejecución HFS y rejetto.



Fuente: Autor

Paso 12: Ingresamos al Shell.

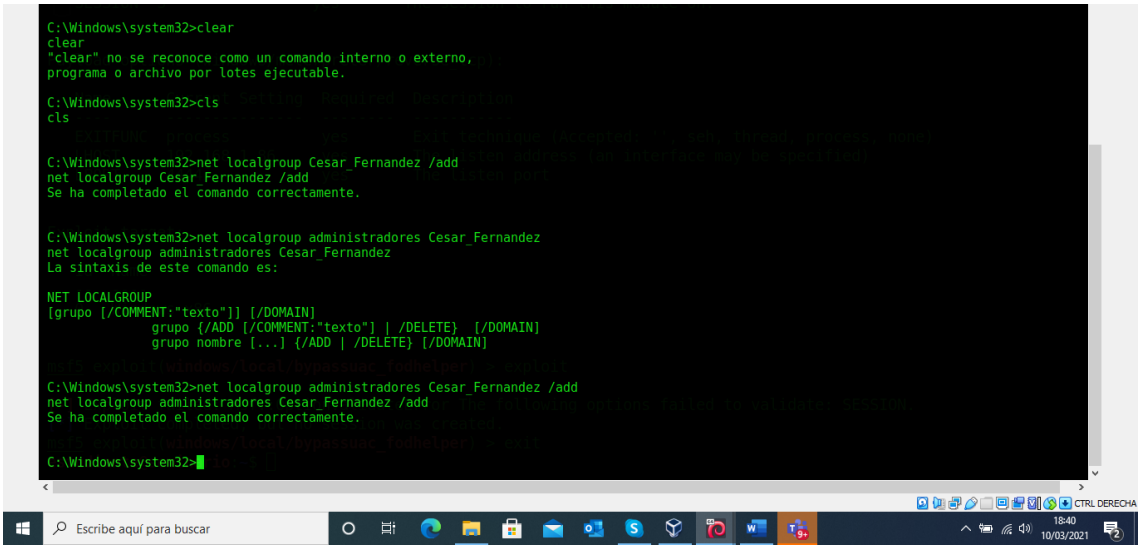
Figura 44 SHELL.



Fuente: Autor

Paso 13: Se crea el usuario y se vuelve administrador (Cesar Fernandez)

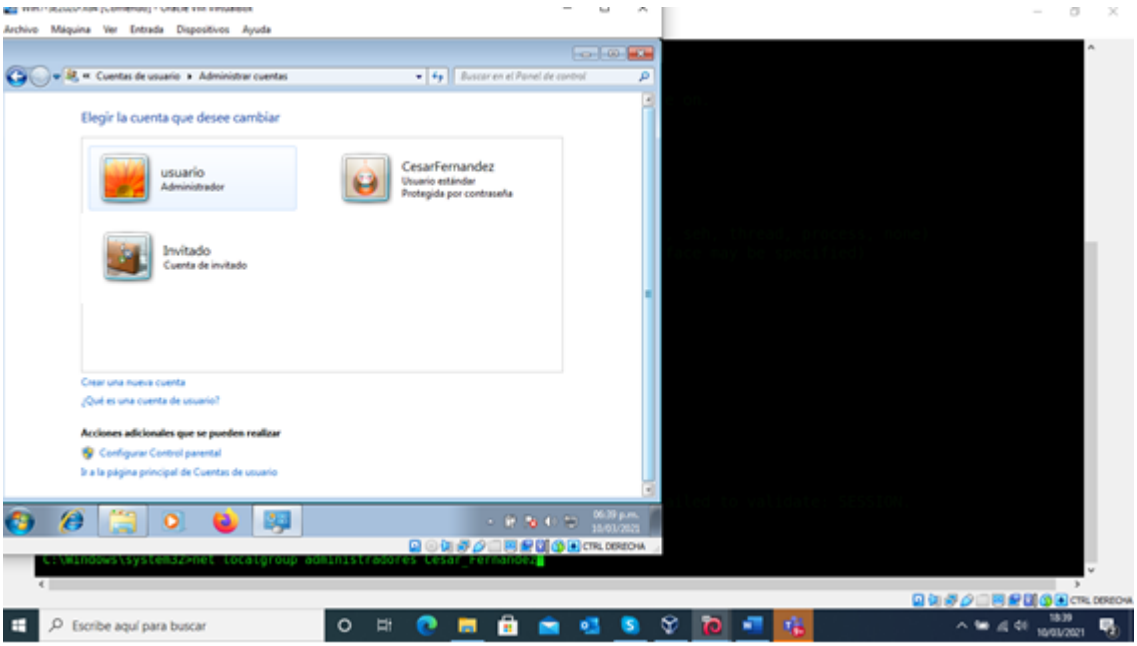
Figura 45 Creación del usuario.



Fuente: Autor

Paso 14: Entono gráfico de la creación del usuario administrador.

Figura 46 Entorno Usuario Administrador.



Fuente: Autor

3.4 Explicación específica del ataque realizado a la maquina (Windows 7 X64).

Con la utilización de las diferentes pruebas de penetración, se logró identificar las debilidades que cuenta el sistema informático, las deficiencias de programas para su seguridad y procesos de vulnerabilidades; lo anterior permite simular ataques que son comúnmente utilizados en alguna organización. Es importante identificar que en Windows las vulnerabilidades son fácilmente explotada por sus puertos, permitiendo utilizar exploit y payload para conseguir un Shell remoto tan solo conociendo su dirección IP.

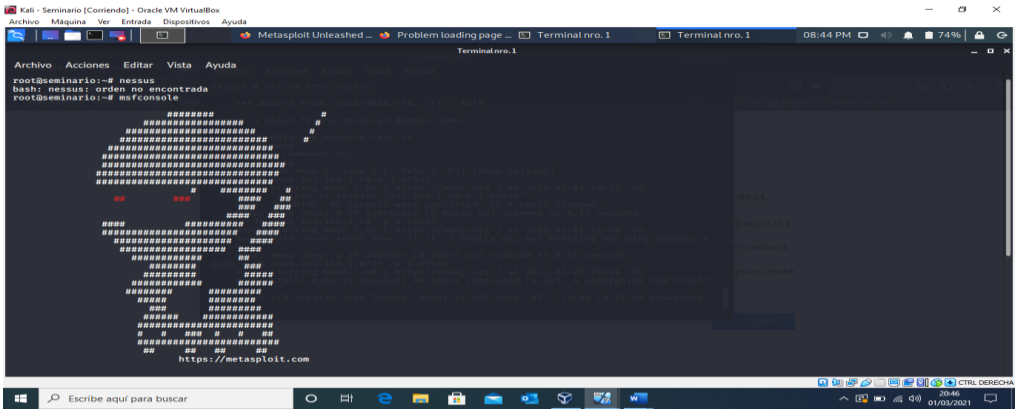
Para realizar el ataque utilizaremos un metasploit, que proporciona una infraestructura que permite automatizar tareas de rutina y complejas, lo cual permite identificar fallas en una organización. Cuando ingresamos en modo consola del metasploit, nos permite ejecutar exploits que, en su manejo de bases de datos, la cual contiene todos los exploits permitidos para identificar cada una de las vulnerabilidades encontradas.

Paso 1: Identificación de comandos para ejecutar en el Metasploit.

Comandos	Descripción
msfconsole	Inicio al Metasploit Framework
exploit	Lanzar ataque, me permitirá tomar ventaja de las fallas en el sistema, aplicación y/o servicio
payload	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 del administrador
pwd	Muestra en que parte me encuentro
ps	Muestra los procesos del sistema

Paso 2: Ingreso al Metasplot framework.

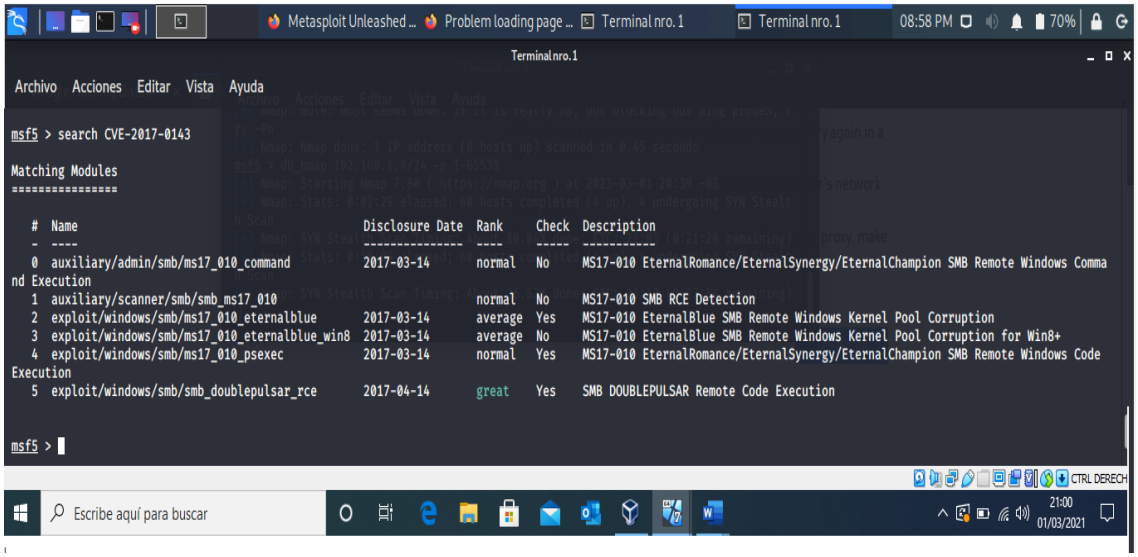
Figura 47 Ingreso Metasplot Framework.



Fuente: Autor

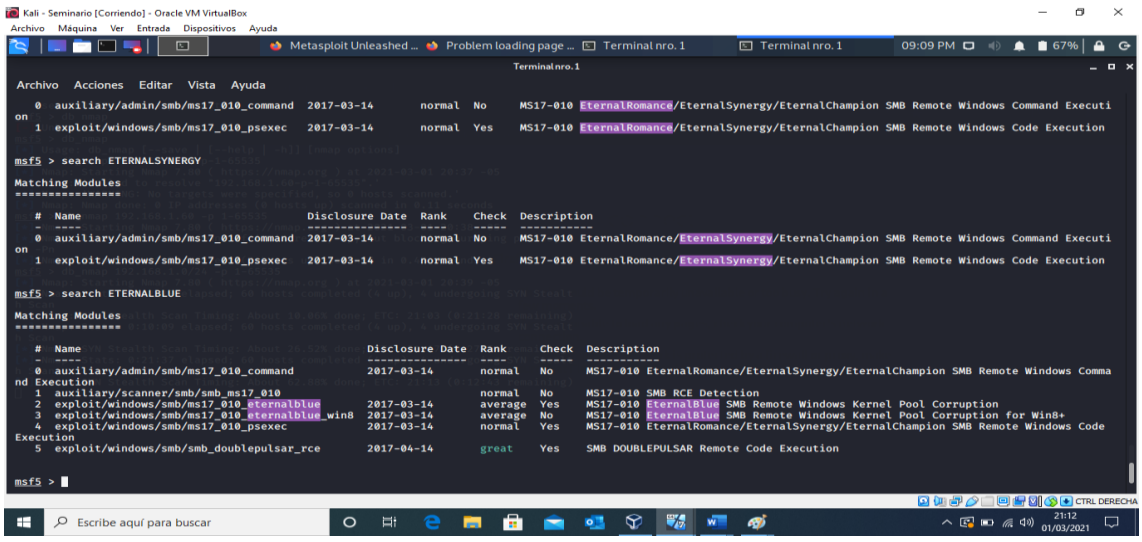
Paso 3: Aplicamos buscador.

Figura 48 Buscador Metasploit.



Fuente: Autor

Figura 49 Buscador Metasploit.



Fuente: Autor

4. Etapa 4 Contención de ataques informáticos.

✓ Anexo 5 – Escenario 4

Situación problema: Análisis Blue team.

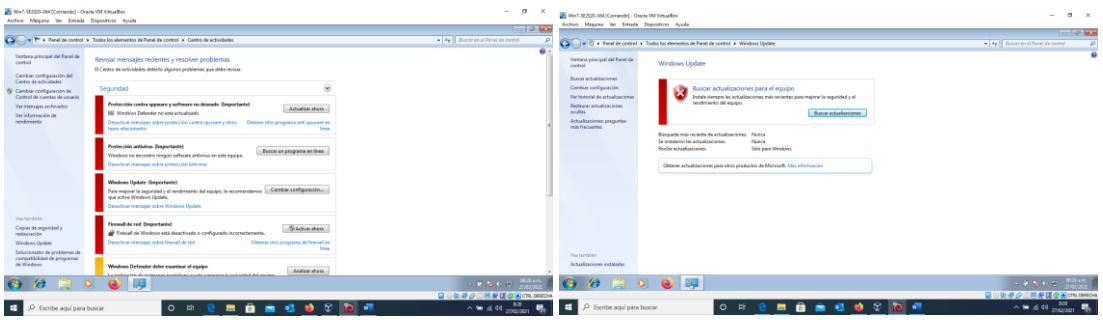
WhiteHouse Security solicita a sus integrantes de Blue team contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

4.1 Acciones propuestas para contener un ataque en tiempo real.

Para poder realizar una contención de un ataque que se está realizando en tiempo real tendría en cuenta los siguientes pasos:

Paso 1: Identificamos el estado del fireware del sistema operativo Win 7 x64.

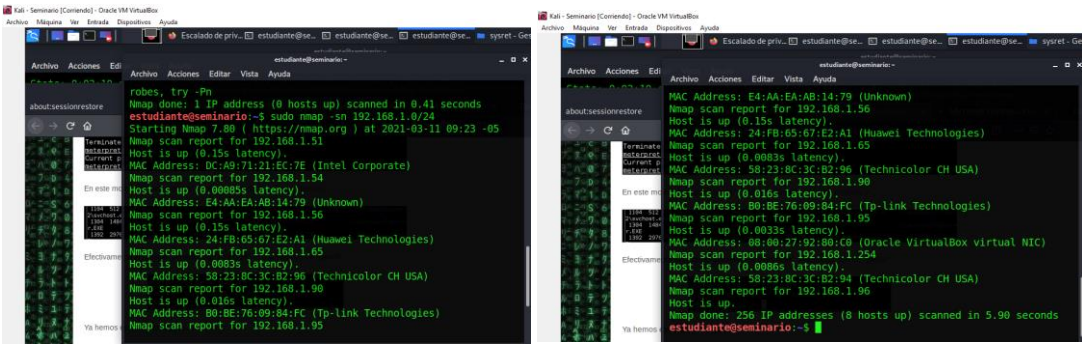
Figura 50 Desactivado fireware y actualizaciones Win 7 x64.



Fuente: Autor

Paso 2: Que dispositivos están conectados a la red.

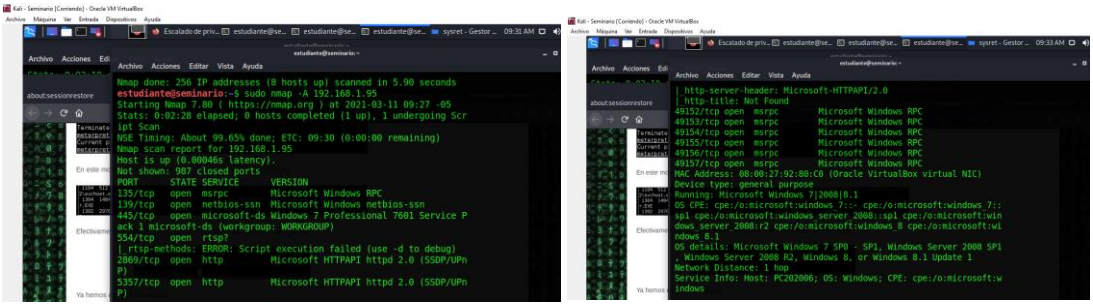
Figura 51 Dispositivos conectados a la red 192.168.1.0



Fuente: Autor

Paso 3: Identificación de puertos y servicios win7 x64.

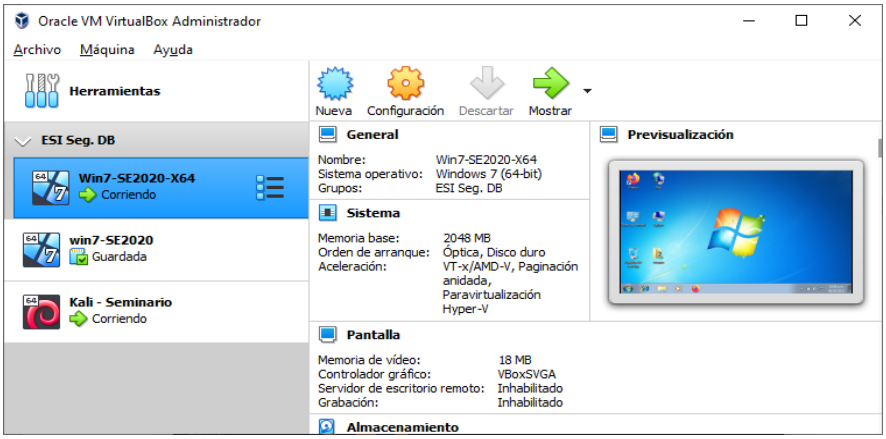
Figura 52 Análisis de puertos y servicios Win 7 x 64.



Fuente: Autor

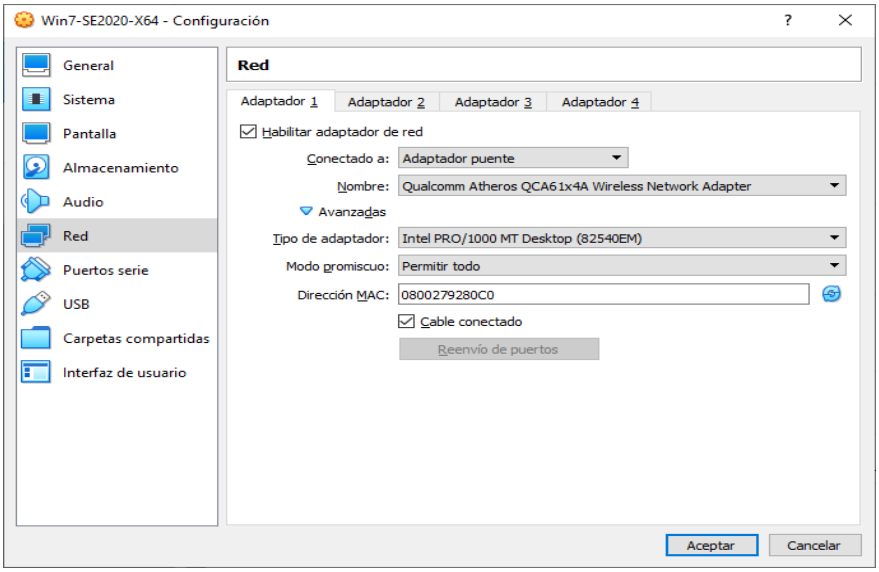
Paso 4: Identificamos configuración de la “RED”.

Figura 53 Entorno configuración máquina virtual Win 7 x64.



Fuente: Autor

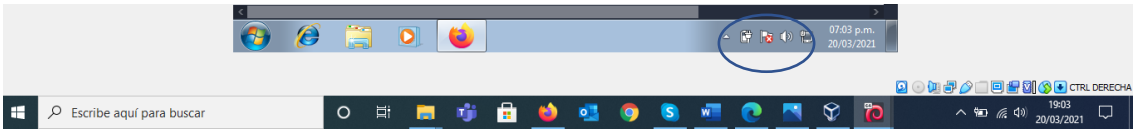
Figura 54 Configuración modo puente – permitir todo.



Fuente: Autor

Paso 5: Identificamos que no cuenta con un antivirus instalado.

Figura 55 No tiene antivirus instalado.



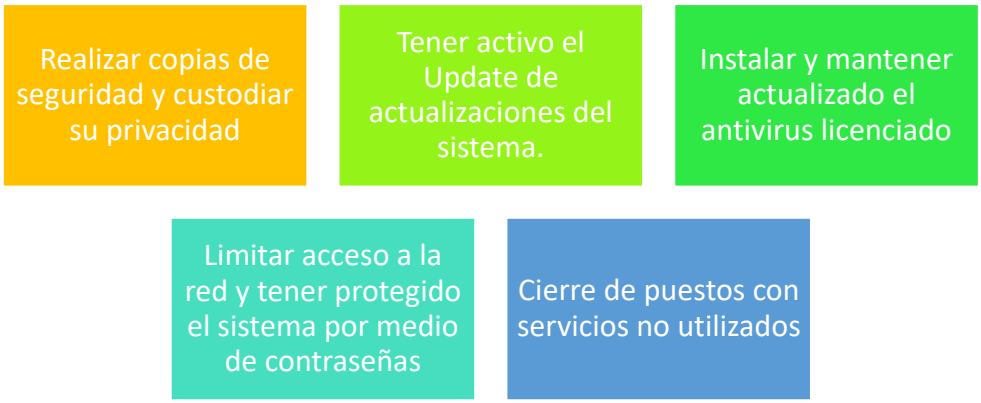
Fuente: Autor

Posteriormente al haber realizado este proceso técnico que permitió identificar los procesos hardware y software que se están ejecutando el equipo que está siendo atacado, se procede a realizar ordenadamente el proceso de prevención, Detección, Recuperación y respuesta de evaluación.

4.1.1 Proceso de prevención.

En esta acción nos permite realizar acciones con metodología preventiva, en donde logramos reunir la gran mayoría de información, identificar los procesos de comunicación y lograr indagar y educar al usuario sobre los procesos de prevención. Para lo anterior podremos tener en cuenta las siguientes medidas:

Figura 56 Medidas de Prevención.

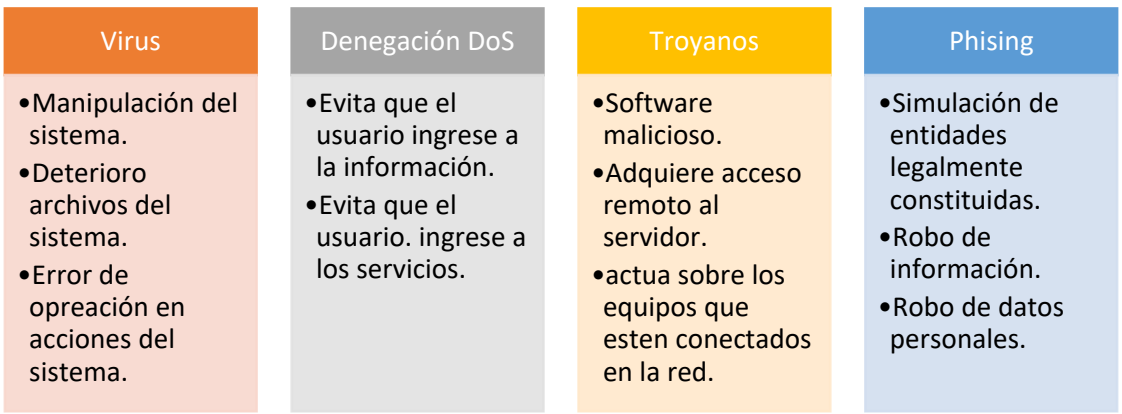


Fuente: Autor

4.1.2 Proceso de detección.

Para realizar el proceso de detección se debe tener muy en cuenta el tipo de ataque que se está realizando. Con lo anterior me permite identificar el alcance y posibilidad de daño que se esté ejecutando en la información del equipo; se debe realizar monitoreo e incluir las partes responsables que desarrollaron labores sobre el equipo, identificar el personal involucrado para realizar preguntas relacionadas con la actividad que desarrollan y con ellos lograr la recuperación en detalle de los datos e información en análisis. A continuación, se mostrarán ataques muy comunes:

Figura 57 Tipos de Ataques.



Fuente: Autor

4.1.3 Proceso recuperación.

Se puede estructurar en este paso de recuperación, 3 fases importantes que me permiten garantizar el desarrollo de rescate del sistema organizacional.

En una primera fase se busca mitigar las respectivas consecuencias del ataque, empleando algún tipo de herramienta de contención que sea idónea para el proceso ejecutado, y que permita limitar el impacto e incidencias del ataque.

La segunda fase es emplear medidas que logren detener el ataque, permitiendo remover cualquier tipo de amenaza, generando planes de contingencia donde se recupere desde el robo de información, bloqueo de cuentas, entre otros.

Y por último la tercera fase es retomar la normalidad en el funcionamiento, estructurando los nuevos planes desde las experiencias vividas del ataque, teniendo como objetivo primordial crear sistemas de backups y copias de seguridad según corresponda.

4.1.4 Proceso de respuesta.

Como último paso del desarrollo del proceso es dar a conocer la respectiva información de los acontecido a cada uno de los interesados de la empresa, entre ellos podemos tener:

- Clientes
- Trabajadores
- Jefes
- Gerentes

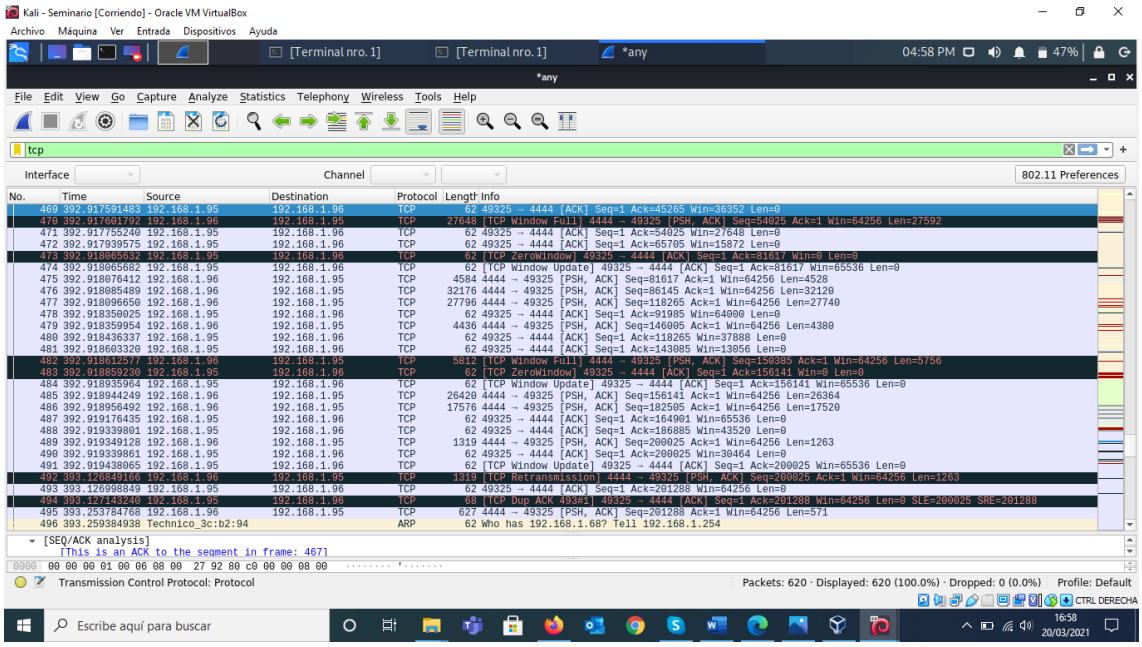
Esto con el fin de dar a conocer cuáles son las consecuencias del ataque que se realizó, las medidas que se adoptan para poder continuar con los procesos que se desarrollan en la organización y una sala de preguntas para poder responder a las personas que generen alguna duda con respecto al proceso desarrollado o consecuencias futuras.

4.2 Acciones de Hardenización a implementar para minimizar o mitigar ataques de seguridad informática.

Para el proceso de hardenización que permite asegurar el sistema informático minimizando las vulnerabilidades encontradas, logrando así endurecer los procesos de seguridad en servicios, usuarios y funciones que se ejecuten en la organización. Para lo anterior se desarrollaron los siguientes pasos de corrección:

Paso 1: Realizamos el sistema de monitoreo con la herramienta Wireshark, permitiendo identificar el estado de la red, si se observa algún tipo de riesgo de ataque.

Figura 58 Análisis red con Wireshark.



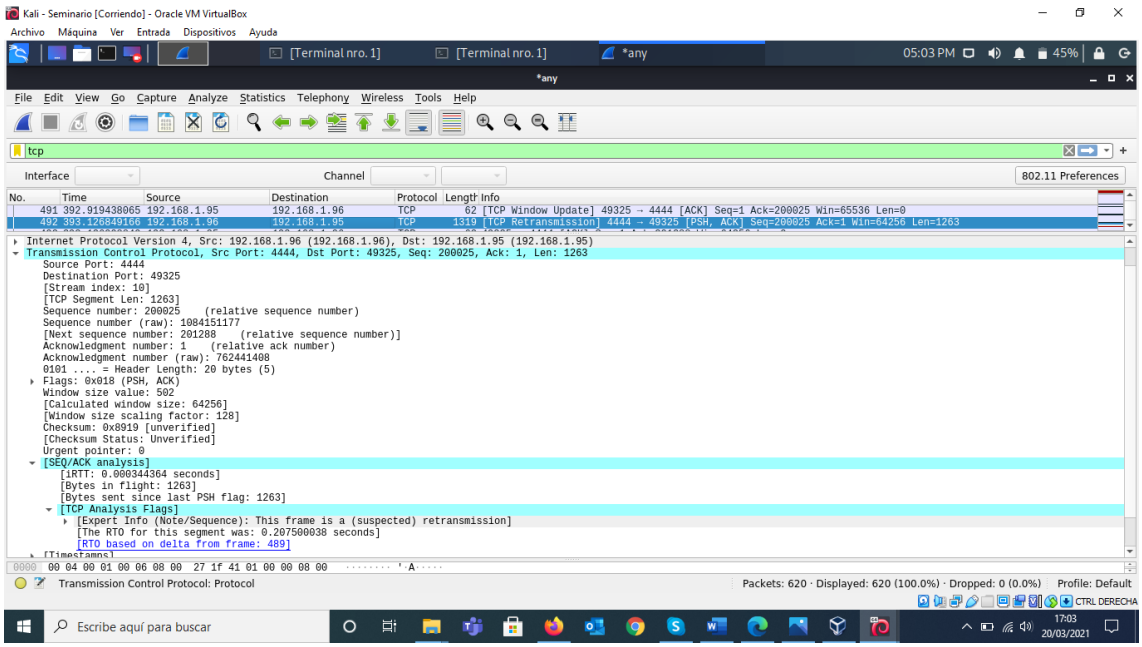
Fuente: Autor

Paso 2: Identificación de los colores que emplea la herramienta de Wireshark para análisis de la red.

- Rojo: Problema serio. En el paquete aparecerá la palabra "Error".
- Amarillo: Indica atención. En el paquete se podrá ver la palabra "Warn".
- Celeste: Situaciones destacables fuera del funcionamiento normal. En el paquete aparecerá la palabra "Note".
- Gris: Información sobre flujos normales que ayuda a entender qué ha ocurrido. En el paquete aparecerá la palabra "Note".

Paso 3: Toma de muestra del análisis de la información en la red y su contexto explicativo.

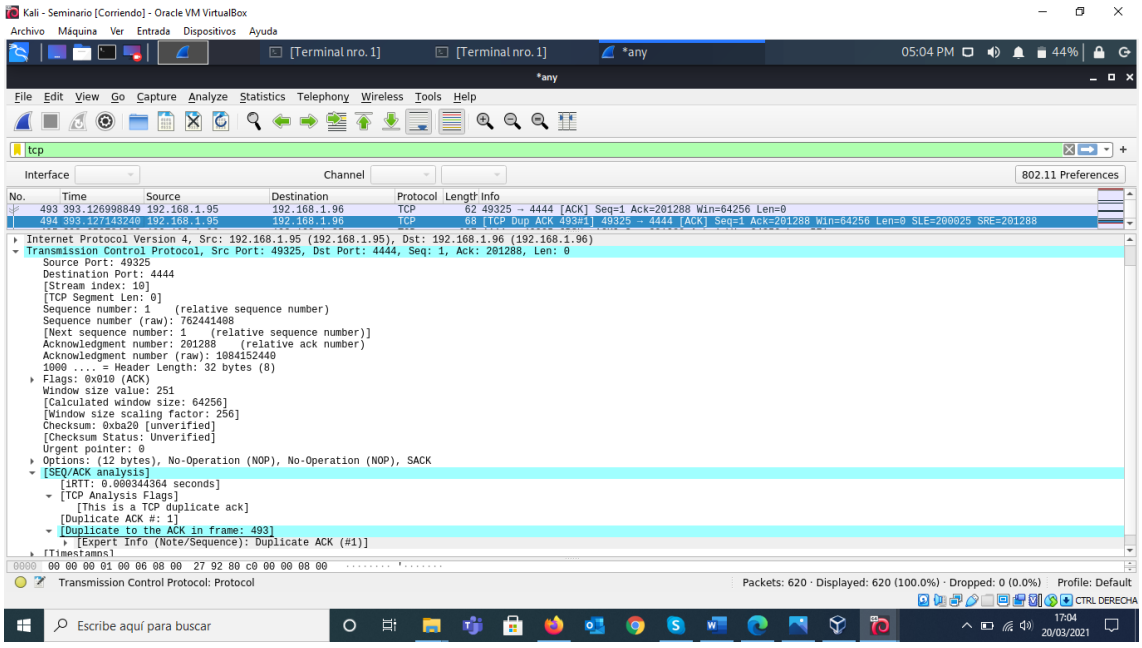
Figura 59 Identificación de anomalía en la red.



Fuente: Autor

Paso 4: Segunda toma de muestra en análisis de la información en la red y su contexto explicativo.

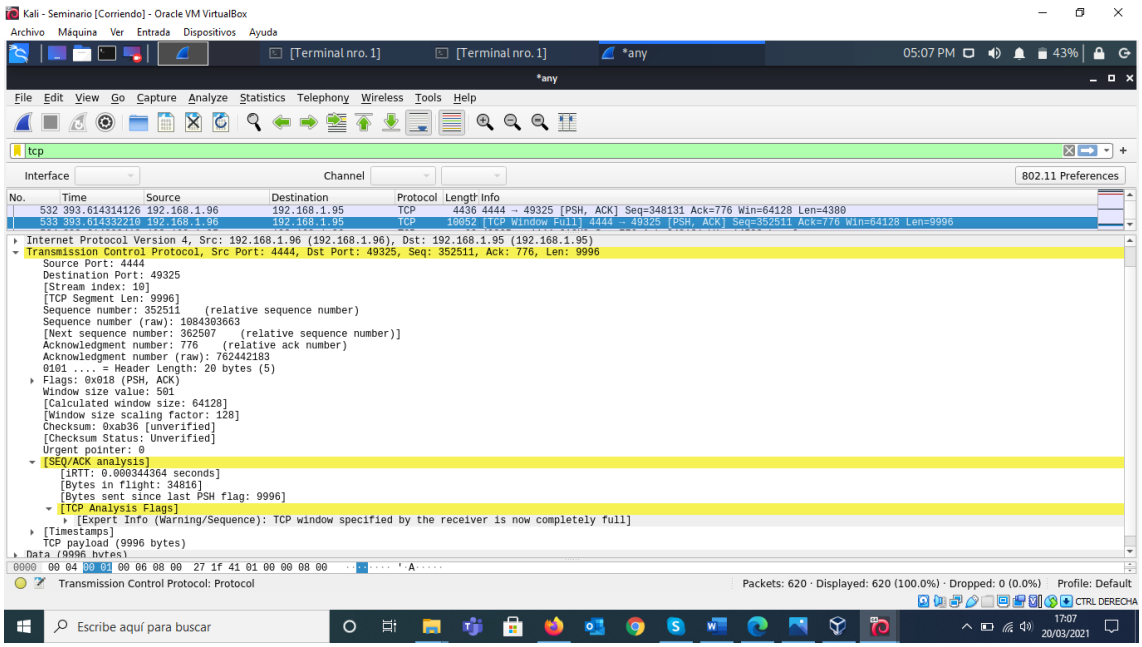
Figura 60 Segunda muestra de análisis.



Fuente: Autor

Paso 5: Tercera toma de muestra en análisis de la información en la red y su contexto explicativo para poder ser graficados.

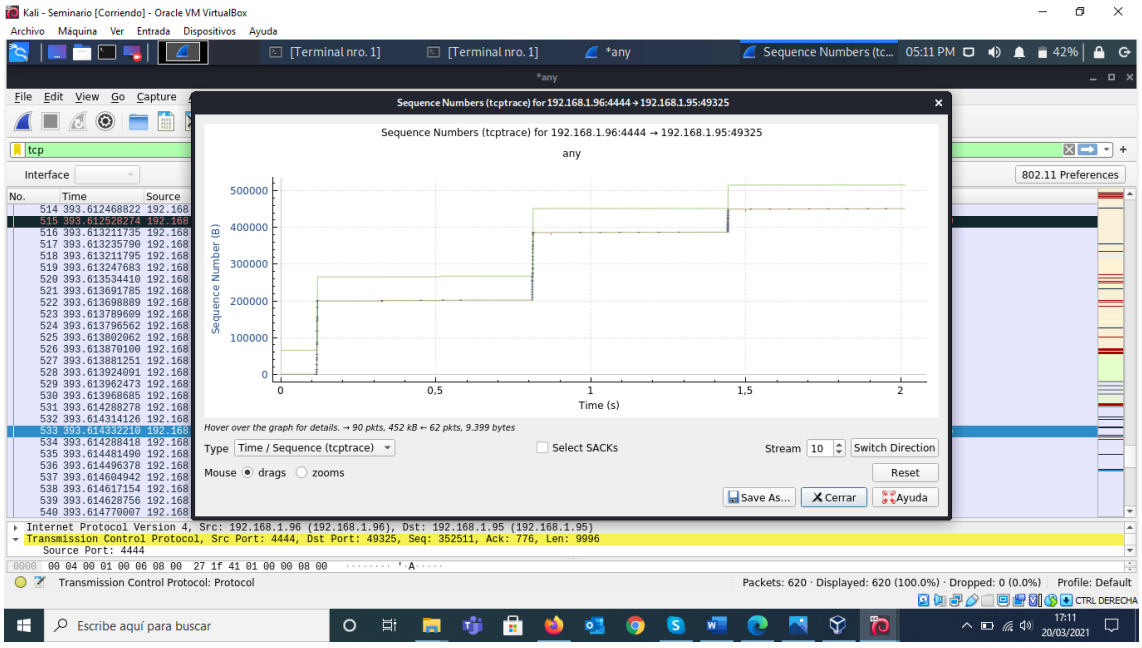
Figura 61 Muestra para ser graficada.



Fuente: Autor

Paso 6: Grafica secuencias numerales de proceso anómalo en la información muestreado.

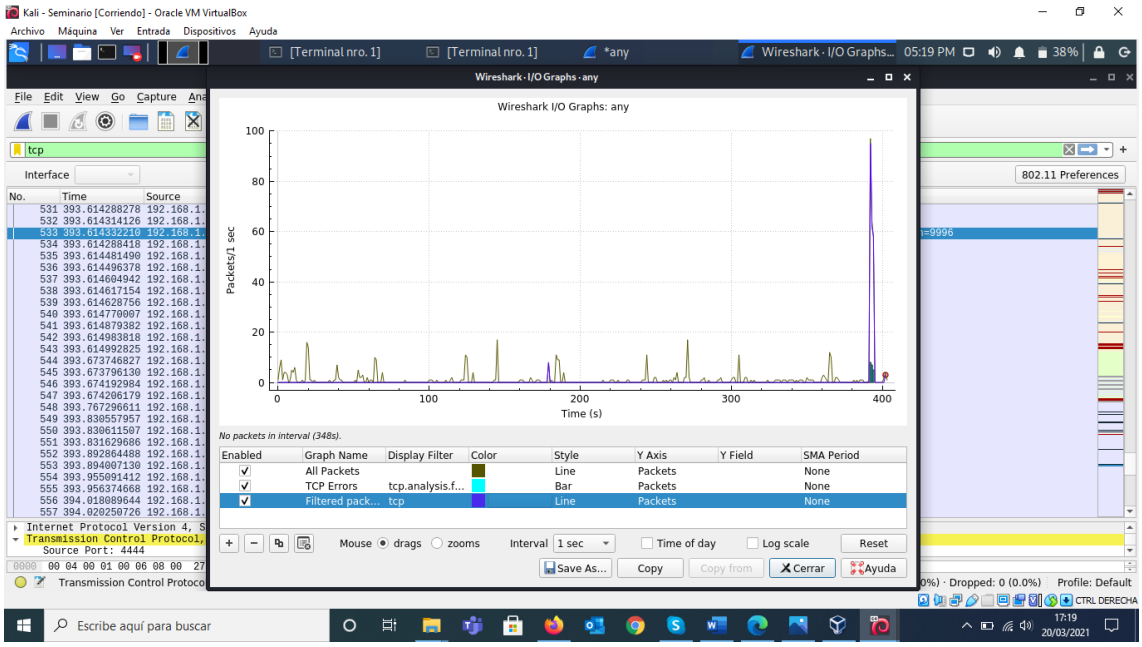
Figura 62 Gráfica Sistema secuencial númeral.



Fuente: Autor

Paso 7: Análisis de gráficas I/O, la cual me permite identificar todos los paquetes de la transmisión, los respectivos errores presentados en TCP y el filtrado de paquetes de la transmisión.

Figura 63 Gráfica I/O

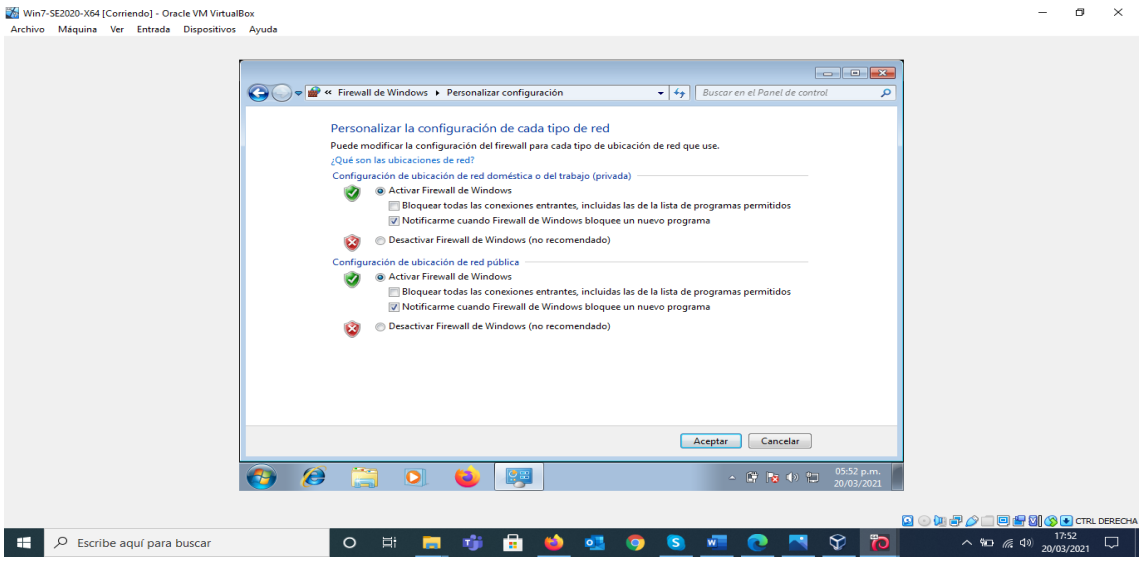


Fuente: Autor

Luego de haber realizado el análisis con la herramienta Wireshark, tomamos las medidas establecidas para minimizar el impacto de riesgo informático.

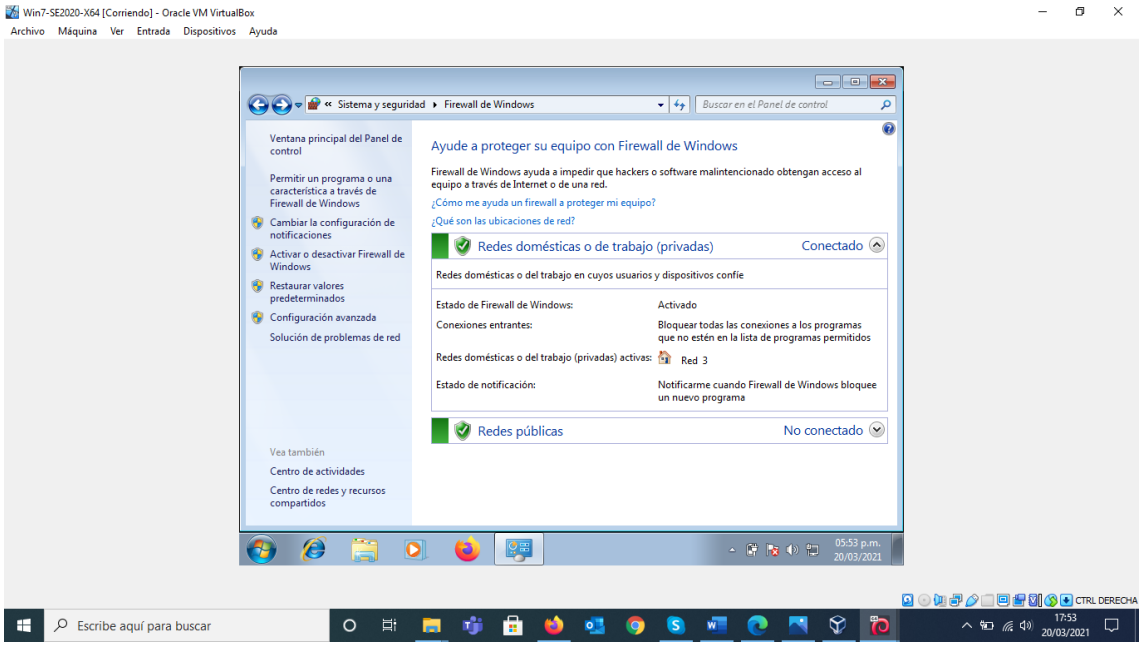
Paso 8: Se procede a realizar la activación del firewall en el equipo Win 7 x64.

Figura 64 Configuración activación firewall en Win 7 x64.



Fuente: Autor

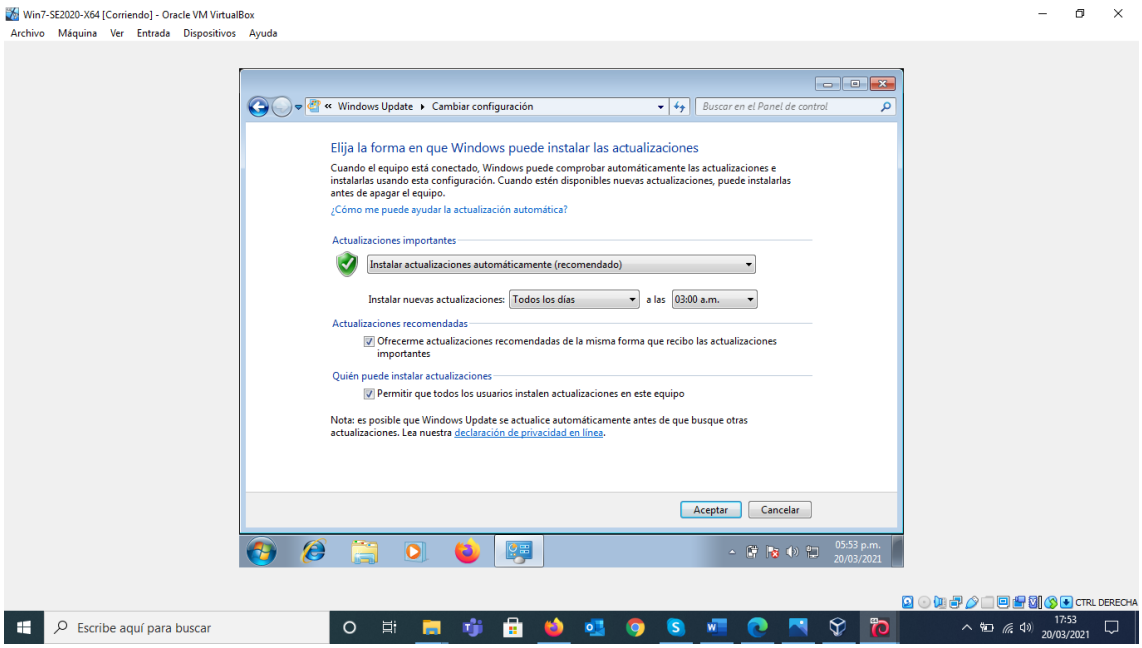
Figura 65 Activación realizada Win 7 x64.



Fuente: Autor

Paso 9: Realizamos la activación del Update de Windows para permitir recibir actualizaciones del sistema.

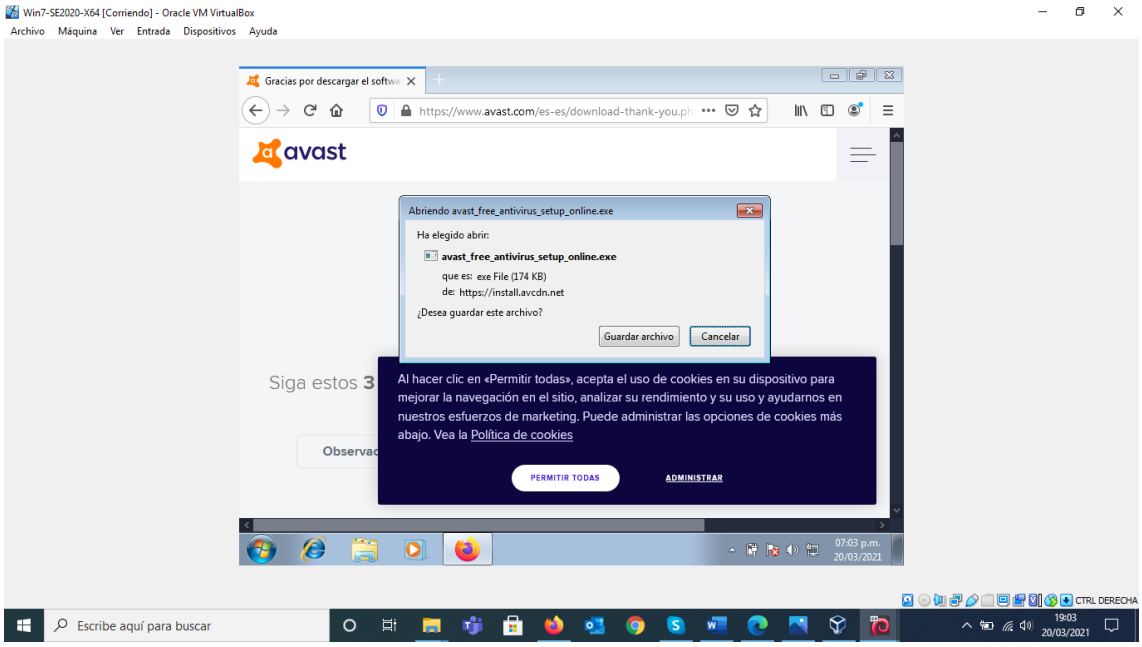
Figura 66 Activación Update Windows.



Fuente: Autor

Paso 10: Se procede a descargar antivirus para protección del equipo, ya que en el análisis mostraba que no tenía ningún tipo de antivirus instalado en el equipo.

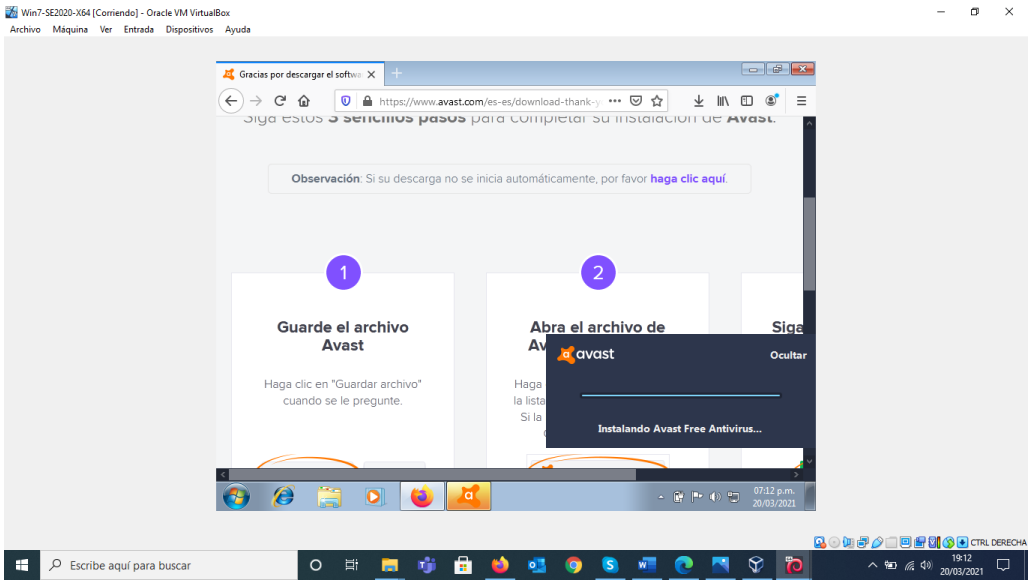
Figura 67 Descarga antivirus.



Fuente: Autor

Paso 11: Instalación antivirus en el equipo win 7 x64 y retirada la alerta de no antivirus.

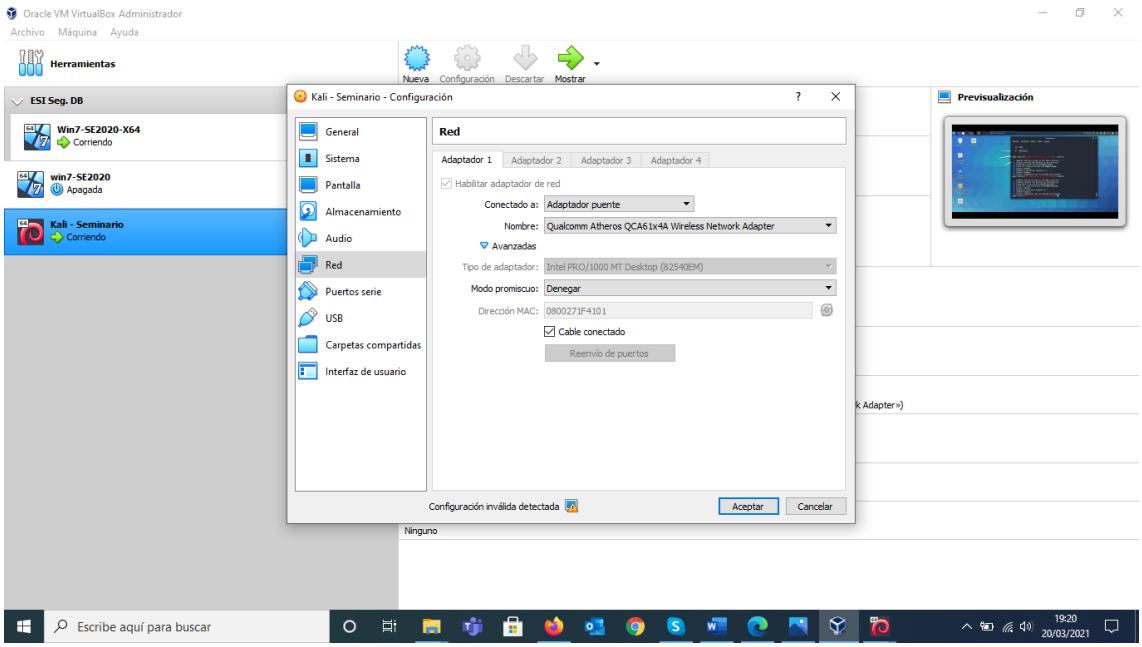
Figura 68 Antivirus Instalado.



Fuente: Autor

Paso 12: Cambiamos los permisos del modo promiscuo que tiene la red del equipo Win 7 x64 y en el Kali Linux.

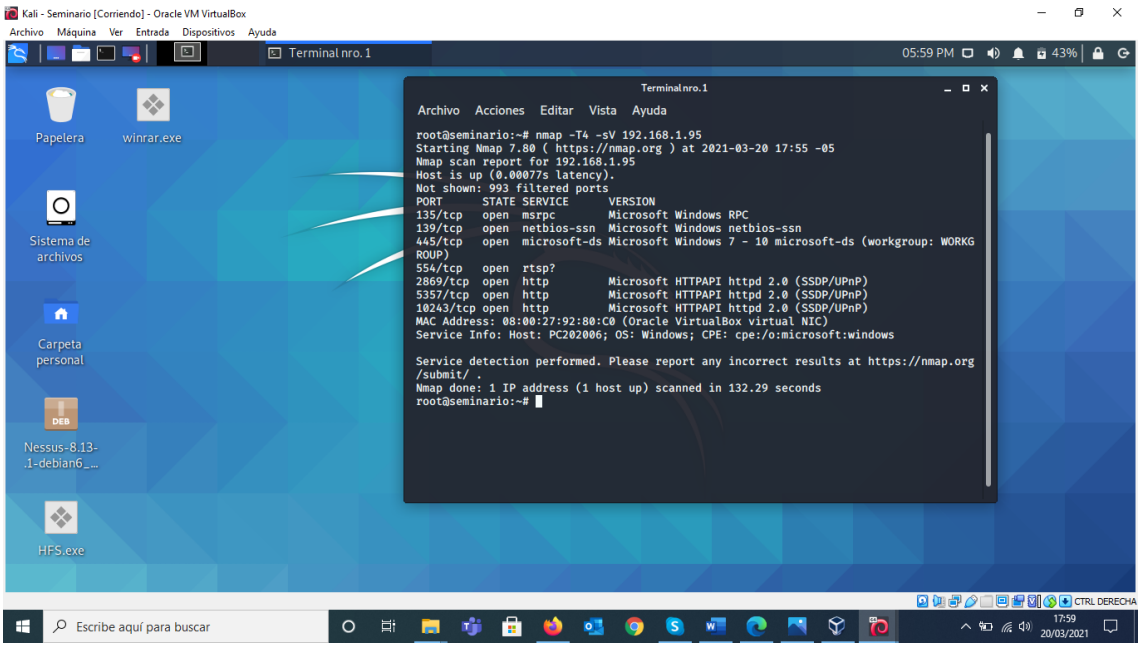
Figura 69 Cambio modo promiscuo denegado Kali Linux



Fuente: Autor

Paso 13: Realizamos nuevamente el ataque para evaluar los procesos de minimización de riesgo informático. Verificación de puertos y servicios.

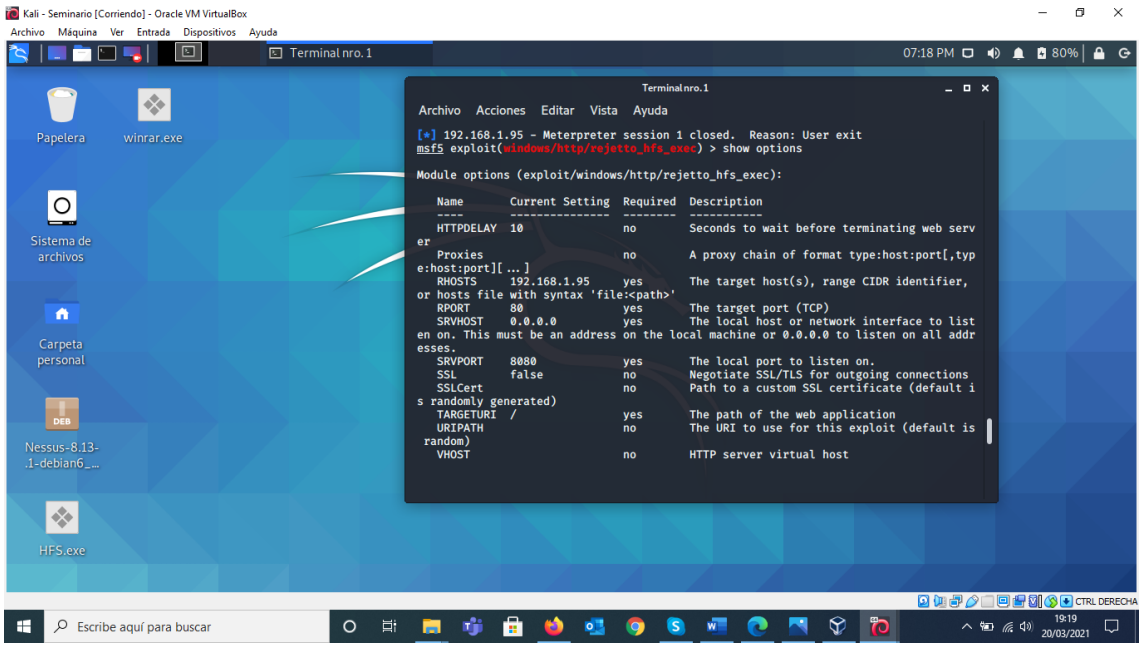
Figura 70 Verificación de puertos y servicios.



Fuente: Autor

Paso 14: Nuevamente realizamos el proceso de set para payload y equipo host.

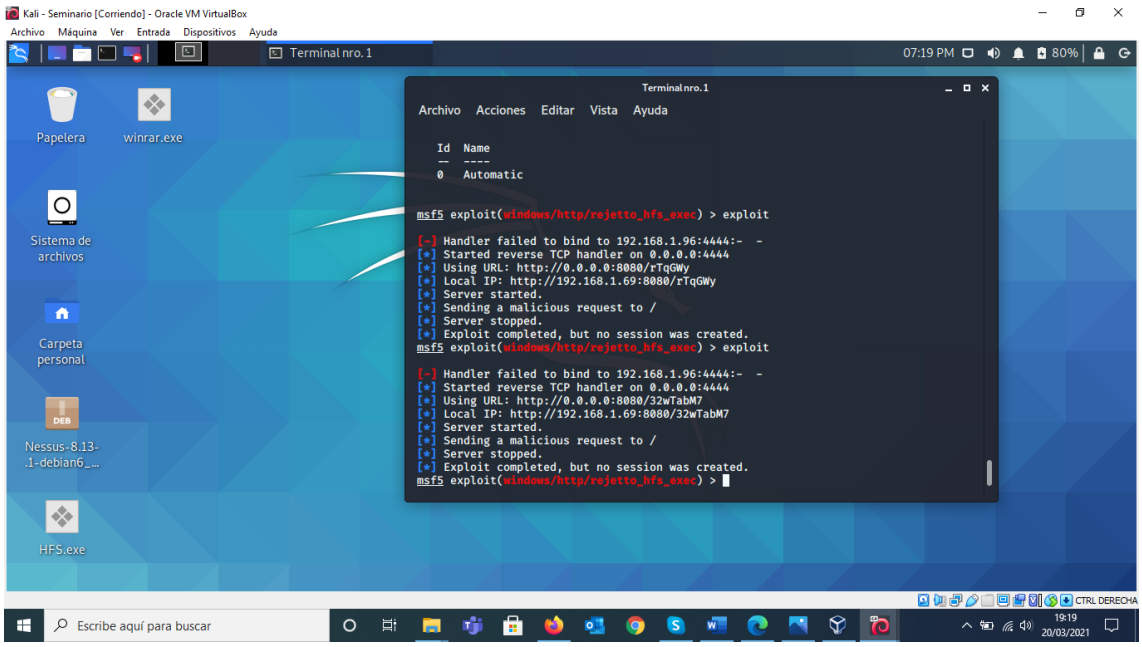
Figura 71 Configuración rejetto.



Fuente: Autor

Paso 15: Enviamos nuevamente el ataque y verificamos que no se puede ejecutar. Se realizan en dos oportunidades el exploit sin tener resultados positivos para el ataque.

Figura 72 Ataque fallido exploit.



Fuente: Autor

En soporte de lo anteriormente realizado, se presenta las características de algunos procesos que se pueden empelar para evitar el ataque:

Figura 73 Procesos anti-ataques.

Configuración política local de seguridad en el sistema.

- Identifica procesos y requisitos de utilización de contraseñas, deshabilitar cuentas de administrador y limitar los privilegios de los usuarios.

Auditorias en archivos organizacionales.

- Permite identificar si el sistema a sufrido algun tipo de alteración o modificación según la base de datos almacenada y tomada al principio de las labores.

Auditorias en los servicios.

- Permite identificar los servicios que se ejecutan, sus características ante un eventual ataque, que puertos son utilizados y que tipo de protocolos son utilizados.

Protección de Hardware.

- Restringue las entradas a cualquier dispositivo de almacenamiento externo, contraseñas de arranque del sistemas.

Aislar procesos.

- Aplicación de servidores dedicados y aislados de la red, denegando el ingreso a intrusos.

Llaves SSH.

- Estructura una autenticación secreta y una para poder compartir con el resto de usuarios.

Programas de seguridad.

- Intalación de antivirus, antispam y antispyware.

VPN - Redes Privadas.

- Creación de conexiones remotas que se encuentran disponibles exclusivamente para ciertos usuarios/servidores.

Fuente: Autor

4.3 Diferencias entre equipo de Blue team y equipo de respuestas a incidentes informáticos.

Como podemos observar a continuación en la (tabla 1 Cuadro comparativo entre equipamiento repuesta incidentes informáticos y Equipos Blue team). Se puede detallar con precisión las diferencias entre equipos Blue team y equipos de respuesta a incidentes informáticos, tendemos en cuenta las características de aplicación y sus respectivos análisis según correspondan a sus acciones.

Tabla 1. Cuadro comparativo entre equipamiento repuesta incidentes informáticos y Equipos Blue team.

Característica	Equipamiento respuesta incidentes informáticos	Equipos Blue team
Equipo	Se enfoca en incidencias informáticas.	Se enfoca en seguridad defensiva.
Operabilidad	Identifica causantes de incidentes y sus consecuencias.	Identifica comportamiento sobre el sistema y aplicaciones.
Hecho	Incidentes de hechos sospechosos.	Actúa sobre ataques de amenaza y riesgos.
Actuador	Gestiona incidencias de una entidad.	Contención de ataques y propone mejoras para la entidad.
Análisis	Analiza situaciones y responde a incidencias	Analiza y evalúa riesgos – soluciones SEIM
Vigilancia	Es periódica, pues los objetivos son específicos y eficientes para nulidad de ataques.	Es constante permitiendo procesos de documentación en bienestar de la entidad.
Estudio	Endurecimiento de software, para reducir el número de incidentes.	Caracterización forense de las maquinas afectadas, propone soluciones y medidas de detección.
Verificación	Efectividad en la respuesta con normalidad en la operatividad de la entidad.	Caracteriza la efectividad de las medidas de seguridad.
Proceso	Gestión de los respectivos incidentes	Rastreo de incidentes de ciberseguridad.

Fuente: Autor

4.4 Análisis sobre la utilización de un equipo Blue team en los procesos de trabajo con CIS “Center For Internet Security”.

Definición CIS (Center For Internet Security): Este sistema de seguridad tiene como objetivo principal mantener la seguridad de internet, realizando actividades como identificar, ejecutar, validar y proporcionar soluciones correspondientes a procesos de ciberdefensa. Este sistema cuenta con diversas herramientas y controles que permiten realizar configuraciones de seguridad sobre el sistema a proteger, coordinado bajo normas legales vigentes.

Como equipo Blue team lo utilizaría como un procedimiento establecido para seguridad contra ataques cibernéticos, ya que maneja un estándar establecido bajo proceso de seguridad y permite controlar al atacante.

Estor procedimientos se ejecutan cuando sucede alguno de los siguientes casos en donde el atacante aprovecha:

- La ubicación de equipos desprotegidos y que se encuentren conectados a una red.
- En el momento de mal uso de los privilegios, caso particular; ser engañado para abrir un archivo maliciosos o acceso a páginas que lo único que buscan es ingresar a tu sistema.
- La explotación de algunas vulnerabilidades como los son puertos, servicios, contraseñas inseguras, cuentas mal protegidas o instalación de software que no son necesarias su ejecución.
- Indagar configuración de la red para exploración remota para distribución de material y/o información maliciosa.
- Alteración del sistema para ingresar configuraciones, manipulación del software y cualquier tipo de información salvaguardada en el disco.
- Engaño de usuarios con falsos procesos de información dañada y aplican códigos maliciosos.
- Buscan identificar e indagar si la información confidencial esta salvaguardada con la misma seguridad de la información ordinaria.
- Intervienen las conexiones inalámbricas para realizar la conexión a la red de la empresa.
- Hacer uso de cuentas no usadas para realizar los procesos de ingreso de información maliciosa, ya que este tipo de cuentas no permiten ser descubiertos.
- Rastreo de operación en servicios mal configurados para implantar procesos maliciosos.

4.5 Características y Funciones principales de un SIEM

Definición SIEM: Modelo informático, que permite realizar el proceso de seguridad de la información y la respectiva gestión de ventos. Tiene como principal objetivo detectar amenazas que se presenten en las organizaciones de manera potencial y resolverlas de manera eficiente en un corto tiempo.

Figura 74 Funciones y características principales SIEM.

FUNCIONES PRINCIPALES.

- Permitir resolver de manera eficiente y eficaz a cualquier tipo de amenaza.
- Analizar en tiempo real ataques que se presente en el hardware y/o software, alertando según el progreso de la amenaza.
- Detectar amenazas, ataques, vulnerabilidad, mal uso del sistema de información, precisando cuál de ellos están en mayor riesgo de ataque.
- Minimizas la afectación del ataque en tiempos cortos.
- Visualizar los proceso y procedimientos de la seguridad en los sistemas teleinformáticas.

CARACTERISTICAS PRINCIPALES.

- Herramientas contra amenazas: Implementar aplicaciones para la seguridad.
- Monitoreo: Convergencia de aplicaciones, fuentes de datos e interfaz, para análisis de la información
- Usuarios: Socializa infracción de políticas de seguridad, bloqueos y desbloqueos de cuentas, cambios en privilegios, entre otros.
- Caracterización: Identificación de eventos discretos, comportamientos sospechosos, concordancias en listas blancas, entre otras.
- Administraciones incidentes: Notifica a los usuarios precisos, procesos de configuración de aletas y acciones automatizadas.
- Contexto de amenazas: Valida eventos sospechosos para ser evaluados y priorizar el de mayor impacto y riesgo.
- Riegos de datos: Recolecta información total del caso generado, ya que permite manejar cantidad de bases de datos.

Fuente: Autor

4.6 Caracterización de 3 herramientas que permiten contener ataques informáticos.

A continuación, se presentan 3 tipos de herramientas que permiten realizar la contención del ataque, permitiendo la minimización del impacto y del riesgo de pérdida o modificación de la información en el sistema de la organización.

- **OSSEC:** Permite realizar análisis en el registro de la información, identifica y caracteriza la integridad e información de las alertas que se presenten, admite realizar la administración del sistema a partir de su monitoreo, puede realizar cualquier tipo de detección de ataques para la mayor parte del sistema operativo.

- **SNORT:** Permite realizar análisis y registros de los paquetes en tiempo real; logra identificar ataques DoS y DDoS. Su utilidad principal es detectar exploits y exploración de puertos. Analiza el tráfico de la red y si existe algún tipo de amenaza bloquea el ataque.

- **OPENWIPS:** Permite la detección y prevención de ataques en el sistema inalámbrico que se presenta en sensores donde se detectan amenazas, manejo de tráfico para su análisis y caracterización del sistema de seguridad; interfaces de red inalámbricas permitiendo analizar ataques que pueda ser expuesto; y servidores que se generan las aletas y respuesta ante algún tipo de amenaza, permite analizar la información envida por los sensores.

CONCLUSIONES

Luego de haber realizado los procesos de análisis, caracterización, fundamentación estratégica y ejecución de pruebas con equipamiento de ciberseguridad para procesos Red Team y Blue Team, se pueden estructurar conclusiones importantes, con el fin de organizar y afianzar conocimientos desde las perspectivas y enfoques de la ciberseguridad:

- ✓ Toda Empresa de dependencia nacional o internacional, debe contar con una estructura organizacional y de gestión sobre procesos de seguridad de la información.

- ✓ Conformar con personal especializado y cualificado en experiencias de seguridad informática, los respectivos equipos de Red Team y Blue Team de la empresa, permitiendo tener un equipo sólido para resolver ataques que atañan sobre la organización.

- ✓ Diseñar e implementar medidas de seguridad que logre minimizar o mitigar el impacto de ataques o amenas sobre el sistema informático. Dentro de las medidas de seguridad tendremos la activación de antivirus, activación y actualización de firewall, activación y actualización de sistemas operativos licenciados, monitoreo y bloqueo de puertos, desactivación de cualquier tipo de acceso remoto y realizar la configuración adecuadas para entrega de permisos de seguridad correspondiente a carpetas y/o archivos del sistema.

- ✓ Es importante tener claridad en el momento de selección de herramientas de contención, realizar el debido análisis de los factores en riesgo del sistema, y fijando las capacidades de respuesta que se tienen con respecto a incidentes que se presente en tiempo real, lo anterior permite evaluar con certeza y eficiencia el proceso desarrollado por el profesional de seguridad, como de la herramienta seleccionada para ejecución el procedimiento.

RECOMENDACIONES

Siguiendo las sugerencias normativas y las estructuras del marco de seguridad informática, se plantean las siguientes estrategias que permiten endurecer los aspectos de seguridad en la organización:

- ✓ Contar constantemente con software de seguridad con activadores licenciados y actualizados, ya que del óptimo funcionamiento que presenten, se podrán generar las estrategias de defensa contra cualquier tipo de ataque.

- ✓ Generar políticas de seguridad en la organización, que permita socializar con cada uno de los empleados la importancia de este sistema de seguridad, mantener capacitaciones de actualización en normativas y procedimientos establecidos para la seguridad informática, contextualizar en las actividades desarrolladas en cada dependencia de la organización la aplicabilidad del código de ética.

- ✓ Establecer procedimiento de monitoreo sobre manejo y actualización de las herramientas que permitan detección de vulnerabilidades, explotación y contención de ataques.

- ✓ Realizar configuración de cuentas administrador/usuario adecuadas, permitiendo a los trabajadores realizar sus labores diarias en cuentas con acceso limitados. Bloquear o deshabilitar cuentas de administrador.

- ✓ Restricciones de instalación de software sobre el sistema sin previa autorización, permitiendo minimizar el impacto desde programas maliciosos que solo buscan el robo de información.

- ✓ Instalar sistemas de seguridad como Antivirus, Antispam y Antispyware.

REFERENCIAS BIBLIOGRÁFICAS

Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. Recuperado de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26) Recuperado de: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29) Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. Recuperado de: https://www.cisecurity.org/cis-benchmarks/

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira. (pp. 18-61). Recuperado de: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27)Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Incibe. (2014). OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. INCIBE-CERT. Recuperado de: https://www.incibe-cert.es/blog/owasp-4

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Mintic. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63) Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26) Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. Recuperado de: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. Recuperado de: https://metasploit.help.rapid7.com/docs/metasploitable-2

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. Recuperado de: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Link video sustentación:

https://youtu.be/pibKXZNSjWE

Link archivo diapositivas sustentación:

https://drive.google.com/drive/folders/1zR4MB15_MMjWXxXwKAWnfa64bR1V9xr2