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

DIEGO ALONSO GÓMEZ NOVOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

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

DIEGO ALONSO GÓMEZ NOVOA

Luis Fernando Zambrano
Tutor de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

Red Team: Equipo encargado de realizar los ataques informáticos con el fin de establecer los fallos en la estructura tecnológica de una determinada empresa.

Blue Team: Equipo encargado de estudiar el comportamiento del sistema y de sus usuarios en una empresa con el fin de identificar rápidamente cualquier incidente informático.

Pentesting: Practica de atacar diversos entornos con el fin de identificar o vulnerabilidades.

Intrusión: Acceso no permitido de seguridad a un sistema.

Vulnerabilidad: Debilidad o fallo en un sistema que pone en riesgo la seguridad de la información de una empresa permitiendo a un atacante comprometer la integridad o disponibilidad.

Amenaza: Según MINTIC2[1], son las causas o factores potenciales que pueden provocar daños dentro de una empresa.

Firewall: Cortafuego, su objetivo es proteger a los equipos de la red externa

Delito informático: Los delitos informáticos son todas aquellas acciones ilegales, delictivas o no autorizadas que hacen uso de dispositivos electrónicos.

[1] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. [Guía No 10]. (15 de diciembre de 2010). Seguridad y Privacidad de la Información. Guía para la preparación de las TIC para la continuidad del negocio. Bogotá, Colombia: MINTIC.p.3

RESUMEN

En la seguridad informática y protección de datos, entra a participar 2 equipos fundamentales como Red team y Blue team, Unir da la definición que son los que tienen la labor de aplicar estrategias en ambientes con control, con el objetivo de crear sitios de ataque y defensa utilizando las diferentes técnicas y herramientas con el objetivo de localizar vulnerabilidades y así poder mitigarlos, tendiendo como fin asegurar los activos primarios de las empresas como es la información y la infraestructura de tecnología.

Este documento presenta una propuesta que especifica las funcionalidades, procesos, herramientas e informes acerca de la colaboración de los equipos Red Team & Blue Team para la detección de vulnerabilidades y asegurar la estructura de tecnología de las empresas, al consolidarse la importancia de los sitios emulados y el entrenamiento que crea para cada uno de los grupos con el objetivo de hacer frente a las amenazas, mitigando que ellas logren afectar a la empresa.

INTRODUCCIÓN

En la seguridad informática y protección de datos, entra a participar 2 equipos fundamentales como Red team y Blue team, Unir[1] da la definición que son los que tienen la labor de aplicar estrategias en ambientes con control, con el objetivo de crear sitios de ataque y defensa utilizando las diferentes técnicas y herramientas con el objetivo de localizar vulnerabilidades y así poder mitigarlos, tendiendo como fin asegurar los activos primarios de las empresas como es la información y la infraestructura de tecnología.

Este documento presenta una propuesta que especifica las funcionalidades, procesos, herramientas e informes acerca de la colaboración de los equipos Red Team & Blue Team para la detección de vulnerabilidades y asegurar la estructura de tecnología de las empresas, al consolidarse la importancia de los sitios emulados y el entrenamiento que crea para cada uno de los grupos con el objetivo de hacer frente a las amenazas, mitigando que ellas logren afectar a la empresa.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

The WhiteHouse Security ha presentado problemas al interior de la organización por lo cual requiere deberá utilizar en una serie de escenarios y problemas complejos para que estos sean gestionados por el personal postulado que busca ser parte del equipo Blue Team.

1.2 FORMULACIÓN DEL PROBLEMA

The WhiteHouse security requiere por medio de una serie de preguntas orientadoras y el montaje del banco de trabajo seleccionar el personal idóneo para hacer parte del equipo de Red Team y Blue Team con el cual se busca identificar el conocimiento mediante los diferentes escenarios planteados, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

2. JUSTIFICACIÓN

A través de los años, la tecnología se convirtió en una necesidad hoy en día, esto ha provocado que las empresas sin importar el tipo de actividad realicen una transformación digital, la cual ofrezca una mejor expectativa a sus clientes internos y externos, generando valor agregado y siendo así más comerciales frente a las demás empresas en el mercado global, por esto es importante asegurar la infraestructura tecnológica y los sistemas de información, realizando de manera constante el análisis de seguridad a través de diferentes metodologías de intrusión y testing con el objetivo de identificar posibles vulnerabilidades para ser corregidas de manera eficiente; esto se puede realizar con equipos de seguridad especializados de equipo rojo y equipo azul quienes se introducen en la búsqueda de vulnerables realizando procedimientos con el fin de ofrecer la seguridad de la estructura de tecnología de las empresas.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar un informe técnico el cual consolide las fases desarrolladas en el seminario de especialización equipos estratégicos en ciberseguridad red team & blue team.

2.2 OBJETIVOS ESPECÍFICOS

Describir margen legal en Colombia sobre delitos informáticos, etapas de pentestig, herramientas de ciberseguridad y configurar banco de trabajo.

Evaluar las acciones de los equipos Red Team & Blue Team de The WhiteHouse Security en el marco de los criterios éticos y legales.

Demostrar vulnerabilidades en un sistema informático a partir técnicas de intrusión.

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en The WhiteHouse Security.

3 MARCO REFERENCIAL

Abarca los aspectos que fundamentan la investigación, por ejemplo: marco teórico, marco conceptual, marco legal, entre otros.

3.1 MARCO CONCEPTUAL

Seguridad informática. La seguridad informática en las empresas cada día preocupa más debido a los ataques cibernéticos que han puesto en riesgo su información, por lo cual es indispensable identificar y eliminar cualquier tipo de amenaza que genere pérdidas económicas en las empresas, por ello, se establecen normas, protocolos y políticas de seguridad informática[2]. La seguridad informática está básicamente orientada a proteger la propiedad intelectual y la información importante de las empresas y de las personas[3]

De acuerdo con lo indicado por Sitel[4] cuenta que "El 70 % de las pequeñas y medianas empresas son el objetivo de ciberataques para robar sus datos o usar su infraestructura para realizar todo tipo de actividades maliciosas. La limitación de recursos hace que los tiempos para detectar y responder a los ciberataques sean altos".

---

[1] UNIR, La universidad en internet. "Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?". {En línea}. {15 noviembre de 2020} disponible en: (https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/).

[2] UNITEL "Seguridad Informática en las empresas. Consejos básicos". {En línea}. {12 octubre de 2020} disponible en: (https://unitel-tc.com/seguridad-informatica-en-las-empresas-consejos/).

[3] Tarazona, Cesar "AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN". {En línea}. {12 octubre de 2020} disponible en: (https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/.).

[4] SITEL "Gestión de la seguridad Blue Team". {En línea}. {13 octubre de 2020} disponible en: (https://www.sistel.es/business-information-security/gestion-seguridad).

Al hablar de seguridad informática en las empresas, entran dos equipos como son red team y blue team los cuales realizan tareas en conjunto con el fin de identificar vulnerabilidades y prevenir amenazas[5].

Red Team. Red team es un equipo encargado de generar escenarios de amenazas (ataques cibernéticos) de manera controlada a los diferentes sistemas informáticos de una empresa, desde el punto de vista de un atacante con el fin de entrenar el equipo de seguridad blue team y medir la respuesta oportuna a los ataques con los diferentes sistemas de seguridad[6]

Blue team. Blue team es un equipo encargado de predecir, prevenir, detectar y brindar respuesta adecuada a los ciberincidentes reales o simulados durante un periodo de tiempo significativo, con lo cual se mide su tiempo de detección y de recuperación, con esto, el equipo aprende a reaccionar y defenderse de diferentes ataques y situaciones variadas[7].

Vulnerabilidades. Empresas tanto públicas como privadas, utilizan recursos que son denominados como activos, los cuales se encuentran expuestos a las diferentes amenazas tanto a nivel interno como externo, estas pueden ser naturales, inducidas por el hombre, de manera accidental o deliberada[8].

---

[5] UNIR, universidad en internet “Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?”. {En línea}. {12 octubre de 2020} disponible en: (https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/).

[6] UNIR, universidad en internet, op. cit,

[7] EC-COUNCIL, Blog “RED TEAM VS BLUE TEAM”. {En línea}. {13 octubre de 2020} disponible en: (https://blog.eccouncil.org/red-team-vs-blue-team/).

[8] SGSI “ISO 27001: Vulnerabilidades de la empresa”. {En línea}. {14 octubre de 2020} disponible en: (https://www.pmg-ssi.com/2015/06/iso-27001-vulnerabilidades-de-la-organizacion/#:~:text=Las%20vulnerabilidades%20pueden%20encontrase%20asociadas,%2C%20equipos%2C%20software%20o%20informaci%C3%B3n.&text=Falta%20de%20aplicaci%C3%B3n%20de%20procedimientos,Fallos%20del%20control%20interno.).

Indibe[9] define que “las vulnerabilidades son las condiciones y características propias de los sistemas de una empresa que la hacen susceptible a las amenazas. El problema es que, en el mundo real, si existe una vulnerabilidad, siempre existirá alguien que intentará explotarla, es decir, sacar provecho de su existencia”.

Ciberseguridad. De acuerdo a lo reportado por destinonegocio[10] indica que “Los ciberataques a las empresas medianas y pequeñas con frecuentes, esto dado que no poseen los recursos económicos necesarios por lo cual se convierten en punto de ataque por los ciberdelincuentes, cuando una empresa se encuentra en su etapa de crecimiento no priorizan la seguridad informática y trabajan sobre sistemas desactualizados, equipos obsoletos, falta de implementación de nuevas tecnologías, personal capacitado que brinde una reacción inmediata sobre los ataques, de 5000 ataques, solo identifican el 56 % y el 41 % son irremediables”.

3.2 MARCO LEGAL

La ley 1273 de 2009 judicializa de manera penal la intrusión, obstaculización, manipulación, interceptación, daños, instalación de software malicioso, suplantación y extracción de información sobre los diferentes sistemas informáticos, los cuales afecten de alguna manera a personas u empresas que atenten contra su integridad, confidencialidad y disponibilidad. Está compuesta por los siguientes artículos:

•Artículo 269A
•Articulo 269B

[9] INCIBE_ “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”. {En línea}. {14 octubre de 2020} disponible en: (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian).

[10] DESTINONEGOCIO “¿Cómo evitar un ciberataque en las empresas?”. {En línea}. {14 octubre de 2020} disponible en: (https://destinonegocio.com/co/gestion-co/recursos-materiales-co-co/ciberataque/).

•Articulo 269D

•Articulo 269E

•Articulo 269H

Los delitos más comunes en Colombia son hurto por medios informáticos, violación de datos personales, acceso abusivo a sistema informático, transferencia no consentida de activos y uso de software malicioso.[11]

[12] EC-COUNCIL, Blog “RED TEAM VS BLUE TEAM”. {En línea}. {13 octubre de 2020} disponible en: (https://blog.eccouncil.org/red-team-vs-blue-team/).

[11] MINTIC, “Ley 1273 de 2009”. {En línea} {03 de octubre de 2020} disponible en: (https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf).

4 DISEÑO METODOLÓGICO

En el presente proyecto se realizan las siguientes etapas de la metodología para consulta, análisis de funciones, procesos y procedimientos.

Tabla 1. Metodología para análisis, consulta, procesos y procedimientos.

	Fase	Actividad
I.	Conocimiento	A travez de la consulta e identificación de fuentes documentales en los diferentes medios tecnológicos sobre información basada en equipos rojo y equipo azul, que proporciona todo lo relacionado con funciones, procesos, herramientas y métodos aplicados.
II.	Interpretación	La información consultada se identifica y clasifica tras analizar la documentación para llevar a cabo el desarrollo de los objetivos, se descartan las fuentes documentales que no son útiles y se completa con nuevas fuentes documentales e informativas.
III.	Análisis	La información recolectada es validada, cuestionada e identificada, la cual es brindada por los equipos equipo rojo y equipo azul de las diferentes fuentes documentales, con el fin de enriquecer, especificar y describir las funciones, procesos, herramientas y métodos ejecutados por los equipos y determinar cómo Contribuyen al aseguramiento de la infraestructura tecnológica en las empresas, además de esto, un informe sobre los métodos aplicados para detectar vulnerabilidades utilizados por los equipos del equipo rojo. y equipo azul.

IV.	Diseño	Se ejecutaron los siguientes pasos: Especifique los roles del equipo rojo y los equipos del equipo azul. Describir los procesos y procedimientos de los equipos rojo y azul en la detección y prevención de ciberataques Red Team & Blue Team de The WhiteHouse Security en el marco de los criterios éticos y legales Identifique las herramientas utilizadas para la intrusión y las pruebas por parte del equipo rojo y el equipo azul en The WhiteHouse Security.

Fuente 2. HERRERA M. Haroldo E. https://www.gestiopolis.com/metodologia-paraevaluacion-diagnostico-y-diseno-de-procesos/.

5 DESARROLLO DE LOS OBJETIVOS

5.1 DESCRIBIR MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS, ETAPAS DE PENTESTIG, HERRAMIENTAS DE CIBERSEGURIDAD Y CONFIGURAR BANCO DE TRABAJO.

Margen Legal en Colombia

Normativas sobre delitos informáticos:

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

Ley 1273 de 2009.

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

Artículos que componen 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.
- 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.

Ley 1581 de 2012.

Ley que permite proteger datos personales que se encuentran registrados en alguna base de datos.

Principios que componen esta 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.

ETAPAS DE UN PENTESTING:

- Fase 1: Recolección de información: Recopilar 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.

- Fase 3: Análisis de vulnerabilidades: Valorar los casos exitosos de nuestras estrategias de penetración a través del análisis y proactividad de vulnerabilidades.

    - Herramientas: NESSUS, Nmap, CVE.

- Fase 4: Explotación: Proceso de intentar conseguir los accesos a los diferentes sistemas objeto de nuestra prueba de penetración.

    - Herramientas: Metasploit, exploitdb.

- Fase 5: Informe:Presentar 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.

HERRAMIENTAS DE CIBERSEGURIDAD:

- Metasploit: 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. Encontramos 3 acciones importantes de referenciar:

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

- Nmap: 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: Herramienta de uso libre, que permite identificar vulnerabilidades logrando realizar correcciones de fallas de seguridad.

On Line Servicios:

- ExploitDB: Herramienta que 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.

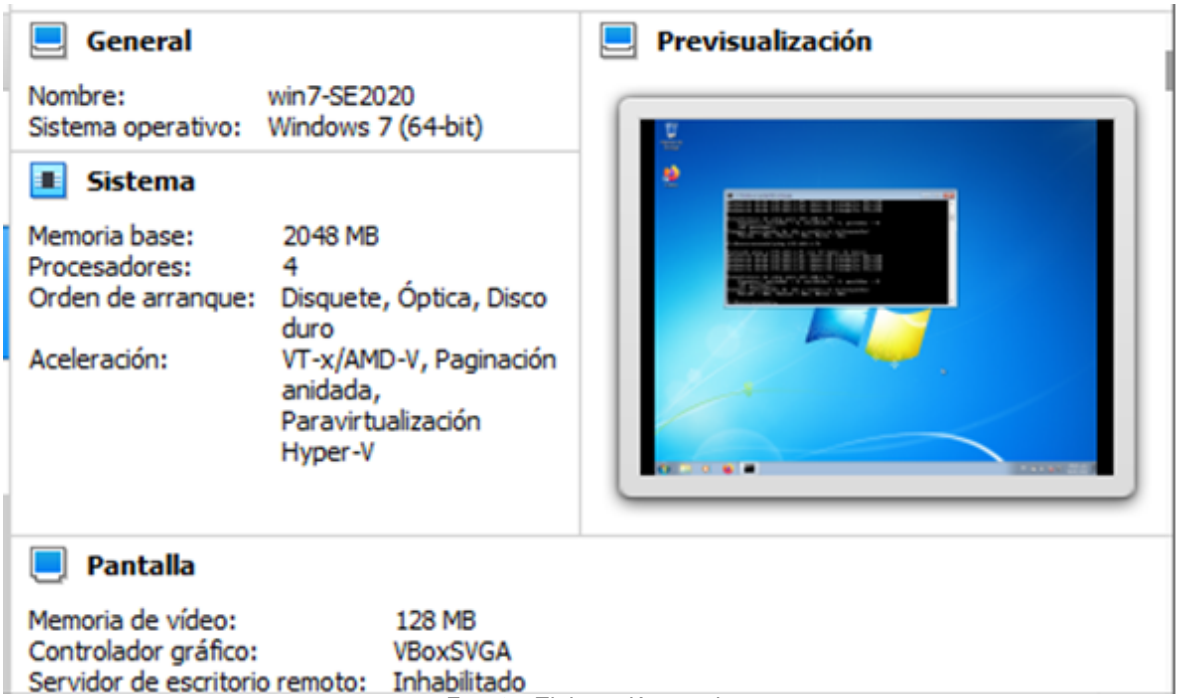
- CVE: Tipo de herramienta cuya característica son las vulnerabilidades y exposiciones comunes, en las bases de datos.

CONFIGURACIÓN BANCO DE TRABAJO:

Prueba de conectividad entre máquinas “win 7 – SE2020- X64” y máquina “win 7 – SE2020”:

Paso 1: Activar las dos máquinas correspondientes de prueba.

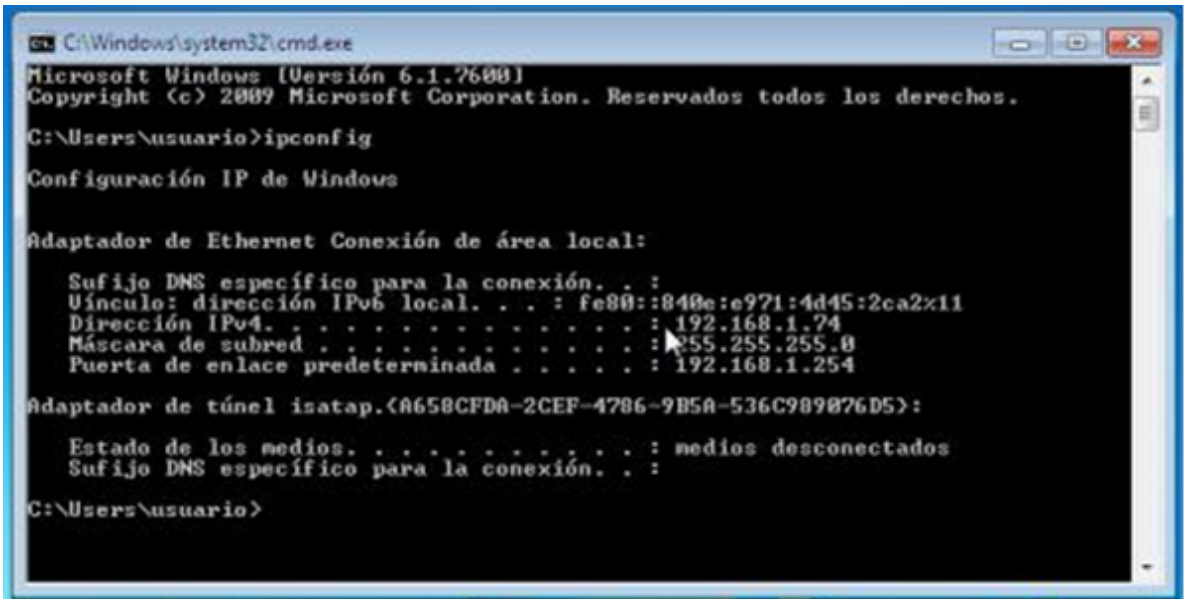
Figura 1. Entorno máquina Virtual win 7 x64 y x86.3



Fuente: Elaboración propia

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

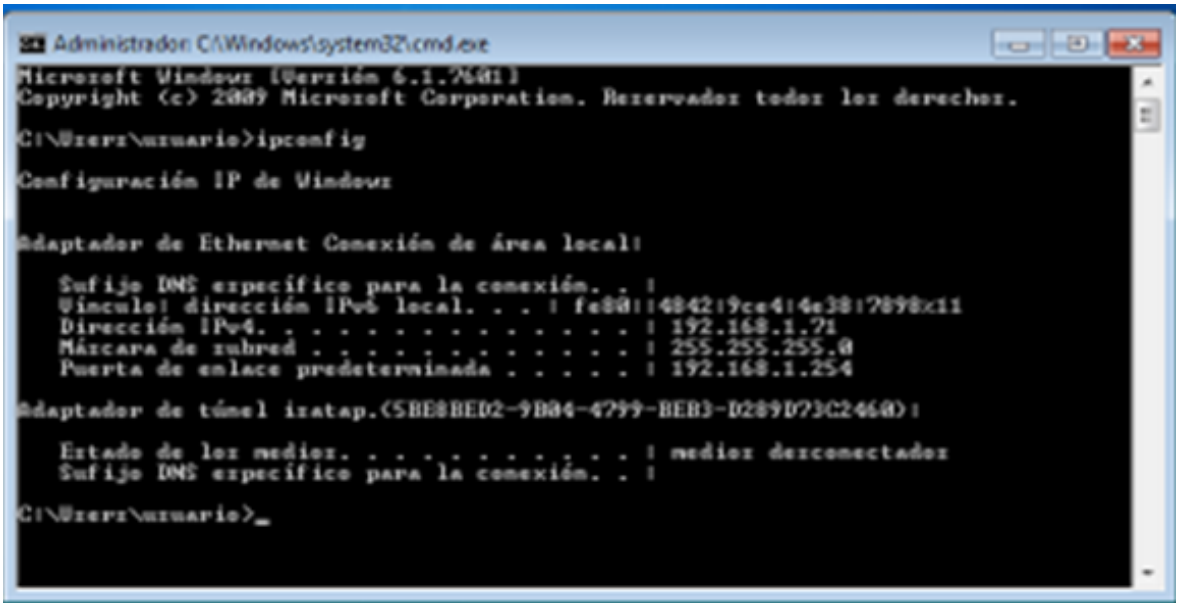
Figura 2. Dirección IP win 7 se2020.



Fuente: Elaboración propia

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

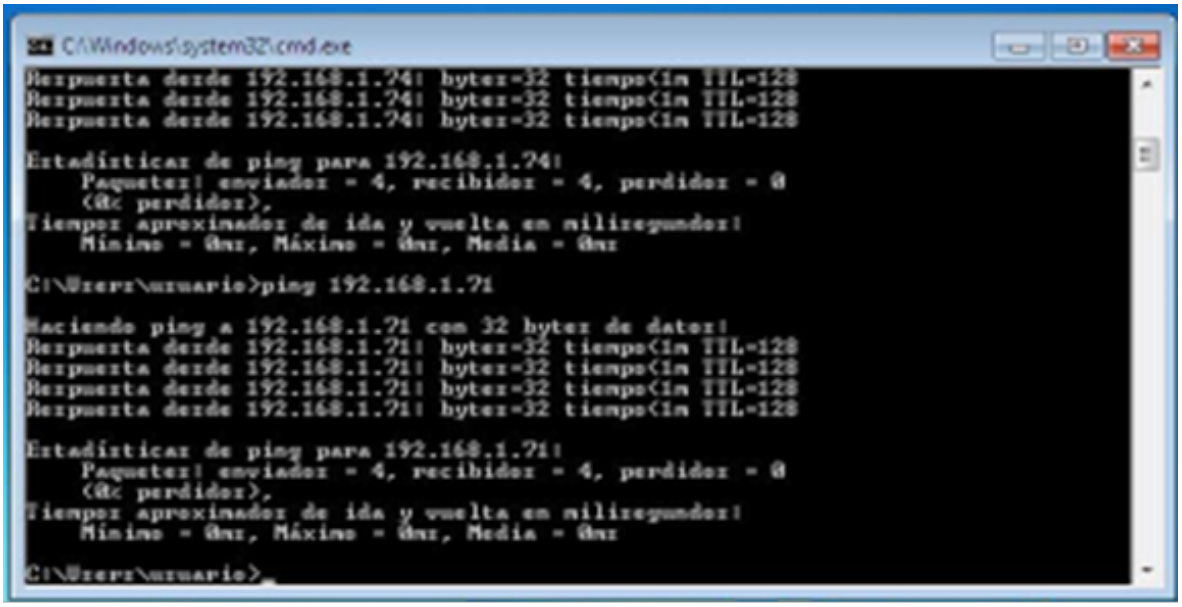
Figura 3. Dirección IP win7 SE2020 x64.



Fuente: Elaboración propia

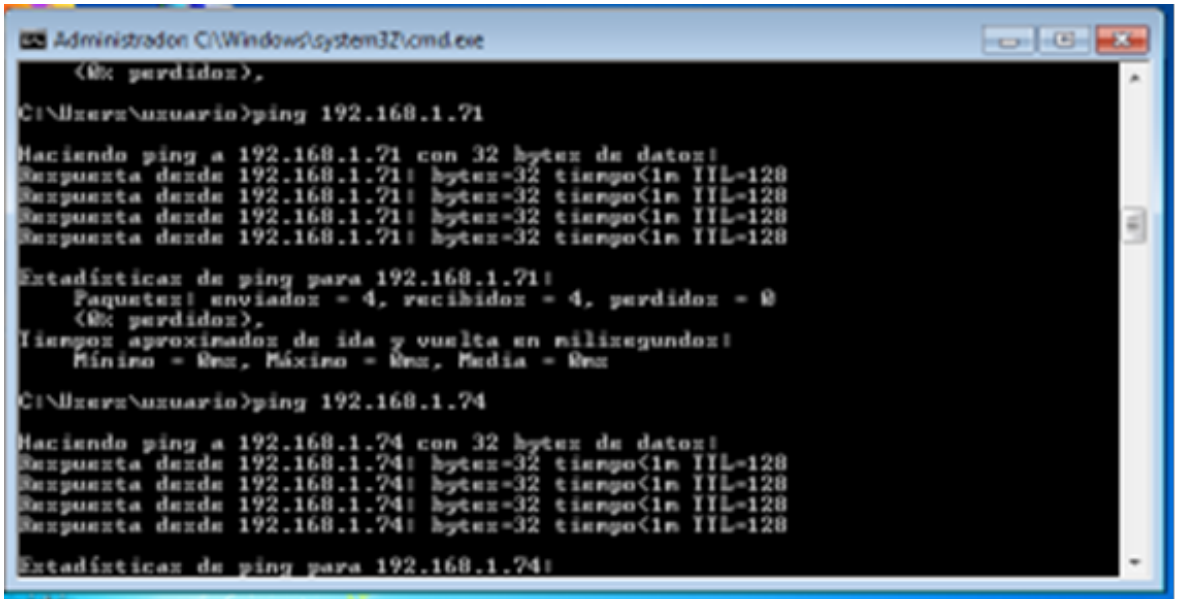
Paso 4: Validar conectividad entre las máquinas virtuales.

Figura 4. Verificación conectividad win 7 SE 2020.



Fuente: Elaboración propia

Figura 5. Verificación conectividad win 7 SE2020 x64.

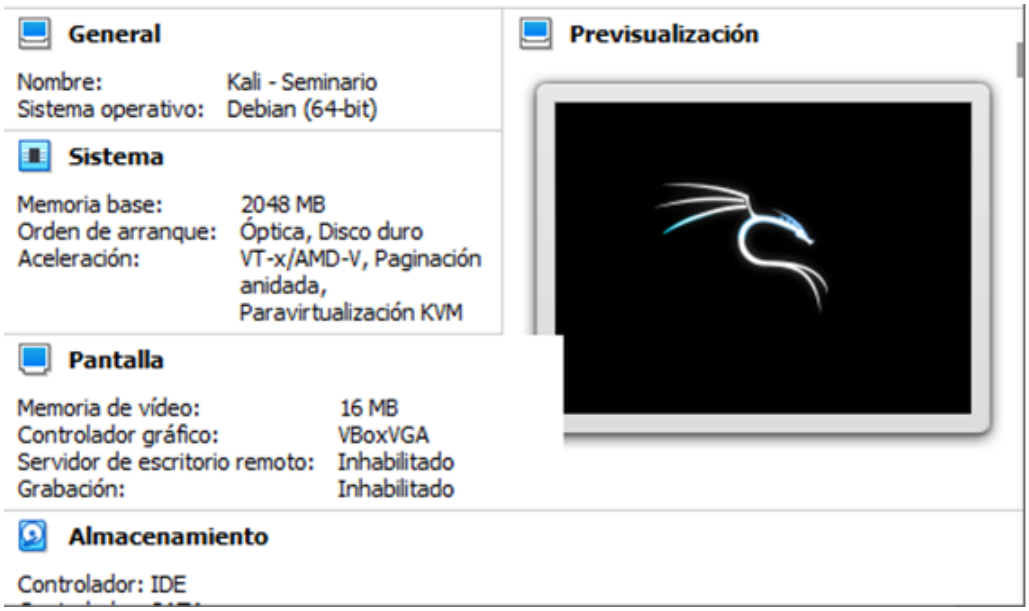


Fuente: Elaboración propia

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

Paso 1: Activar las dos máquinas correspondientes de prueba.

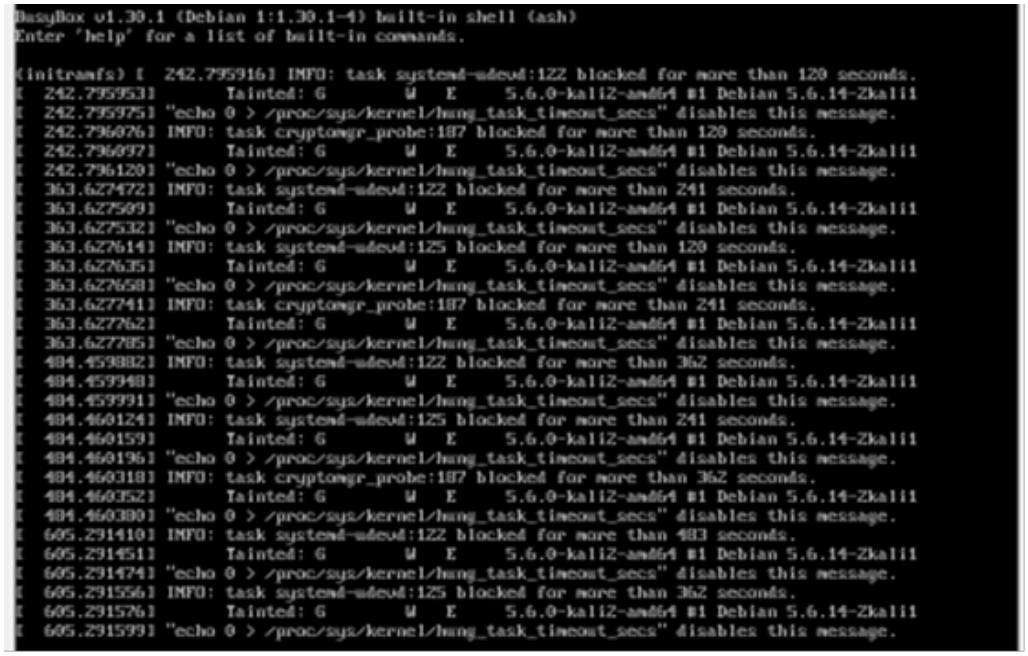
Figura 6. Entorno máquinas virtuales win 7 SE 2020 y Kali seminario.



Fuente: Elaboración propia

Paso 2: Cargar los archivos de Kali – seminario.

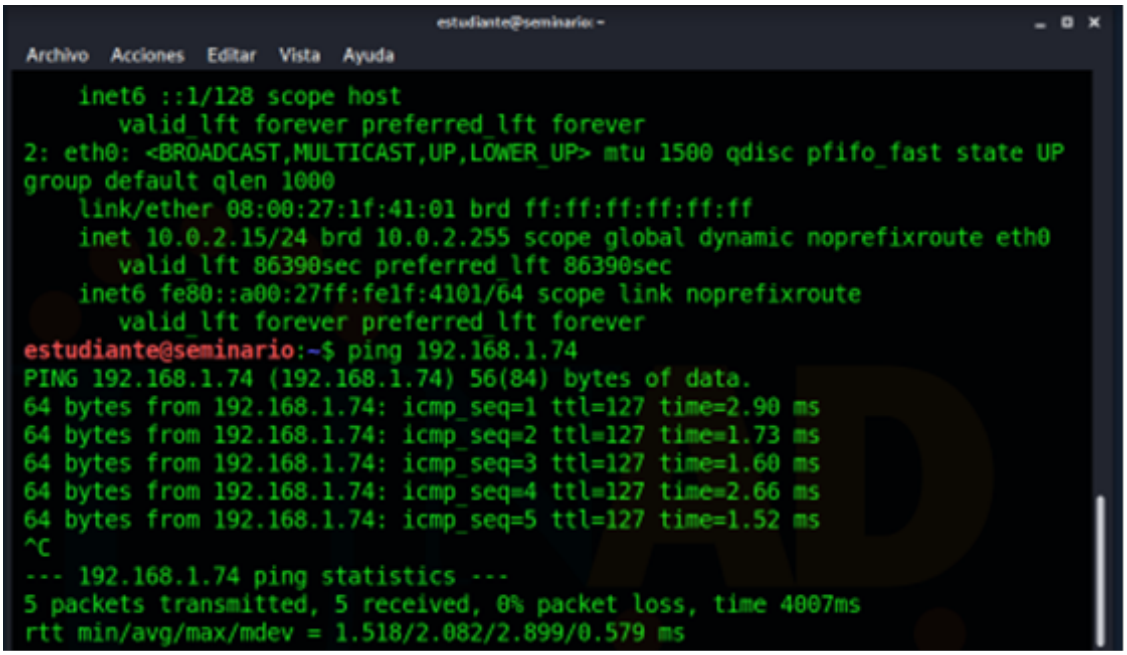
Figura 7. Cargue archivos Kali - seminario.



Fuente: Elaboración propia

Paso 3: Ping exitoso desde la maquina de Kali – seminario a la maquina win 7 – SE2020

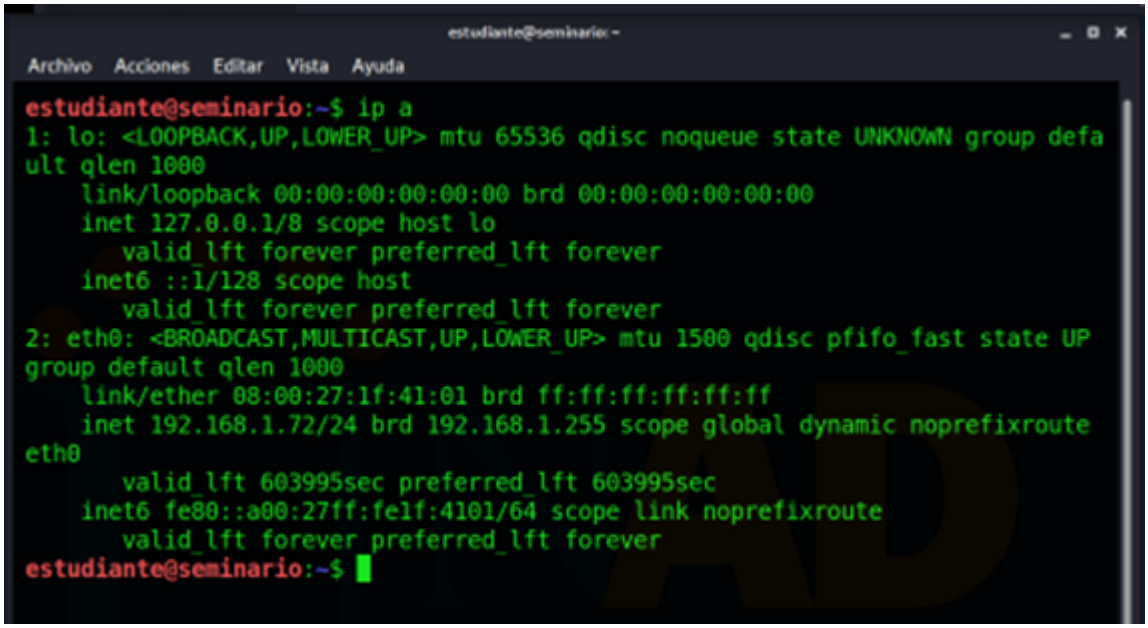
Figura 8. Conectividad entre Kali seminario y win 7 SE 2020.



Fuente: Elaboración propia

Paso 4: Configurar MODO Adaptador Puente. IP 192.168.1.72

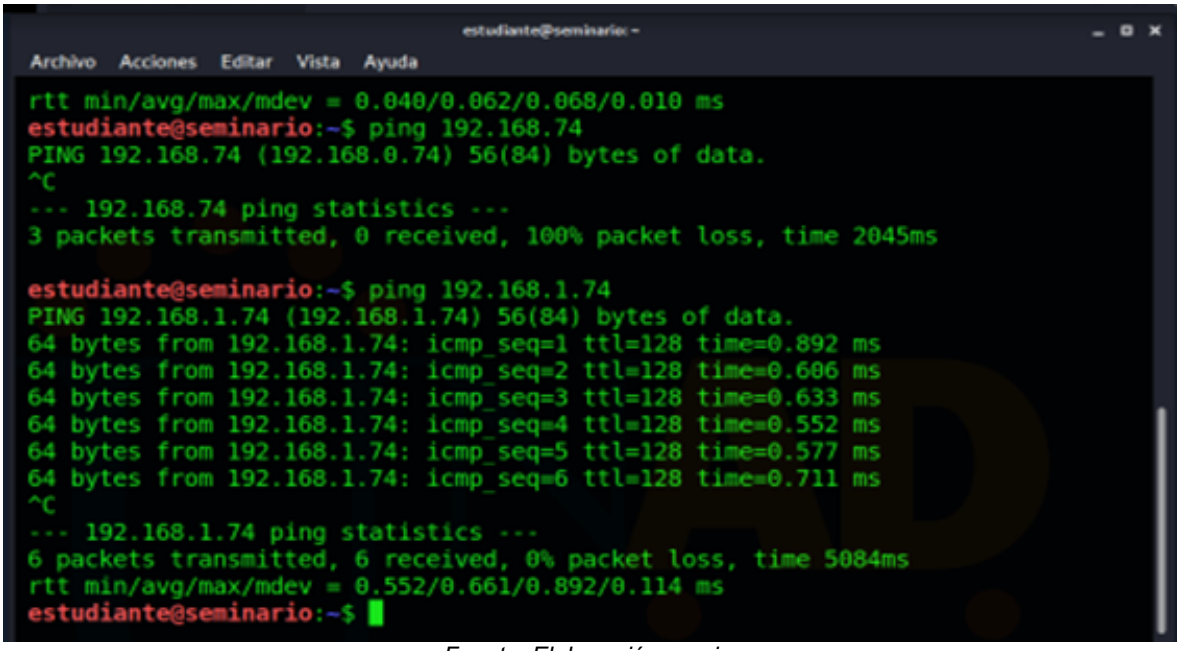
Figura 9. Dirección IP Kali seminario.



Fuente: Elaboración propia

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

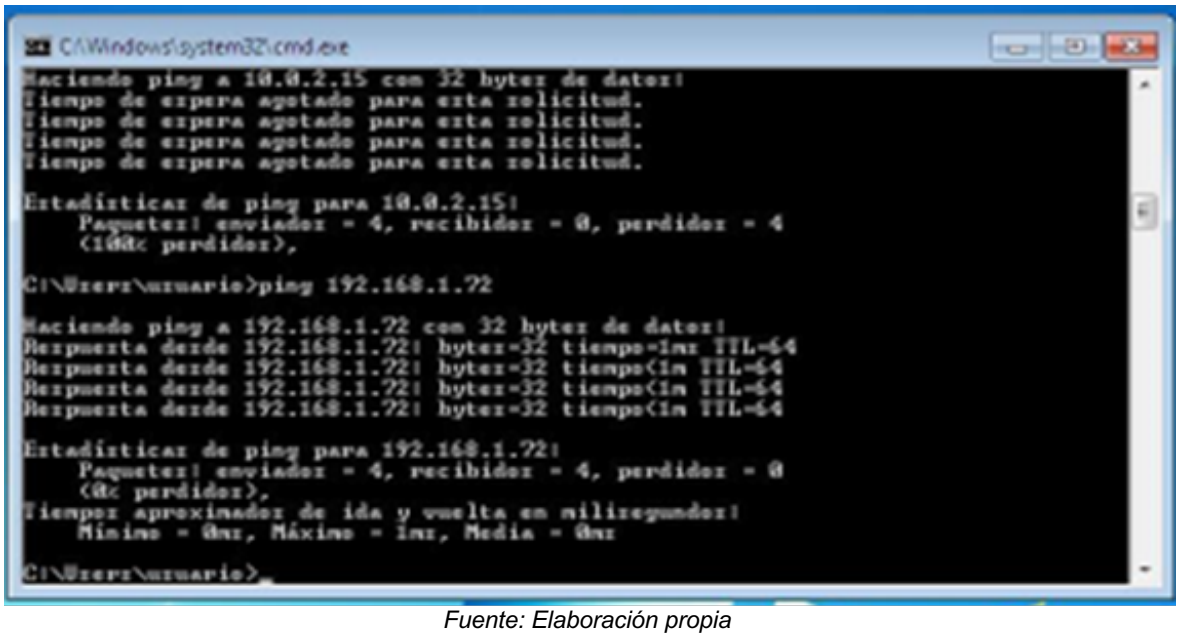
Figura 10. Conectividad win 7 SE 2020.



Fuente: Elaboración propia

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

Figura 11. Conectividad Kali seminario.



Fuente: Elaboración propia

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

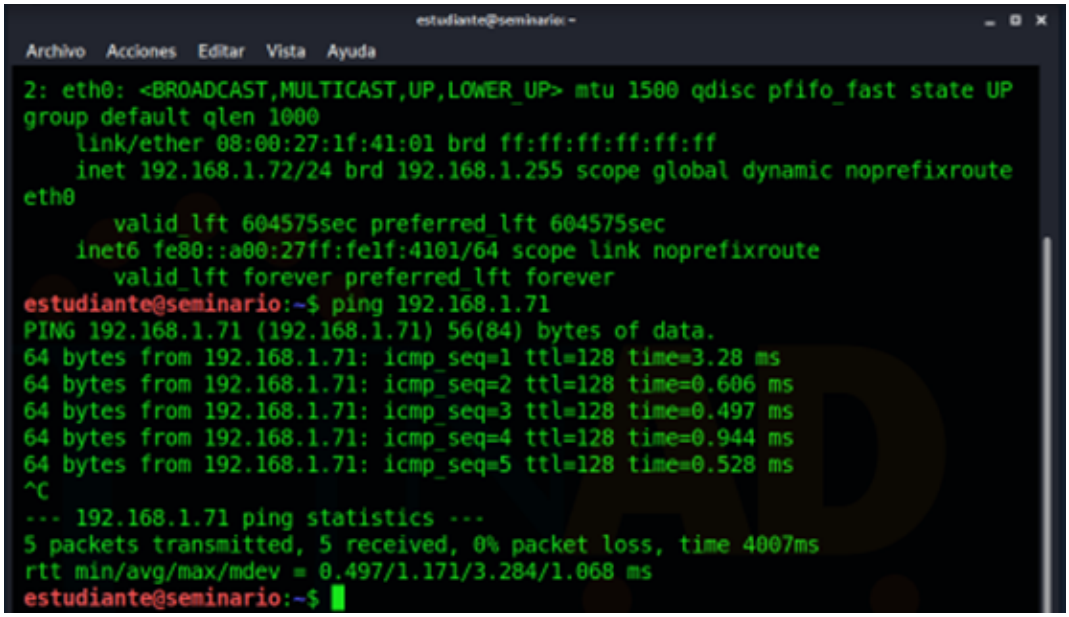
Paso 1: Activar las dos máquinas correspondientes de prueba.

Figura 12. Entorno máquinas virtuales.

Fuente: Elaboración propia

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

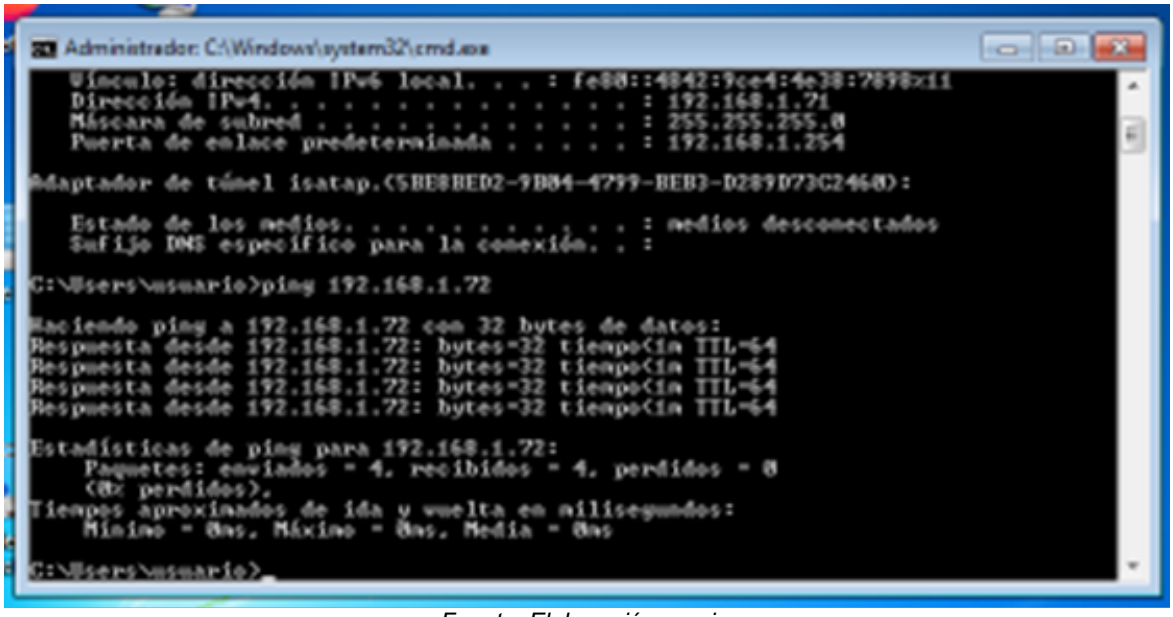
Figura 13. Conectividad win 7 SE 2020 x 64.



Fuente: Elaboración propia

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

Figura 14. Conectividad Kali seminario.



Fuente: Elaboración propia

5.2 EVALUAR LAS ACCIONES DE LOS EQUIPOS RED TEAM & BLUE TEAM DE THE WHITEHOUSE SECURITY EN EL MARCO DE LOS CRITERIOS ÉTICOS Y LEGALES.

1. **Analizar los anexos Escenario Segundo y Acuerdo con base a la legalidad y no ética.**

   En el Anexo 3 / Acuerdo, se presenta algún procedimiento ilegal y sin ética los cuales son de carácter irregular, y hace evidente que la compañía Whitehouse Security hace alguna actividad sospechosa que vulnera algunos de los artículos en la ley 1273 de 2009.

   Visualizaremos cláusulas y partes que contemplan alguna irregularidad:

   Cláusula primera: Objeto:

Acerca de los procedimientos ilegales en Whitehouse Security no deberán ser comunicados.

(Acá se especifica que el proceso ilegal que maneja la compañía no podrá ser divulgado).

Cláusula segunda: Definición de datos confidenciales:

Punto Segundo. Toda dato de la sociedad, diseños industriales, técnica, de mercado, jurídica, comercial, financiera, estratégica, patentes, de nuevas tecnologías, productos, datos secretos como "interceptar dato, modelos de utilidad, datos de chuzadas, accesos abusivos a sistemas informáticos".

(Profundiza la chuzada e interceptaciones, y acceso abusivo a la sistematización).

Cláusula Cuarta. Obligación de la posición receptora:

Punto Tercero. La no denuncia a la autoridad de ley, alguna actividad sospechosa de espionaje u otro proceso en donde se interviene la apropiación de datos sobre terceros.

(Dato de no reportar a la autoridad de ley alguna actividad sospechosa).

Punto Cuarto. La no denuncia y publicación de datos confidenciales e ilegales que se conozca, recibir o intercambiar con la eventualidad de alguna reunión sostenida.

(La no generación de algunas denuncias acerca de los datos ilegales que existan en alguna reunión).

Punto Séptimo. Responsabilidad por la mala utilización que haga algún representante de los datos confidenciales.

(Responsabilizarse por la mala utilización que realicen a los datos confidenciales algún representante que pueden ser incluso miembros de la compañía).

Punto Octavo. Responsabilizarse frente a alguna autoridad de ley competente por la autoría en la eventualidad de que cualquier dato esté en su poder dentro de un procesamiento de algo allanado.

(Responsabilizarse legalmente de los datos que estén en posesión del autor).

Punto Noveno. El receptor está en la obligación de no revelar, comunicar, transmitir, divulgación total o parcial, privada o pública, los datos confidenciales o ilegales sin el debido consentimiento documentado por medio de Whitehouse Security.

(La no divulgación de los datos ilegales sin aviso previo documentado a la compañía).

Cláusula Octava. Solución a alguna controversia:

Si los datos ilegales o confidenciales se encontraran en poder del receptor éste tiene que apoyarse de un jurídico privado y solventar ante alguna responsabilidad penal y legal a Whitehouse Security.

(La compañía no da la garantía como responsable de los datos o proceso ilegal que puede llegar a tener).

2. **Analizar cada anexo, relacionados con vulnerar la ley 1273 evidenciando alguna ilegalidad.**
Según las ilegalidades encontradas en el Anexo 3 / Acuerdo, se relacionan los artículos en la ley 1273 de 2009[1] en los que existirían vulnerabilidades:

Artículo 269A: Acceder abusivamente a un sistema de información. Cárcel de Cuarenta y Ocho meses a Noventa y Seis meses y una multa de Cien a Mil salarios mínimos mensuales legales vigentes.

Artículo 269C: Interceptar algún dato informático, condenas de cárcel desde Treinta y Seis a Setenta y Dos meses.

En mención, en el Anexo 3 / Acuerdo, de la Cláusula segunda: Definición de datos confidenciales, menciona la información secreta como chuzar, interceptar datos y accesos abusivos donde se requiere de una órden de un juzgado que al vulnerarse generará penas de carcel que son relacionadas en los artículos mencionados anteriormente.

3. **Analizar la oferta laboral, teniendo como base el revizar la posición legal y ética.**

   A pesar de que la propuesta laboral brinda un un buen salario y una contratación atractiva, luego de analizarse el Anexo 3 / Acuerdo, se da un proceso irregular lo cual no es óptimo para ser aplicado al trabajo, pues con base al código ético del Ingeniero, existen compromisos con generalidades que como lo establece COPNIA[2] en los artículos Treinta y Treinta y Dos, el profesional debe reportar los delitos, faltas del desempeño de su profesión allegando todo tipo de datos y evidencias, además de esto, recibir bonificaciones en ocasión del desempeño de la profesión que como se demuestra en la propuesta laboral están siendo aplicadas en el honorario y clase de contratación.

4. **Analizar el caso "OPERACIÓN ANDROMEDA BUGGLY" desde su situación teniendo como base los detalles de legalidad y ética.**

   Según el artículo de Enter.co[3], en la fachada Andrómeda se hicieron procederes ilícitos donde no tenía alguna clase de orden de un juzgado por interceptar alguna comunicación y uso de aplicaciones maliciosas para adquirir datos de alguna persona, y esto es un agravio de gravedad que condena la ley 1273 de 2009 en los artículos 269A, 269C, 269D, 269F y 269H. Sin embargo, eran procederes con patrocinio de las fuerzas militares y no había quien controlara legítimamente en todo lo que se hacia en ésta fachada perjudicando el código ético del cuerpo militar, a los ciudadanos y el propio gobierno.

5.3 DEMOSTRAR VULNERABILIDADES EN UN SISTEMA INFORMÁTICO A PARTIR TÉCNICAS DE INTRUSIÓN.

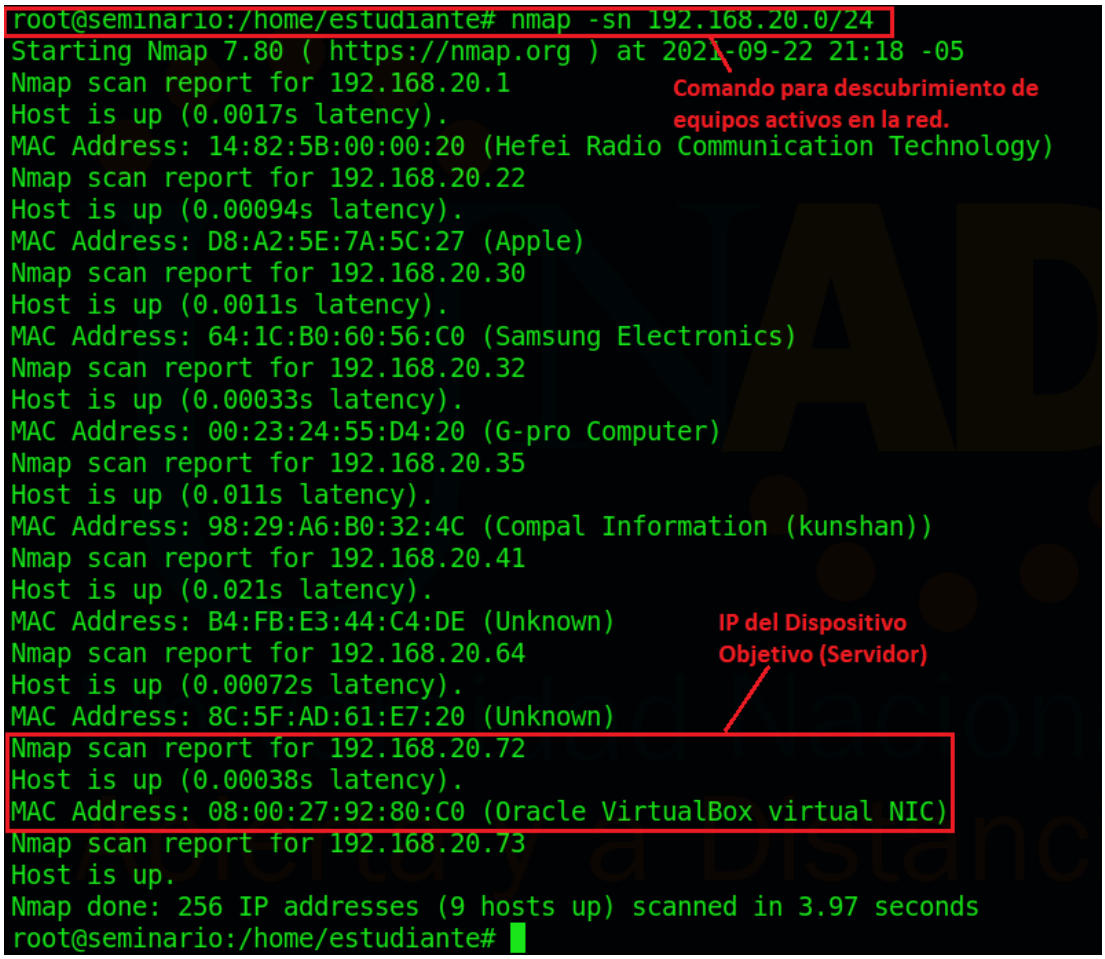
Paso Uno:

En la recolección de los datos, al observar se encuentra en el Anexo 4 / Escenario 3 se visualiza un SO antiguo y software rejetto v. 2.3 que está vulnerable.

Paso Dos:

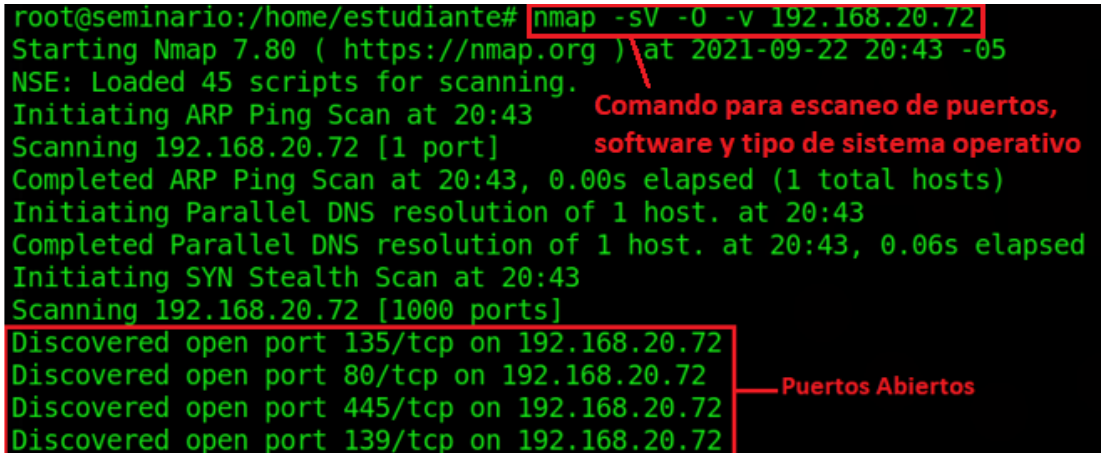
Usando KaliLinux, se encuentra y establece dispositivos activados dentro de la red por medio de la herramienta **NMAP**, y del Escáner del comando **nmap -sn 192.168.20.0/24** visualiza los dispositivos interconectados en la red y con el comando **nmap -sV -O -v** identificamos el SO, aplicación instalada bajo los puertos en apertura y versión de los objetivos. Así identificamos alguna vulnerabilidad y posibilidad de un vector de ataques. Visualizar Figuras 1, 2 y 3.

Figura 15. **Escáner local de la red.**



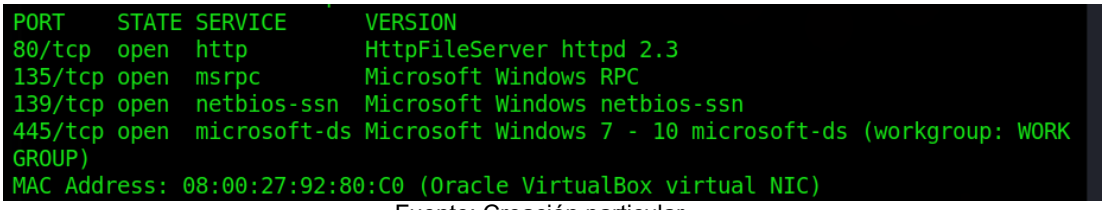
Fuente: Creación particular.

Figura 16. **Escáner software y versiones.**



Fuente: Creación particular.

Figura 17. **Cada puerto con su versión.**



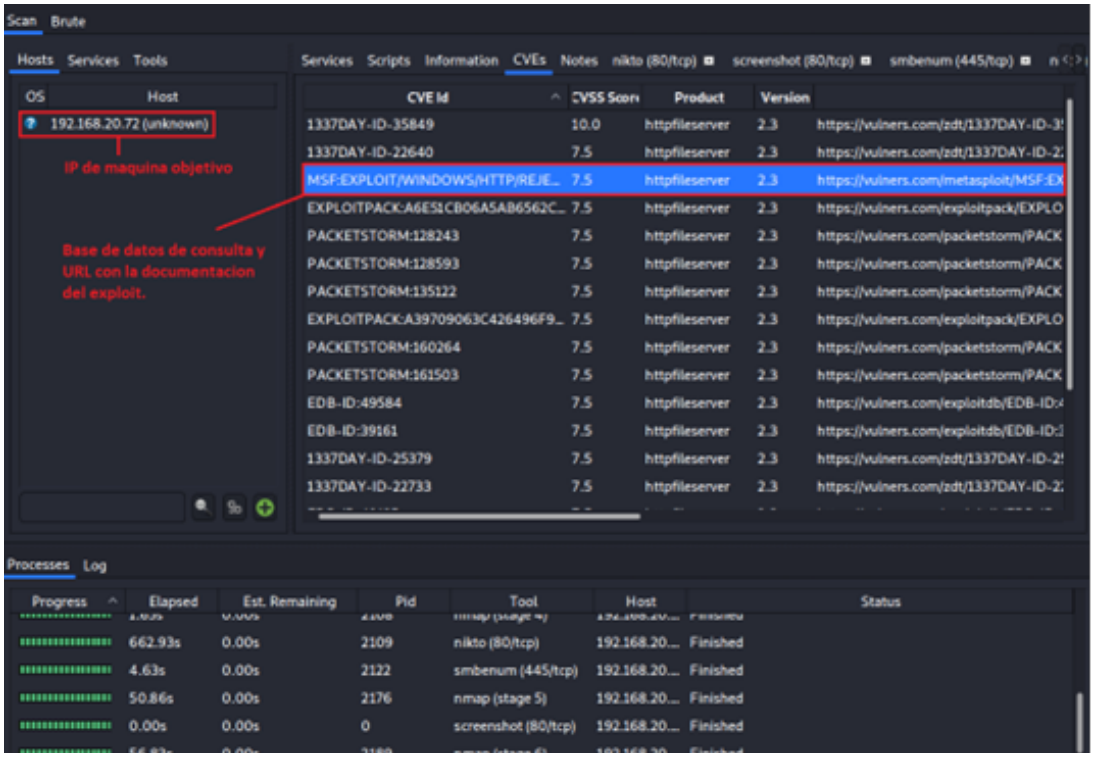
Fuente: Creación particular.

Relacionamos los datos que ayudaron a establecer la falla en la seguridad:

- Aplicación rejetto v. 2.3 el cual presenta una asociación de un exploit publicado y se indica el procedimiento acerca de cómo explotar la vulnerabilidad.
- Escape de datos, esto indica la existencia de pérdidas de datos a causa de conectividades externas.
- Al escalar los privilegios señala que hay un usuario con privilegios adecuados para establecer alguna modificación o ajuste en el sistema.
- SO Microsoft Windows 7 sufre de obsolescencia y visualiza varias vulnerables.

Usamos las herramientas NAMP y LEGION que están incorporadas dentro de Kali Linux, posteriormente realizamos el examen de alguna vulnerabilidad del objetivo en la máquina, evidenciando la falencia en la seguridad y exploit que presenta el software rejetto v.2.3.

Figura 18. **Herramienta LEGION.**



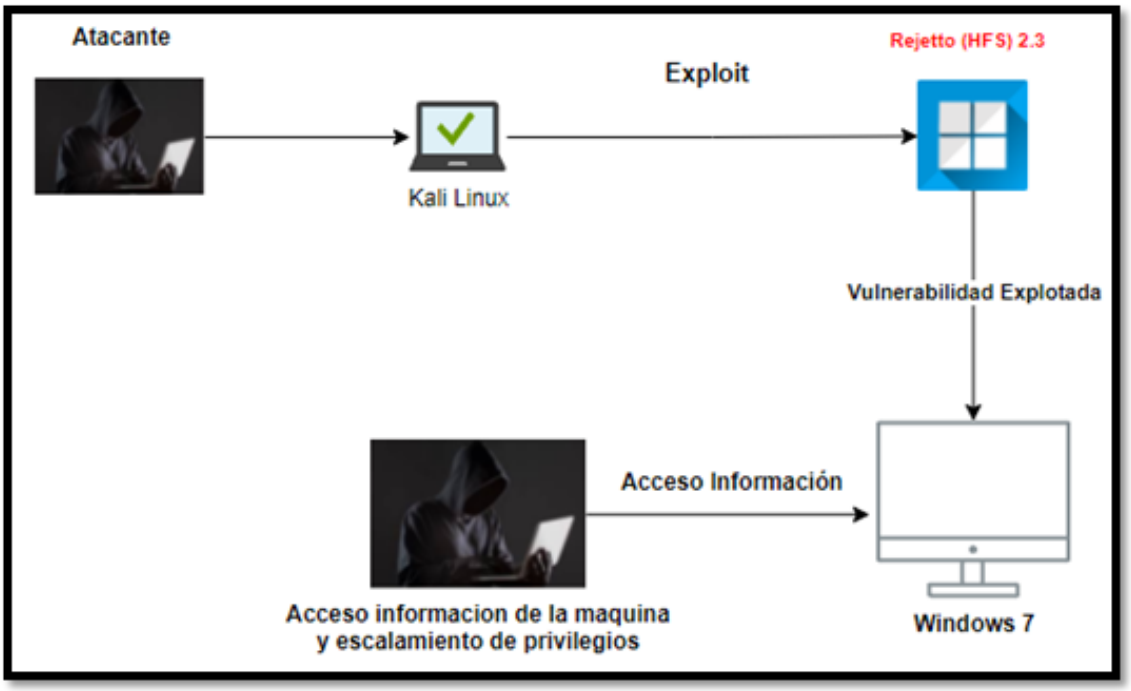
Fuente: Creación particular.

El paquete rejetto v. 2.3 utiliza el puerto 80.

Por medio del Escáner de puertos, y alguna vulnerabilidad con LEGION y NMAP, aparecen exploits dispuestos en la máquina Microsoft Windows 7 evidenciado en la Figura 4, donde se realiza la explotación por medio de Metasploit Framework con los payloads dispuestos, generando que la máquina resulte exponiéndose ante esas vulnerabilidades y exista algún aumento de privilegios al existir la posibilidad de captura de datos, ejecución de malware y keylogger.

Por medio de la Figura 5, explicamos el ataque de la vulnerabilidad descubierta en la máquina Microsoft Windows 7 / 64 bits.

Figura 19. **Esquema del atacante.**



Fuente: Creación particular.

Paso Uno.

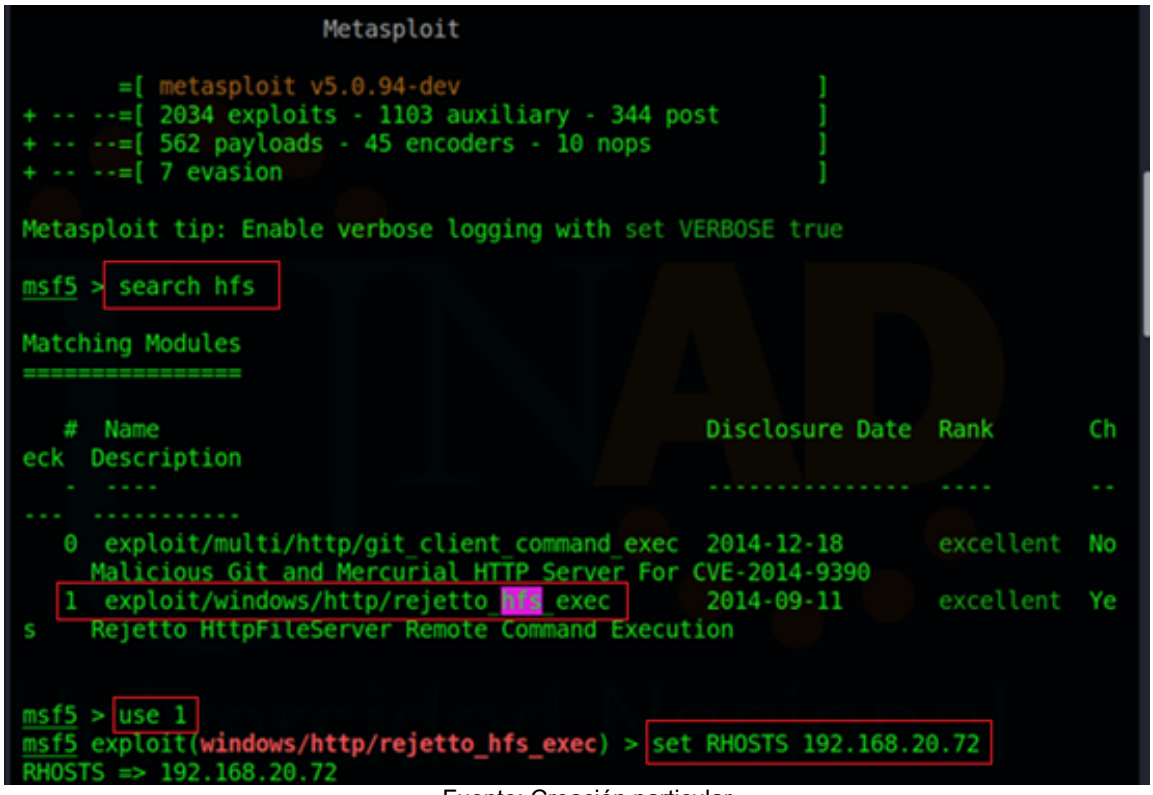
Ejecutamos el paquete Metasploit integrada dentro de Kali Linux con la que iniciamos explotar la vulnerabilidad visible.

Paso Dos.

Visualizado en la Figura 6, ejecutamos el comando **search hfs** con el fin identificar el exploit.

Luego de encontrado el exploit, lo utilizamos al ejecutar el comando **use 1** y se aplica la IP de la máquina objeto por medio del comando **set RHOST 192.168.20.72**.

Figura 20. **Comando Search hfs.**

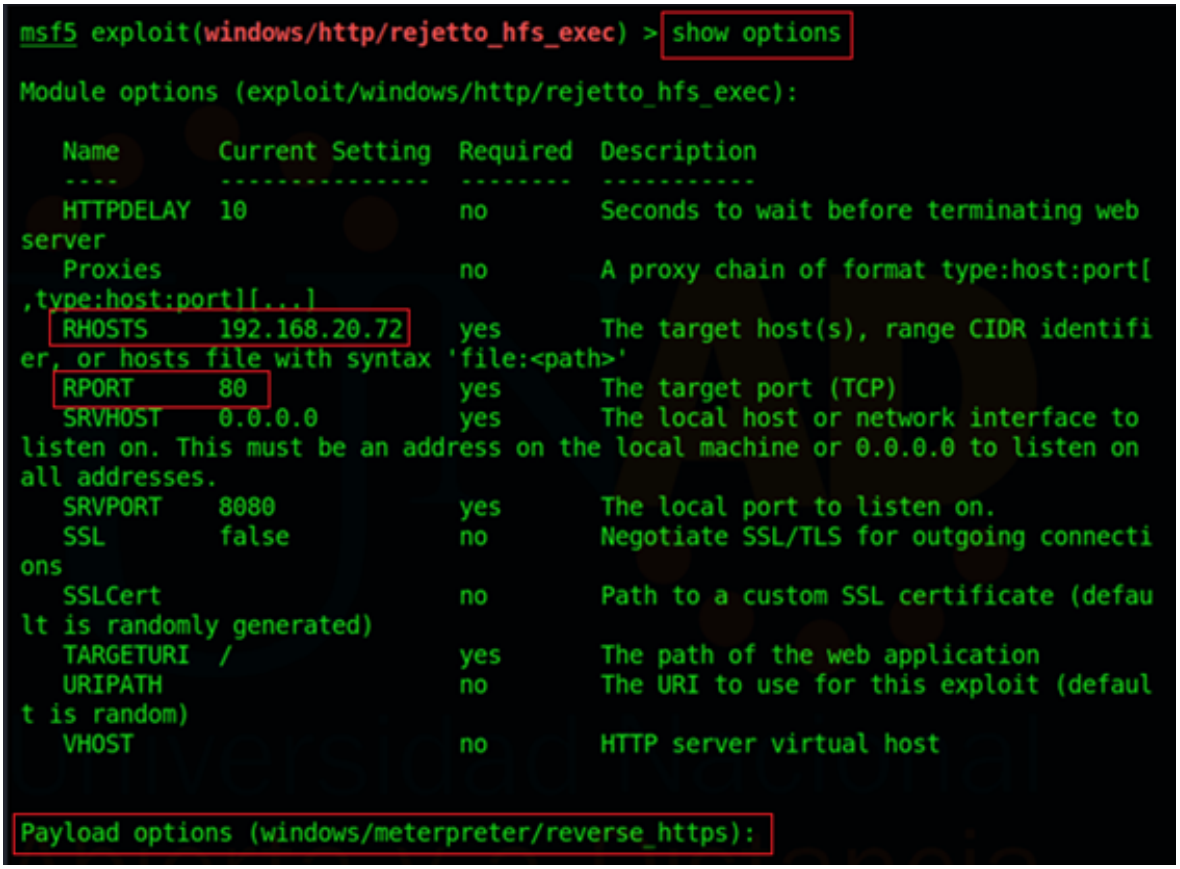


Fuente: Creación particular.

Paso Tres.

Al aplicar la IP objeto, por medio del comando **show options** se visualizan las alternativas del exploit (visualizar Figura 7).

Figura 21. **Comandos exploit.**



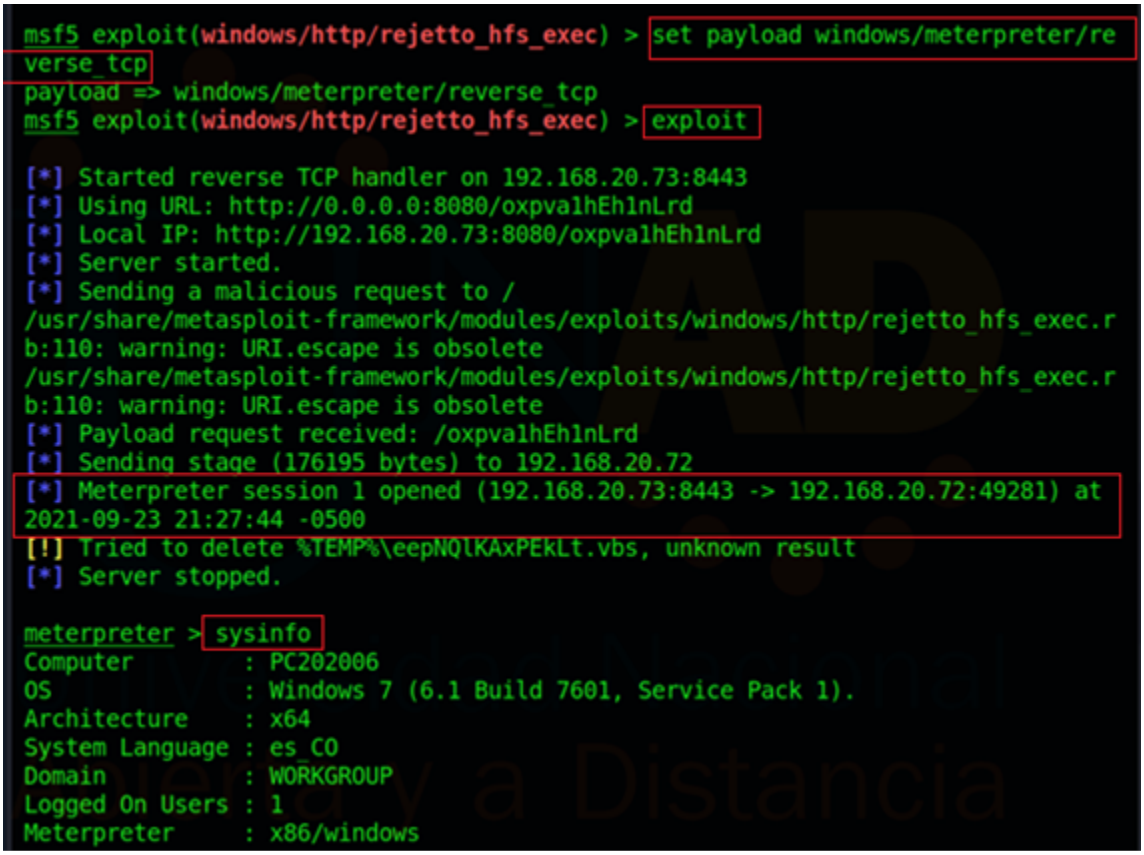
Fuente: Creación particular.

Paso Cuarto.

Cargamos el payload por medio del comando **set payload Windows/emterpreter/reverse_tcp** y ejecutamos el comando **exploit** donde iniciamos la explotación de las vulnerabilidades donde el proceder realizar aperturas de la Shell meterpreter y permite acceder a la máquina objeto. (visualizar Figura 7).

Iniciando la Shell meterpreter ejecutando el comando **sysinfo**, podemos validar que muestra datos de la máquina que explota como la clase de SO, dominio y arquitectura. (visualizar figura 7).

Figura 22. **Comandos Payload y Shell.**

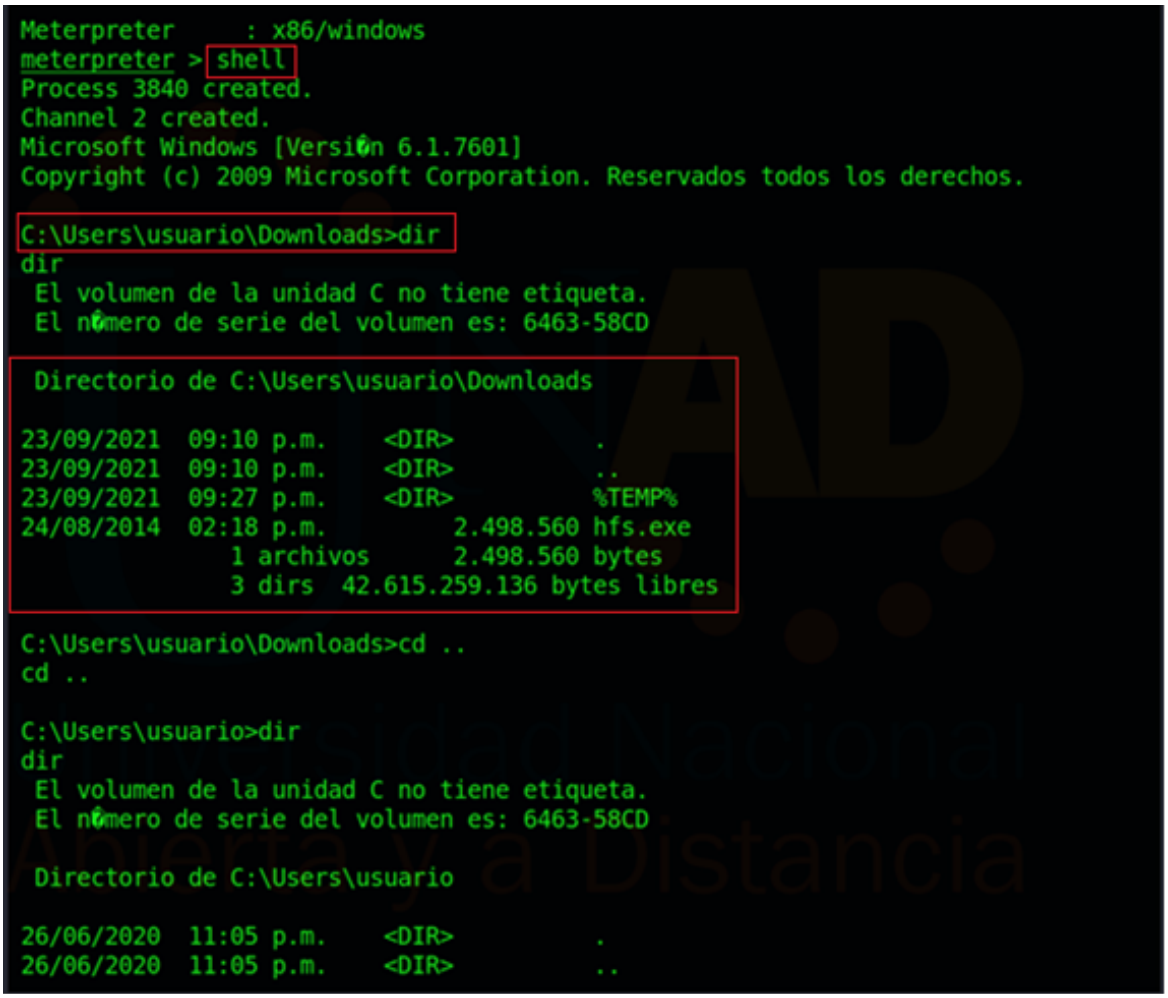


Fuente: Creación particular.

Paso Quinto.

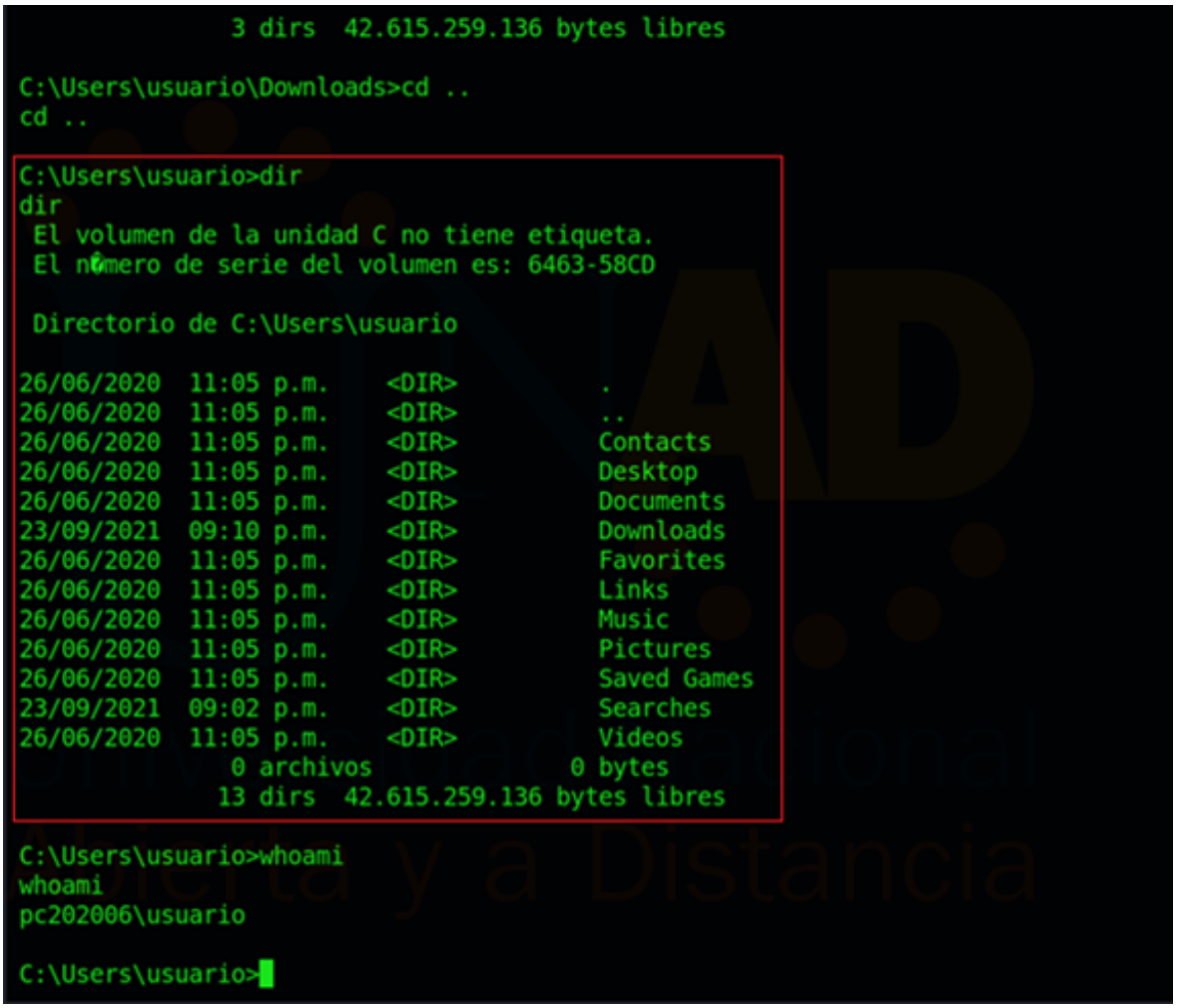
Ejecutando el comando **Shell** en meterpreter, ingresamos al terminal de comandos CMD en la máquina objeto donde podemos ejecutar algún tipo de proceder en el sistema y/o en los datos que la máquina resulte, facilitando el escape de datos. (ver Figura 8 y Figura 9).

Figura 23. **Comando Shell.**



Fuente: Creación particular.

Figura 24. **Objetivo CMD.**

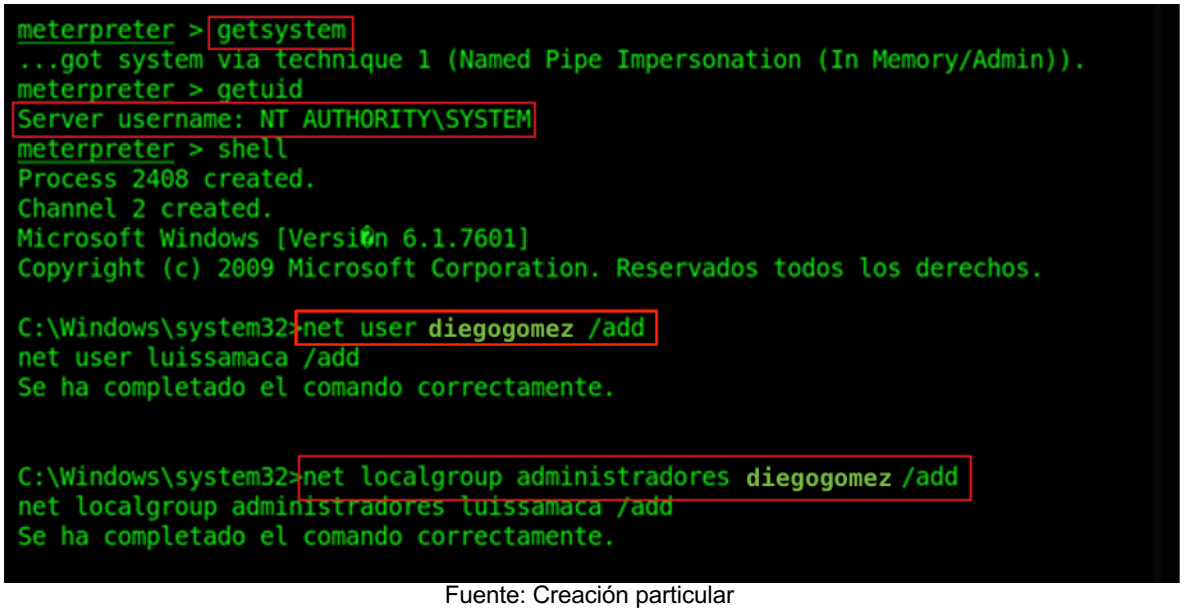


Fuente: Creación particular.

Paso Seis.

Por medio del comando **getsystem** en meterpreter, realizamos el procedimiento de escalar el privilegio para acceder bajo el usuario **NT AUTHORITY\SYSTEM** y creando el usuario **diegogomez** con el privilegio de administrador. (visualizar la Figura 10).

Figura 25. **Elevación de privilegio.**



Fuente: Creación particular

Evidenciamos el crear el usuario administrador con el escalado del privilegio. (visualizar Figura 11).

Figura 26. **Usuario administrador.**

Fuente: Creación particular

5.4 FORMULAR ESTRATEGIAS DE CONTENCIÓN MEDIANTE EL ANÁLISIS DE RIESGOS Y VULNERABILIDADES EN THE WHITEHOUSE SECURITY.

1. *¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos*.

- Evitar ataques de manera ágil haciendo escaneos, analizando y monitoreando cada dispositivo y redes internas lozalizando alguna vulnerabilidad que terminaron explotadas.
- Establecer los alcances que hubo en el ataque teniendo en cuenta cada dispositivo, equipo y software que lograron involucrarse retirándolos de las redes.
- Modificar corrigiendo alguna vulnerabilidad que fue identificada.
- Restaurar los servicios en caso de que hubiese sido afectadas la fluidez del comercio.
- Demandar por medio de la autoridad competente el delito informático.
- Sugerir alguna mejora continua para blindar de manera segura la infra-estructura.

2. *¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?*

   Se proponen las siguientes medidas con las que podemos evitar que esta clase de ataques sean repetitivos:

- Realizar actualizaciones y aplicar parches al SO hacia la versión que ofrezca la garantía de las seguridades requeridas, para esta situación, Windows 7 es un SO obsoleto debido a que no ofrece cada actualización reciente lo que hace al SO vulnerable a cualquier explotación.
- Realizar actualizaciones al software rejetto v. 2.3 hacia una versión reciente que ofrezca la garantía de seguridad para su utilización o en su lugar usar un software que de cumplimiento con iguales funciones y aplique el diagrama de seguridad eficientemente sobre actualizaciones, teniendo en cuenta que hubiese hecho una investigación cautelosa del software con la verificación con el fin de que no exista las vulnerabilidades.
- Monitorear el tráfico de las redes con el objetivo de localizar el aumento de tráfico donde se podrá evidenciar la fuga de datos.
- Eludir a los usuarios para que adquieran privilegios para realizar instalaciones de software, así se garantizaría la instalación de software de forma protocolaria y con la coordinación del responsable del departamento de las TIC.

3. *¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?*

   El BlueTeam se encargará de ofrecer proactivamente la seguridad, con el análisis y monitoreo constante de patrones no normales, ofreciendo una continua mejora para la seguridad del cimiento tecnológico con el objetivo de encontrar y proceder a algún ataque.

   El Equipo de Respuesta a Incidentes Informáticos (CSIRT) ofrece respuestas prioritarias a posibles ataques que puedan presentarse, estableciendo alguna acción reactiva y proactiva para contenerlo y acompañando el procedimiento de recuperación y restablecer el servicio en la incidencia visualizada.

4. *¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?*

   Aplicado en controles básicos tales como:

- Tipificación de alguna actividad anormal o maliciosa en las redes.
- Investigación y auditorias en los logs para la determinación y respuestas ante las posibilidades de algún ataque.
- Vigilar y catalogar el software aplicado en cada equipo de las redes con el objetivo de dar identidad a la posible instalación no autorizada por la compañía.
- En cada prueba de penetración y procedimiento de RedTeam.
- Implementación de una mejor práctica para defender ante la ciberseguridad.
- Implementación continuada ante cada vulnerabilidad.

5. *Explique y redacte las funciones y características principales de lo que es un SIEM.*

   Tal y como lo visualiza **nsit**[1], herramienta con la finalidad de descubrir, contestar y contrarrestar alguna amenaza cibernética donde su principal finalidad es la de obtener una perpectiva generalizada de todos los entornos de redes permitiéndonos la recepción de la información en tiempos reales de las actividades que presenten un peligro para la compañía.

Tiene las siguientes características primordiales:

- Seguimiento de forma central para cada amenaza potencial.

- Descubrir entre algún falso incidente y amenaza real.
- Posibilidad de brindar respuestas en tiempos reales.
- Documentación de los procesos de detecciones, resoluciones y actuaciones.
- Creación de bases de información para cada conocimiento.
- Escala cada caso o incidente al analista de seguridad correspondiente.

6. *Defina por lo menos 3 herramientas de contención de ataques informáticos "hardware o software", recuerde que las herramientas de contención son diferentes a las herramientas de detección.*

1. **Firewall Endian:**

   Cortafuegos que se basa en Linux[2] que permite solucionar, prevenir, contener y gestionar cada amenaza, que contempla funciones anti-virus, VPN y filtraje de contenidos, además, permite monitorear, registrar e informar en tiempos reales acerca de los comportamientos y la actividad de las redes equipado con una sistematización para prevenir todo intruso (IPS).

2. **ModSecurity (WAF):**

   Tal y como lo visualiza **GEEKFLARE**[3] Representa un corta fuegos de aplicativos web de open source que proporciona el proteger en contraposición a cada tipo de ataque siguiente:

   - Cross-site scripting
   - Troyanos
   - Ataque web común
   - SQL Inyección
   - Fugas de datos
   - Actividades maliciosas

3. **Snort:**

   Software de open source para contener y detectar cada intruso, posee la competencia de detención y generación para alerta de troyanos, gusanos, e intenciones de vulnerar el cortafuegos, además, avisa acerca de alguna posibilidad de escanear algún puerto en las redes o comportamiento irregular.

6 CONCLUSIONES

- Se presenta de manera precisa los resultados que se obtuvieron con el desarrollo de los objetivos propuestos. De acuerdo con los conocimientos adquiridos sobre el funcionamiento de los Equipos de respuesta Red y Blue Team, se identifica la importancia de contar con los servicios que brindan, dado que mide la seguridad de la infraestructura tecnológica de una organización y las vulnerabilidades que se pueden encontrar en ella.

- En la seguridad informática y protección de datos, entraron a participar 2 equipos fundamentales como Red team y Blue team, Unir1 da la definición que son los que tienen la labor de aplicar estrategias en ambientes con control, con el objetivo de crear sitios de ataque y defensa utilizando las diferentes técnicas y herramientas con el objetivo de localizar vulnerabilidades y así poder mitigarlos, tendiendo como fin asegurar los activos primarios de las empresas como es la información y la infraestructura de tecnología.

- Este documento presento una propuesta que especifica las funcionalidades, procesos, herramientas e informes acerca de la colaboración de los equipos Red Team & Blue Team para la detección de vulnerabilidades y asegurar la estructura de tecnología de las empresas, al consolidarse la importancia de los sitios emulados y el entrenamiento que crea para cada uno de los grupos con el objetivo de hacer frente a las amenazas, mitigando que ellas logren afectar a la empresa.

- Se encuentra que las metodologías y técnicas utilizadas por los Equipo Red Team y Blue Team brindan un gran aporte en la detección y prevención de ataques cibernéticos para las organizaciones, dado que permiten establecer

el aseguramiento de la información siguiendo las diferentes fases y procesos que se ejecutan.

- Se identifica y se hace un análisis de las herramientas utilizadas por los Equipos Red y Blue Team las cuales brindan un importante apoyo para el proceso de testeo a la infraestructura tecnológica de una organización, donde se revelan las vulnerabilidades y fallas que esta puede presentar mediante los ejercicios realizados por los equipos de ataque y defensa.

7 RECOMENDACIONES

En este caso a los usuarios, administradores y gerentes de la compañía se les recomienda:

- Que cuenten con equipos de ciberseguridad preparados para mitigar cualquier tipo de amenaza a la infraestructura tecnológica, realizando constantemente monitoreo sobre sus redes y aplicaciones.

- Que se mantengan los sistemas operativos actualizados con los últimos parches de seguridad, actualizar dispositivos obsoletos que no posean soporte y realizar pruebas periódicas de pentesting con el fin de identificar vulnerabilidades de manera proactiva.

- Garantizar a su equipo de tecnología el apoyo necesario para blindar la seguridad de su infraestructura, esto incluye la adquisición de nueva tecnología, contratación de personal capacitado y brindar entrenamientos basados en seguridad al personal de la organización con el fin de mitigar amenazas de ingeniería social.

8 BIBLIOGRAFÍA

Catoira, Fernando, “PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: EXPLOTANDO UNA VULNERABILIDAD CON METASPLOIT FRAMEWORK”. {En línea}. {07 octubre de 2021} disponible en: (https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-como-hacer.html).

Chaparro, Maria. “Legislación informática y protección de datos en Colombia, comparada con otros países”. {En línea} {07 octubre de 2021} disponible en: (file:///C:/Users/Samakinho/Downloads/1014-Texto%20del%20art%C3%ADculo-2757-1-10-20150430.pdf).

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. [Guía No 10]. (12 octubre de 2021). Seguridad y Privacidad de la Información. Guía para la preparación de las TIC para la continuidad del negocio. Bogotá, Colombia: MINTIC.p.3.

COPNIA, “Código de Ética”. {En línea}. {07 octubre de 2021} disponible en: (https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf).

CVE “CVE”. {En línea}. {06 octubre de 2021} disponible en: (https://cve.mitre.org/).

DESTINONEGOCIO “¿Cómo evitar un ciberataque en las empresas?”. {En línea}. {07 octubre de 2021} disponible en: (https://destinonegocio.com/co/gestion-co/recursos-materiales-co-co/ciberataque/).

EC-COUNCIL, Blog “RED TEAM VS BLUE TEAM”. {En línea}. {06 octubre de 2021} disponible en: (https://blog.eccouncil.org/red-team-vs-blue-team/).

ENTER.CO, “Detrás de Buggly: la historia de la fachada Andrómeda”. {En línea}. {08 octubre de 2021} disponible en: (https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/).

GEEKFLARE. (2021). 4 Firewall de aplicaciones web de código abierto para una mejor seguridad. Recuperado de https://geekflare.com/es/open-source-web-application-firewall/.

INCIBE_ “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”. {En línea}. {07 octubre de 2021} disponible en: (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian).

INFOSEC, Industries. “OpenVAS / Greenbone Community Edition”. {En línea}. {07 octubre de 2021} disponible en: (https://infosecindustries.com/vendors/greenbone/openvas-greenbone-community-edition.html).

LogRhythm. (2021). Gestión de eventos e información de seguridad (SIEM). Recuperado de https://logrhythm.com/solutions/security/siem/.

MINTIC, “Ley 1273 de 2009”. {En línea} {07 octubre de 2021} disponible en: (https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf).

NMAP, “Escáner de seguridad de Nmap”. {En línea}. {07 octubre de 2021} disponible en: (https://nmap.org/).

Revista HackingEtico, “FASES DEL PENTESTING Aprende Como Hacer Auditoria De HACKING A Empresas”. {En línea}. {07 octubre de 2021} disponible en: (https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-como-hacer.html).

SIC, “LEY 1273 DE 2009”. {En línea}. {07 octubre de 2021} disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

SGSI “ISO 27001: Vulnerabilidades de la organización”. {En línea}. {07 octubre de 2021} disponible en: (https://www.pmg-ssi.com/2015/06/iso-27001-vulnerabilidades-de-la-organizacion/#:~:text=Las%20vulnerabilidades%20pueden%20encontrase%20asociadas,%2C%20equipos%2C%20software%20o%20informaci%C3%B3n.&text=Falta%20de%20aplicaci%C3%B3n%20de%20procedimientos,Fallos%20del%20control%20interno.).

SITEL “Gestión de la seguridad Blue Team”. {En línea}. {06 octubre de 2021} disponible en: (https://www.sistel.es/business-information-security/gestion-seguridad).

Tarazona, Cesar “AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN”. {En línea}. {06 octubre de 2021} disponible en: (https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/.).

UNITEL “Seguridad Informática en las empresas. Consejos básicos”. {En línea}. {06 octubre de 2021} disponible en: (https://unitel-tc.com/seguridad-informatica-en-las-empresas-consejos/).

UNIR, universidad en internet “Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?”. {En línea}. {06 octubre de 2021} disponible en: (https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/).

9 ANEXOS

ANEXO 1. ENLACE DEL VIDEO DE LA SUSTENTACIÓN:

https://youtu.be/IEdCfuEf3MU

ANEXO 2. ENLACE DE LA PRESENTACIÓN EN DIAPOSITIVAS DE POWER POINT:

https://unadvirtualedu-my.sharepoint.com/:p:/g/personal/dagomezno_unadvirtual_edu_co/EZom-Q5c_vhNoI-VtyHUwjQBc7X7Ur3d_dwf8cm7_I9-nA?e=fTO4VS