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

KHATERIN SÁNCHEZ SÁNCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2022

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

KHATERIN SÁNCHEZ SÁNCHEZ

M.Sc. JOHN FREDDY QUINTERO
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2022

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

GLOSARIO

BLUE TEAM: Es el equipo de seguridad encargado de proteger activamente a la organización de los ataques. Realizan una vigilancia constante, analizando patrones y comportamientos quese salen de lo común tanto a nivel de sistemas y aplicaciones como de las personas, enlo relativo a la seguridad de la información . La función principal de este equipo de ciberseguridad es evaluar diversas amenazas que puedan afectar a la organización conun monitoreo constante de (red, sistema, entre otros) y proponer planes de acción para reducir riesgos.

CIBERATAQUES: Es un desarrollo intencional a sistemas informáticos, empresas y redes que dependen dela tecnología. Estos ataques utilizan código malicioso para cambiar la lógica o los datos de la computadora, lo que tiene consecuencias perjudiciales para toda la empresa. Un ciberataque puede involucrar a un equipo de élite de piratas informáticos que trabajan bajo la autorización de un estado-nación. Su propósito es crear programas que explotenfallas previamente desconocidas en el software. El propósito de los ataques cibernéticoses intentar exponer, cambiar, desestabilizar, destruir y eliminar para obtener acceso no autorizado.

RED TEAM: Realizar un proceso de simulación de los escenarios de amenazas que la organización puede enfrentar, analizar la seguridad desde la perspectiva de un atacante y proporcionarla al equipo más seguridad[1].

El equipo rojo utiliza sus propias herramientas para simular un atacante y tiene la función de explotar vulnerabilidades de seguridad y claves de seguridad en el sistema y / o aplicaciones. El Equipo Rojo es un equipo de profesionales que ataca (siempre controlado) contra los objetivos previamente definidos por el cliente en base a contratosde confidencialidad y alcance.

SEGURIDAD INFORMÁTICA: Se concentra en proteger la infraestructura informática y todo lo relacionado especialmente con la información contenida en la computadora o la información transmitida a través de la red informática para ello existen una serie de estándares, acuerdos, métodos, reglas, herramientas y leyes diseñadas para minimizar los riesgos potenciales para la infraestructura o la información. “es el proceso de prevenir y detectarel uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros

[1] UNIR revista, Red Team, Blue Team y Purple Team. [Online]. ¿Cuáles son sus funciones y diferencias? 07 de enero 2020. Consultado el 22 de octubre de 2020. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente”[2].

SEGURIDAD INFORMÁTICA: Se concentra en proteger la infraestructura informática y todo lo relacionado especialmente con la información contenida en la computadora o la información transmitida a través de la red informática para ello existen una serie de estándares, acuerdos, métodos, reglas, herramientas y leyes diseñadas para minimizar los riesgos potenciales para la infraestructura o la información. “es el proceso de prevenir y detectarel uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente”**[3]**.

VULNERABILIDADES: Es el peligro que un individuo, sistema u objeto puede sufrir frente a peligros inminentes. Una vulnerabilidad es una debilidad que puede poner en peligro toda una red y por esodeben existir los expertos en ciberseguridad para aliviar las amenazas **[4]**.

Una vulnerabilidad es una debilidad o mal funcionamiento en un sistema de información,que pone en riesgo la seguridad de la información y puede permitir que un atacante destruya su integridad, disponibilidad o confidencialidad, por lo que es necesario encontrarlos y eliminarlos lo antes posible.

---

[2] Universidad Nacional de Valencia. ¿Qué es la seguridad informática y cómo puede ayudarme? [Online]. CIENCIA Y TECNOLOGÍA. 21 marzo 2018. Consultado el 22 de octubre de 2020. Disponible en Internet: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

[3] Universidad Nacional de Valencia. ¿Qué es la seguridad informática y cómo puede ayudarme? [Online]. CIENCIA Y TECNOLOGÍA. 21 marzo 2018. Consultado el 22 de octubre de 2020. Disponible en Internet: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

[4] Campus de Ciberseguridad. Tipos de vulnerabilidades en ciberseguridad. [Online]. Los tipos de vulnerabilidades. noviembre 27 2015. Consultado el 22 de octubre de 2020. Disponible en: https://www.campusciberseguridad.com/blog/item/118-tipos-de-vulnerabilidades-en-ciberseguridad

RESUMEN

El presente trabajo consiste sobre los equipos de ciberseguridad Red Team y Blue Team en la prevención de ataques informáticos en las organizaciones privadas de Colombia. Cuando hablamos de seguridad informática y protección de datos se utilizan dos equiposfundamentales el equipo rojo y el equipo azul, ambos realizan un trabajo complementario para detectar vulnerabilidades y sobre todo emular escenarios de amenaza. Es importante que las organizaciones privadas colombianas sin importar su tamaño o naturaleza jurídica cuenten con equipos de ciberseguridad Red Team y Blue Team que faciliten la implementación de procedimientos de revisión técnica por parte de controladores y seguridad de la información de esta misma.

En la actualidad el impacto en las organizaciones colombianas tras sufrir ciberataques se extiende en la parte económica con la perdida de activos financieros, afecta su productividad, existe perdida de información privilegiada y data sensible. Comprender losriesgos asociados con la ciberdelincuencia a los que están expuestas las organizacionesprivadas colombianas día a día hacen relevante el trabajo de los equipos de ciberseguridad Red Team y Blue Team de los cuales estudiaremos.

Por consiguiente, se hace evidente comprender la importante del comportamiento de losequipos de ciberseguridad red y Blue Team. El equipo rojo es responsable de analizar y determinar el nivel de preparación de las empresas de Colombia ante posibles ciberataques y realizar pruebas de penetración contra estos objetivos. Al encontrar vulnerabilidades en el sistema, el equipo azul es el responsable de implementar métodosde prevención contra ataques dirigidos y pérdida de información.

Mediante el uso de red y Blue Team se busca identificar las principales vulnerabilidades de cada una de las empresas colombianas para comprender e inferir la ruta del atacante. El propósito es delinear una serie de medidas preventivas a través de un plan de acciónpara mitigar riesgos y vulnerabilidades en la infraestructura de TI de la empresa Colombia.

INTRODUCCIÓN

La ciberseguridad debe ser una prioridad para todas las organizaciones privadas colombianas y más en estos momentos que la transformación digital está en constante evolución. Esta situación hace necesario realizar análisis de las principales amenazas y vulnerabilidad a las que se encuentran expuestas las organizaciones en Colombia, pues el desconocimiento y la falta de ciberseguridad hacen más vulnerables los sistemas y danopción a los siguientes delitos como estafas, falsificación de identidad, phishing y ataques más elaborados con un grado técnico muy alto.

El continuo desarrollo de la tecnología informática y el continuo desarrollo de Internet hahecho posible que personas y organizaciones contraten un equipo de expertos en pruebas de penetración para analizar las vulnerabilidades en sus instalaciones y sistemasinformáticos para asegurar la integridad confidencialidad disponibilidad de la información, lo que aumenta la productividad y la competitividad empresarial en general.

En la presente actividad se debe presentar un informe técnico donde relacione los aspectos relevantes del desarrollo de las actividades anteriores y plantee recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por Red Team y Blue Team.

OBJETIVOS

1.1 OBJETIVOS GENERAL

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

1.2 OBJETIVOS ESPECÍFICOS

- Evaluar las acciones de los equipos Red Team y Blue Team de una organizaciónen el marco de los criterios éticos y legales.

- Integrar las acciones de los equipos Red Team y Blue Team de una organizaciónen el marco de los criterios éticos y legales.

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

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

2 DESARROLLO DEL TRABAJO ETAPA 1

2.1 Conceptos equipos de seguridad

La actividad consiste en:

De manera individual usted deberá consultar y dar respuesta a las preguntas orientadorasteniendo en cuenta los siguientes pasos:

- Consultar
- Leer
- Comprender
- Redactar
- Citar
- Referenciar

Una vez tenga en cuenta los pasos indicados anteriormente debe responder los siguientes puntos de manera argumentativa:

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

Colombia es un país que poco a poco ha ido evolucionando en temas tecnológicos de igual manera en normatividad sobre delitos informáticos sin embargo en relación al desarrollo del margen legal en Colombia en pro de defender la confidencialidad, integridad y disponibilidad de los sistemas informáticos esta falta mucho por regular y hacer cumplir.

Algunos elementos importantes en base a la protección de datos personales tenemos lassiguientes leyes y decretos:

2.2 LEY 1273 DE 2009

“Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las Tecnologías de la información y las comunicaciones, entre otras disposiciones.”[5]

[5] COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones Ley 1341 de 2009 [Online]. MINTIC, julio 30 del 2009. Consultado el 10 de febrero de 2022. Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913 11

Artículo 269A: Uso indebido del acceso a los sistemas informáticos. Cualquier persona, no autorizada o fuera de convenio, que tenga acceso, en todo o en parte, a un sistema informático protegido o no seguro, o que permanezca en él contra la voluntad de cualquiera que tenga derecho a excluirlo.

Artículo 269B: Obstrucción ilícita de sistemas informáticos o redes de telecomunicaciones. Impedir o dificultar el funcionamiento o normal acceso a los sistemas informáticos, datos informáticos contenidos en los mismos o redes de telecomunicaciones, sin autorización para ello.

Artículo 269C: Intercepción de datos informáticos. La interceptación de datos informáticos, o las radiaciones electromagnéticas que emanan del sistema informático que los transmite, sinorden judicial previa, dentro del origen, destino o sistema informático de los datos informáticos.

Artículo 269D: Daños informáticos. El que destruya, dañe, borre, deteriore, altere o suprima datos informáticos o sistemas de procesamiento de información o sus partes lógicas o componentes sin autorización

Artículo 269E: La persona que produzca, transporte, obtenga, distribuya, venda, envíe, introduzca o extraiga malware u otros programas informáticos con efectos nocivosdentro del territorio del país sin autorización.

Artículo 269F: Violación de Datos Personales. Quien, sin tener derecho a ello, obtenga, recopile, sustraiga, ofrezca, venda, permute, envíe, compre, intercepte, divulgue, modifique o utilice claves personales, contenidas en documentos, archivos, bases de datos o medios análogos.

Artículo 269G: Suplantación de identidad en un sitio web para obtener datos personales. Quien diseñe, desarrolle, transmita, venda, ejecute, programe o envíe páginas electrónicas, enlaces o pop-ups con fines ilícitos y sin derecho a ello.

Artículo 269H: Pena aumentada: Las penas impuestas conforme a las disposiciones de este título se incrementarán de la mitad a las tres cuartas partes.

Artículo 269I: Robo por medios informáticos y similares. El que vulnere las medidas de seguridad informática manipulando sistemas informáticos, redes de sistemas electrónicos y realizando los actos previstos.

Artículo 269J: Transferencia involuntaria de bienes. Cualquier persona con ánimo de lucro y utilizando cualquier operación informática o medio similar para transferir cualquier activo sin consentimiento en perjuicio de un tercero.

2.3 LEY 527 DE 1999

La misma fue firmada y expedida en la república de Colombia en el año 1999 el 18 de agosto la cual trata sobre la reglamentación del acceso y uso de datos, comercio electrónico y firmas digitales por último se estableció cuáles serán las entidades certificadas para tales fines y otras disposiciones.

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, también del comercio electrónico, de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

2.4 LEY 962 DE 2005

Fue expedida en la república de Colombia el día 8 de julio del 2005, por medio de la cual se establecieron disposiciones legales en base a los trámites administrativos de los organismos y entidades del Estado particularmente para los que son funcionarios públicos.

2.5 LEY 1341 DE 2009

Fue expedida en la República de Colombia el día 30 de julio del 2009, "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones[6]."

2.6 LEY 1581 DE OCTUBRE 17 DE 2012

Fue expedida en la república de Colombia del día 17 de octubre del año 2012, pormedio de la cual se prohíbe la trasferencia de datos a países que no tiene regulados la protección de datos. "Esta prohibición **NO** REGIRÁ cuando se trate de: Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia."

2.7 DECRETO 1377 DE 2013

Fue expedido en la República de Colombia el año 2013, "Por el cual se reglamentaparcialmente la Ley 1581 de 2012"[7] tiene por objeto "(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y

[6] COLOMBIA. Secretaría General de Bogotá. Ley 1341 de 2009 (30 de julio del 2009). [Online]. Consultado el 10 de febrero de 2022. Disponible en: https://secretariageneral.gov.co/transparencia/normatividad/normatividad/ley-1341-2009

[7] COLOMBIA. Función Pública. Decreto 1377 de 2013 (26 de junio 2013). Consultado el 28 de noviembre de 2020. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, ylos demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma[8]".

2.8 Documento COMPES 3854 política nacional de seguridad digital

La política nacional de seguridad digital, objeto de este documento, cambia el enfoque tradicional al incluir la GESTIÓN DEL RIESGO como uno de los elementos más importantes para abordar la seguridad digital. Las estrategias para alcanzar su objetivo principal son: fortalecer las capacidades de las múltiples partes interesadas, para: • Identificar • Gestionar • Tratar • Mitigar los riesgos deseguridad digital en sus actividades socioeconómicas en el entorno digital[9]."

"El documento incluye un diagnóstico de la situación del país en el que se exponen las debilidades en seguridad digital y se definen los objetivos de la Política propuesta. Además, se incluye un Plan de Acción a corto plazo para implementar en los próximos dos años con actuaciones concretas para: (i) fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado; (ii) actualizar el marco de gobernanza en materia de seguridad digital y (iii) analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías para preparar al país a los desafíos de la llamada Cuarta RevoluciónIndustrial".[10]

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutarde forma organizada lo que se conoce como pruebas de penetración o pentesting;usted como futuro experto deberá redactar con sus palabras y definir cada una delas etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

"Un test de penetración por lo general es una acción acordada entre un pentester y una empresa o individual que desea tener sus sistemas informáticos puestos a prueba para identificar y posteriormente corregir posibles vulnerabilidades y los

[8] COLOMBIA. Función Pública. Decreto 1377 de 2013 (26 de junio 2013). Consultado el 28 de noviembre de 2020. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[9] JARAMILLO, Alejandro. CONPES 3854 copyright © 2016, fireeye, inc. all rights reserved. de la protección reactiva a la respuesta proactiva junto a fireeye. [en línea]. 2014 Consultado: 01 de octubre de 2021. Disponible en internet: https://www.minambiente.gov.co/images/tecnologias-de-la- informacion-y-comunicacion/pdf/conpes_3854_politica_nacional_seguriad_digital.pdf

[10] PROGRESO. Confianza y Seguridad Digital. Documento CONPES 3995 Consejo Nacional de Política Económica y Social (CONPES) [en línea]. Consultado: 01 de octubre de 2021. Disponible en internet: http://www.fundacionmicrofinanzasbbva.org/revistaprogreso/confianza-seguridad- digital-documento-conpes-3995/

peligros asociados a las mismas. Esta auditoría representa para el cliente una importante fuente de información ya que el pentester actuará como un atacante proporcionando información desde un punto de vista totalmente diferente al que el propio equipo de IT de la empresa (en caso que no se realicen tests de penetración) pueda aportar.

El objetivo del test de penetración variará de cliente en cliente, se puede pedir al pentester comprobar una aplicación web, intentar ejecutar ataques de ingeniería social, actuar como un atacante interno, comprobar los sistemas físicos de seguridad en la oficina, etc. Normalmente cualquier test de penetración se debe efectuar siguiendo unos pasos predeterminados para poder presentar finalmente unos buenos resultados, estos pueden variar en cierta medida dependiendo del auditor pero generalmente vienen a ser los siguientes.[11]

2.9 FASES DE UN TEST DE PENETRACIÓN

2.9.1 Fase 1 Contacto

En esta fase inicial, el cliente debe acordar de qué se tratará la prueba de penetración, cuál es el objetivo de la prueba de penetración, cuáles son los servicios críticos de la empresa y qué problemas mayores pueden surgir en caso de un ataque.

2.9.2 Fase 2 de recolección de información

Recopilación de información en esta fase de pruebas de penetración, se trabaja en obtener toda la información posible sobre la empresa a través de arañas y escáner para comprender los sistemas y programas que se están ejecutando. La actividad de un empleado en la red social de una empresa también puede revelar los sistemas que utiliza, el correo electrónico y más.

Se explica al cliente los tipos de test de penetración: Black box Gray, Box White box

2.9.2.1 Auditoría caja negra

La "caja negra" se denomina auditoría de seguridad o prueba de penetración,

[11] CYBERSEGURIDAD.NET. Las fases de un test de penetración (Pentest) (Pentesting I) [en línea]. 23 agosto 2015 Consultado: 11 de febrero de 2022. Disponible en internet: https://www.cyberseguridad.net/las-fases-de-un-test-de-penetracion-pentest-pentesting-i

en la que el auditor no comprende la infraestructura técnica subyacente. Este control de seguridades muy adecuado para simular ataques de personas ajenas a la organización y comprender el alcance de los ataques. En este tipo de revisión de seguridad el equipo auditor tampoco tiene usuarios previos para interactuar con la aplicación a analizar. El equipo de analistas debe recopilar información sobre la plataforma en este tipo de trabajopara poder elaborar el plan de ataque más razonable.

2.9.2.2 Auditoría caja blanca

Esta es una auditoría de seguridad más completa. Entre ellos, proporciona información técnica sobre el activo a auditar, incluida información que depende del activo que se analiza, como usuarios, contraseñas y mecanismos de seguridad existentes. Con este método, el auditor no necesita gastar energía adicional para buscar información, pero puede concentrarse en aquellos elementos que son críticos para su negocio.

El propósito es proteger la plataforma de ataques más sofisticados, brindar mayor protección a la plataforma contra atacantes que tienen más recursos o por la criticidad dela información que manejan.

2.9.2.3 Auditoría caja gris

Esta es una auditoría que mezcla las características de las dos primeras. Puede ser la mejor auditoría porque se simula el ataque y se obtiene un mejor código para nuestra aplicación. Parte de la información se puede informar al auditor y pedirle que intente "escalar" Para el resto del sistema, también puedes intentar iniciar esta prueba desde múltiples puntos, estas pruebas incluyen red interna, red externa, Wi-Fi, puesto de empleado, extranet, etc.

2.9.3 Fase 3 de modelado de amenaza

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

Los métodos más comunes son: Google Hacking, Osint, Doxing.

2.9.4 Fase 4 de Análisis de vulnerabilidades

Fase de análisis de vulnerabilidad, en este punto, se debe evaluar el éxito probable de laestrategia de penetración mediante la identificación proactiva de

vulnerabilidades. Es en este momento que se revela el poder del probador de penetración debido a su creatividad.

2.9.5 Fase 5 de Explotación

Etapa de desarrollo, es hora de intentar acceder al sistema objetivo de la prueba de penetración, para ello se realiza un exploit contra las vulnerabilidades identificadas en la etapa anterior, o simplemente se utiliza las credenciales obtenidas para acceder al sistema.

A continuación, relaciona las algunas herramientas con las que se realiza la explotación de un sistema informático: Aircrack-ng, THC Hydra, Netcat, Nmap, Nessus, WireShark, Snort, Kismet Wireless.

2.9.6 Fase 6 de Post-Explotación

Fase de post-desarrollo, una vez que se ingrese al sistema del cliente, comienza la etapaen la que se debe demostrar qué significa esta brecha de seguridad para el cliente. Acceder a una computadora vieja que ni siquiera es parte de un dominio no es lo mismoque ir directamente a un DC.

2.9.7 Fase 7 de Informe

Fase de Informe final, se debe presentar los resultados de la auditoría al cliente para quecomprenda la gravedad del riesgo que representan las vulnerabilidades descubiertas ensu empresa u organización, destacando los puntos donde la seguridad se ha implementado correctamente.

2.10 LAS HERRAMIENTAS DE CIBERSEGURIDAD

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

2.10.1 Metasploit

Es una herramienta desarrollada en Perl y Ruby y se enfoca en auditar, sin embargo, la seguridad también se utiliza con fines maliciosos por los ciberdelincuentes, esta herramienta tiene muchas vulnerabilidades y se utiliza vulnerabilidades conocidas en las que los módulos se denominan cargas útiles es el código que explota la vulnerabilidad. tiene otros módulos llamados codificadores, que contienen la evasión de antivirus o sistema de seguridad. Además, permite la interacción con otras herramientas como Nmap.

2.10.2 Nmap

Esta es una herramienta de código abierto para explorar la red y realizar auditorías, esta herramienta utiliza paquetes IP para determinar qué equipos están disponible en la web. Con esta herramienta es posible determinar servicios, como el nombre y versión de la aplicación, sistema operativo y tipo de cortafuegos en ejecución.

2.10.3 OpenVas

Open Vulnerability Assessment Scanner, es un framework, es una herramienta de escaneo de vulnerabilidades que puede detectar diferentes tipos de problema es de bajo riesgo para el usuario.

Ofrece un gran número de servicios y herramientas, con las cuales se obtiene unabuena alternativa para el escaneo y gestión de vulnerabilidades; tiene la potencialde examinar múltiples protocolos de internet e industriales, de alto y bajo nivel.

2.10.4 ExploitDB

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

2.10.5 CVE

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

Las advertencias de seguridad que emiten los proveedores y los investigadores casi siempre mencionan al menos uno de estos identificadores. Los CVE permiten que los especialistas en TI coordinen sus iniciativas para priorizar y solucionar los puntosvulnerables, a fin de reforzar la seguridad de los sistemas informáticos.”[12]

2.11 INSTALACION Y CONFIGURACION DEL “BANCO DE TRABAJO”

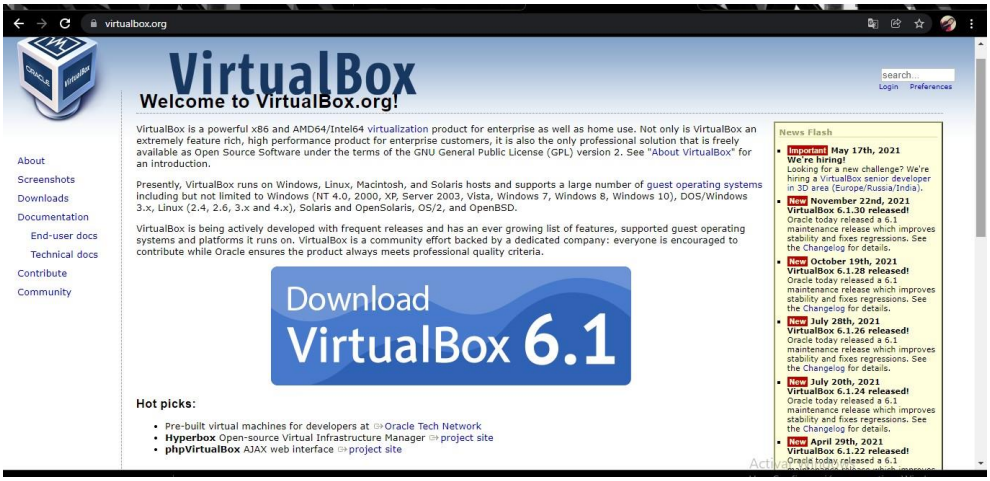
Para finalizar esta actividad es importante que se reconozca, analice y configure el “banco de trabajo”, lo solicitado en el anexo 1 Escenario 1 sobre el cual deberá

[12] RED HAT. El concepto de CVE. [On line]. 25 noviembre 2020. Consultado: 11 de febrero de 2022. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo escenario 1 es lo siguiente:

Paso A: descargar la herramienta virtualizadora “VirtualBox” en su última versión.

Figura 1. Descarga Máquina Virtual

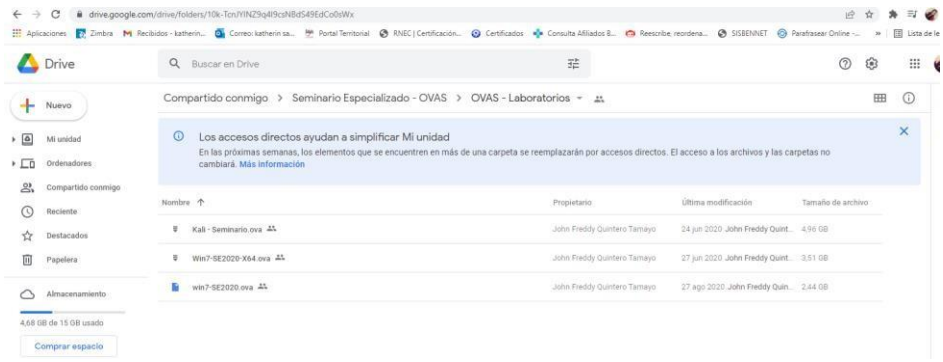


Fuente: propia

Paso B: una vez se realice apertura del foro para el desarrollo dela actividad se procederáa compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, lasimágenes en formato. OVA las cuales se encuentran ya preconFiguradas para serutilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un Windows 7 X86, un Windows 7 X64, un Kali Linux.

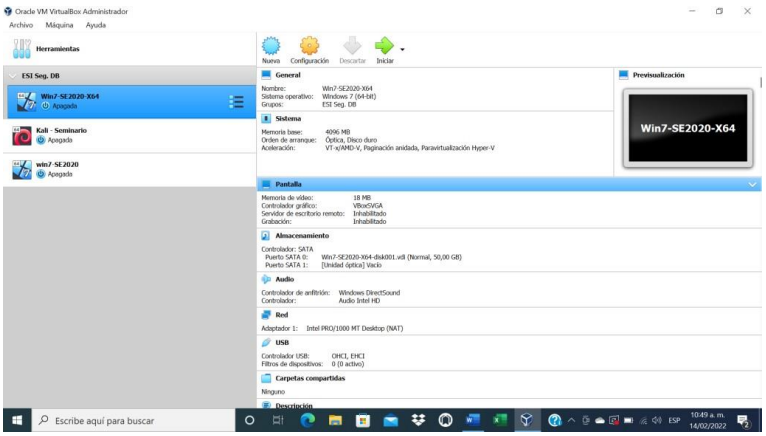
Como se indicó en la guía el tutor nos comparte un drive con las OVAS preconFiguradasde Un Windows 7 X86, un Windows 7 X64, un Kali Linux. https://drive.google.com/drive/folders/10k-TcnJYINZ9q4I9csNBdS49EdCo0sWx

Figura 2. Descarga de OVAS



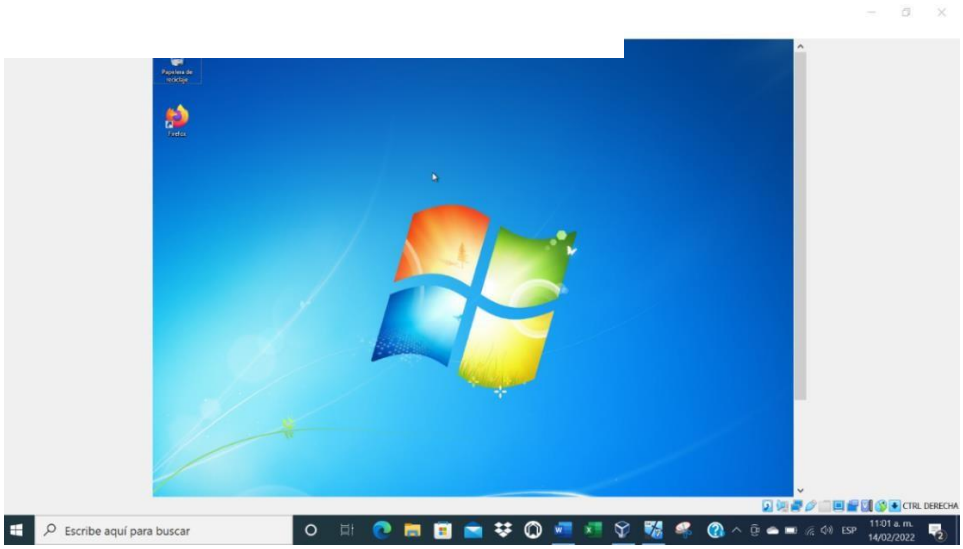
Fuente: propia

Figura 3. Instalación de OVAS



Fuente: propia

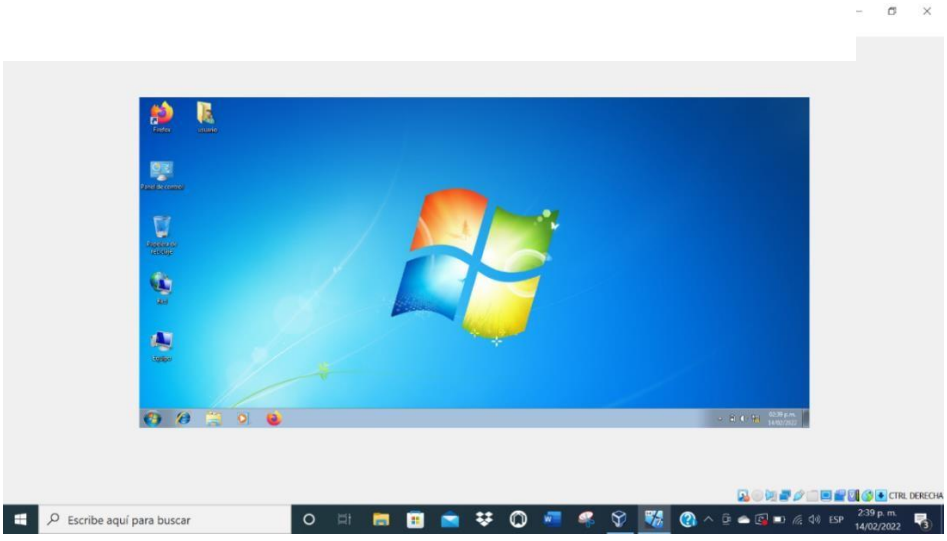
Figura 4. Instalación Windows 7 x86



Fuente: propia

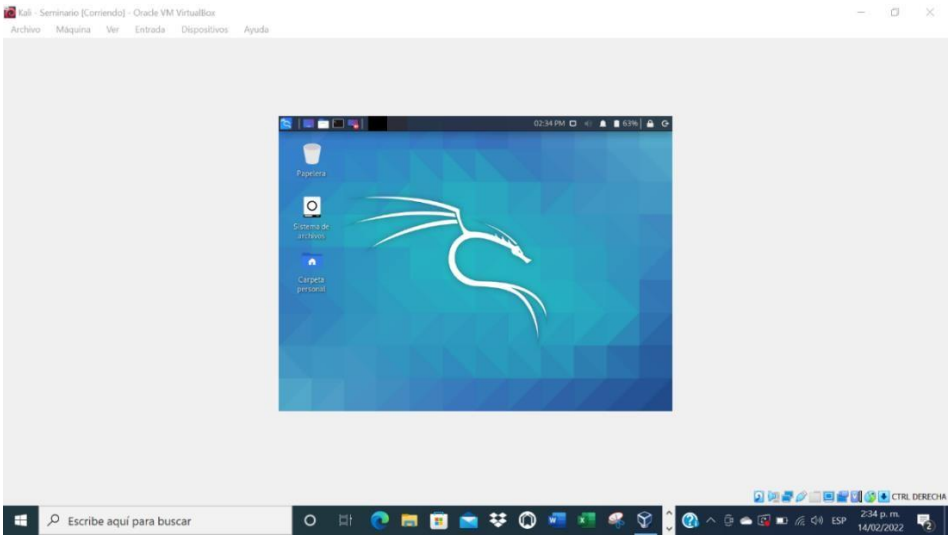
En la Figura 4 se observa la instalación del sistema operativo Window7

Figura 5. Instalación Windows7 x64



Fuente: propia

Figura 6. Instalación Kali Linux

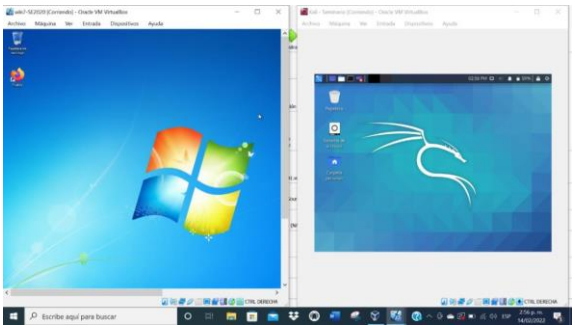


Fuente: propia

Paso C: se debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde porfavor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Se observa en la presente imagen que no se obtuvo ningún colapso de los recursos del hardware, se tiene las dos máquinas corriendo sin problema.

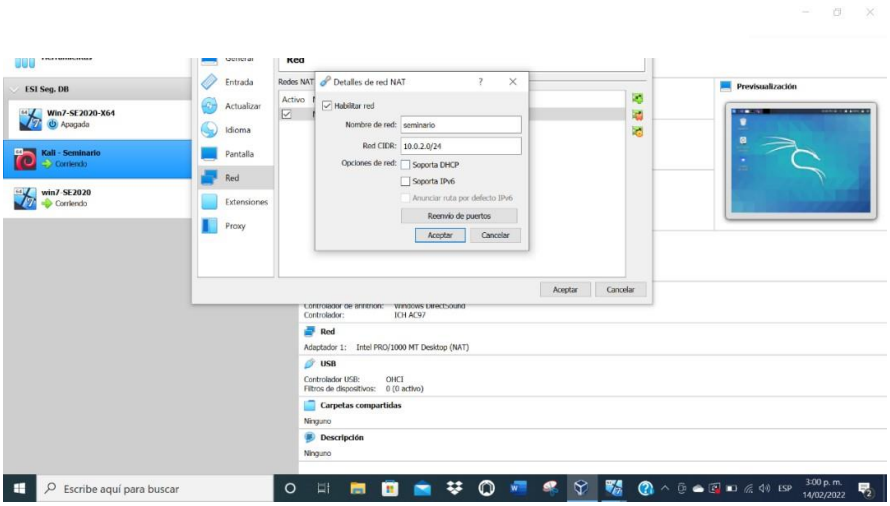
Figura 7. Equipo Windows y Kali Linux corriendo



Fuente: propia

Para poder tener conexión entre las máquinas debemos crear una red la cual asigne pornombre “seminario” y el direccionamiento manual el cual tiene una cobertura entre 0-24.

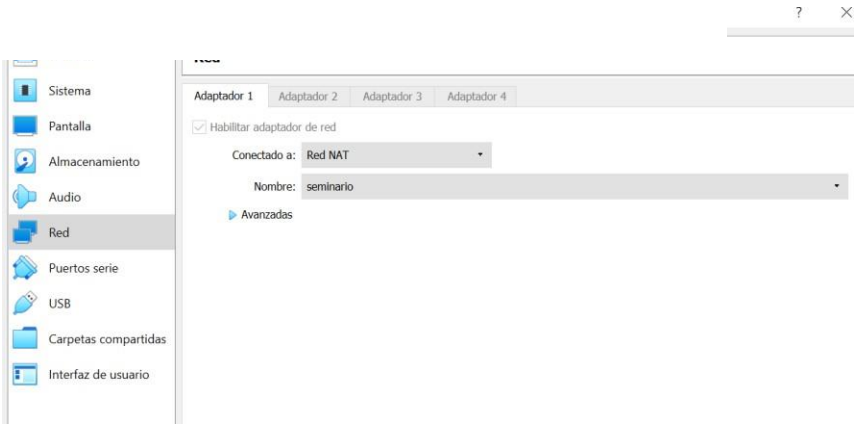
Figura 8. Creación de red seminario



Fuente: propia

En cada una de las máquinas se debe hacer la modificación en: red conectado a red NAT, también en nombre “seminario” que fue la red que inicialmente se creó.

Figura 9. Cambio de red en Kali Linux por "seminario"



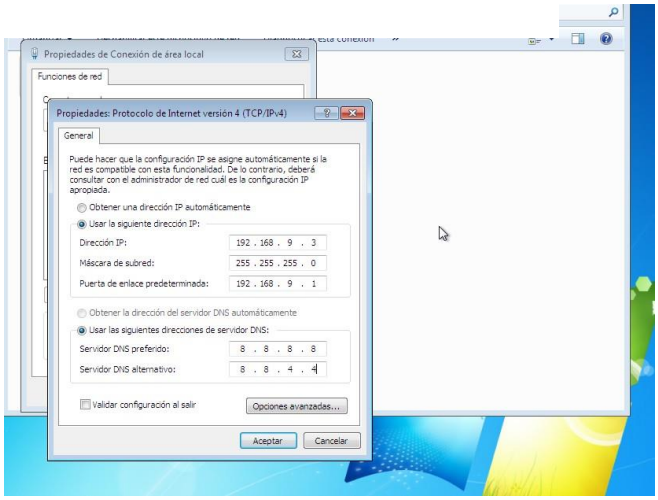
Fuente: propia

Para tener conexión entre las máquinas se debe asignar direccionamiento IP

manualmente. En la máquina de Windows quedaron así:

Windows7 x84 192.168.9.3
Windows7 x64 192.168.1.107

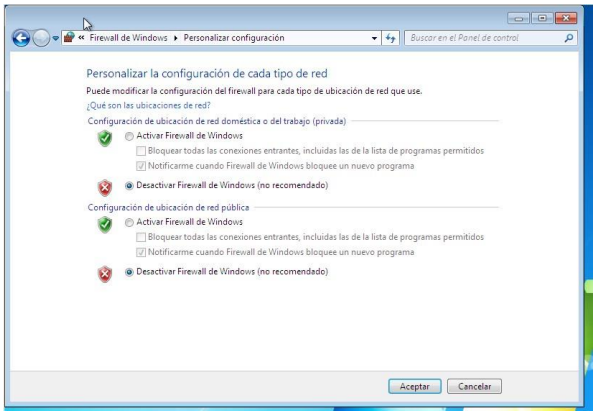
Figura 10. Cambio de direccionamiento IP



Fuente: propia

En Windows se debe verificar que el firewall esté desactivado para que se tenga unabuena conexión como se muestra en la Figura 11.

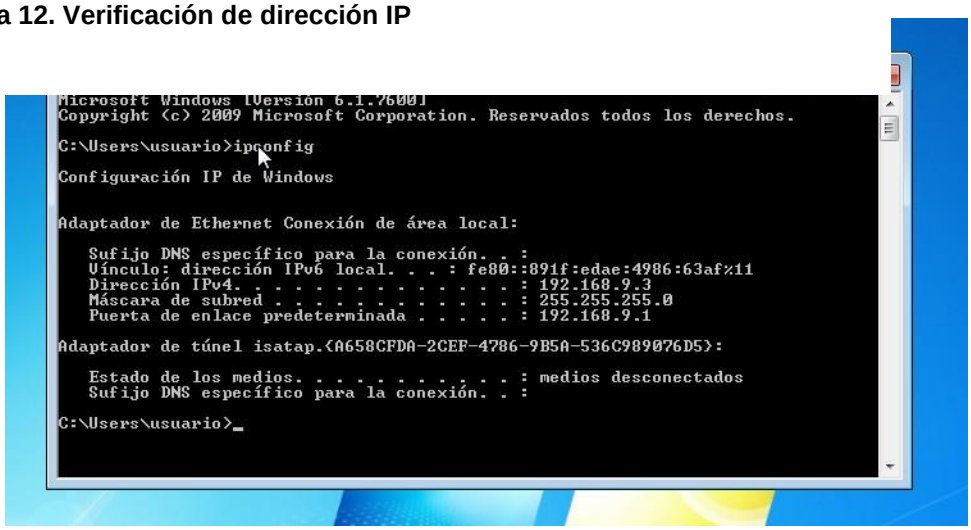
Figura 11. Desactivar firewall de Windows



Fuente: propia

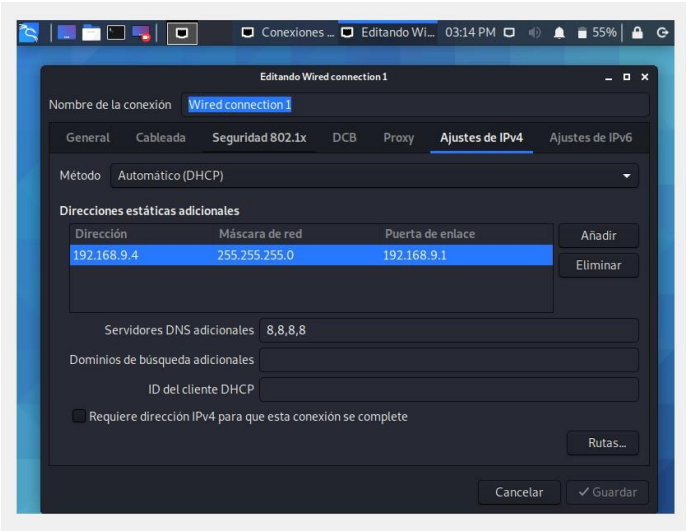
Paso D: evidenciar con printscreen el montaje del banco de trabajoy explicar cómo se encuentra desplegado características técnicas de hardware.

Figura 12. Verificación de dirección IP



Fuente: propia

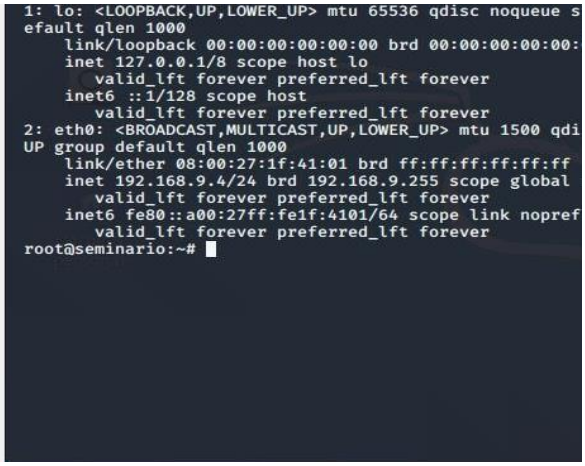
Figura 13. Cambio de dirección IP en Kali Linux



Fuente: propia

Ingresando el comando ip address se verifica que el cambio de ip fue efectivo y quedó: 192.168.9.4

Figura 14. Verificación de cambio de IP



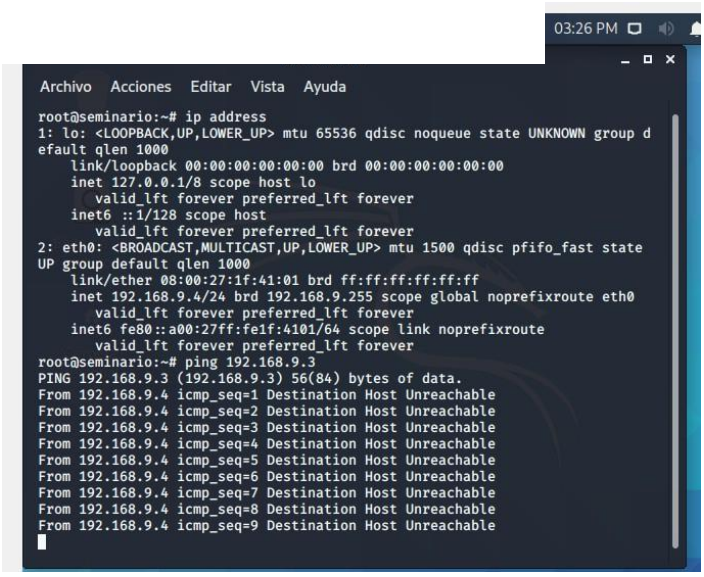
Fuente: propia

Ingresando el direccionamiento de Windows en Kali Linux: LinuxPing

192.168.9.3

Se obtiene lo descrito en la imagen 15.

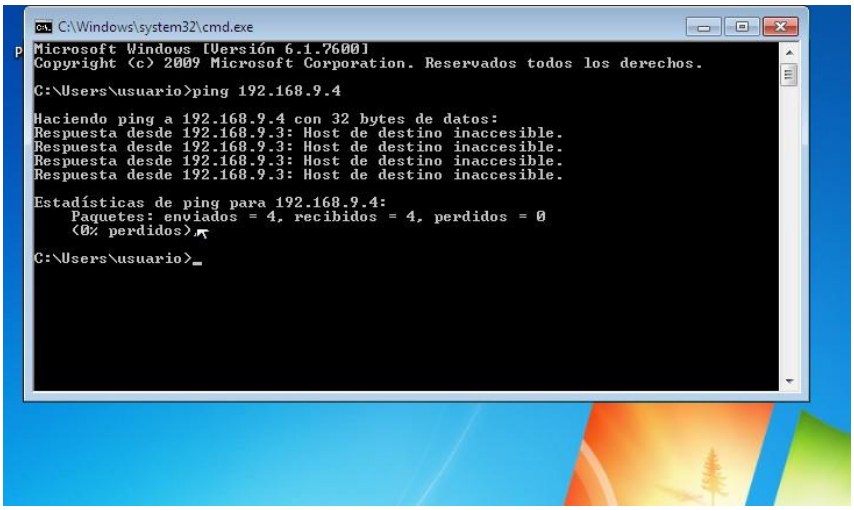
Figura 15. Conexión del Windows con Kali Linux



Fuente: propia

Cuando se realiza la conexión de la máquina Kali Linux en Windows se puede evidenciarque se envían 4 paquetes y se reciben otros 4.

Figura 16. Conexión del Windows con Kali Linux



Fuente: propia

3 DESARROLLO DEL TRABAJO ETAPA 2

3.1 Actuación Ética y Legal

De manera individual usted deberá leer el problema que se encuentra en el anexo 2 – Escenario 2, además deberá leer y analizar el anexo 3 – Acuerdo para generar la solución a las siguientes preguntas orientadoras:

Una vez leído el anexo 2 – escenario 2 y el anexo 3 - acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

3.2 Evidencia de procesos ilegales en anexo 2 – escenario 2

En base a lo estudiado en ambos escenarios se puede evidenciar que se encuentran fragmentos ilegales de la organización WhiteHouse Security, primero que todo se evidencia que los contratos son **“elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos.”** En mi conocimiento es algo muy imprudente por parte de la organización dejar que una persona que no se encuentra vinculada dentro de la misma realice contratos y mucho más que fue despedido por encontrar procesos ilícitos, cuando la organización lo despidió debió acudir a las autoridades competentes para no volver a ejercer ningún cargo por el estilo

Por otro lado, se tiene que **“La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna”** algo supremamente grave puesto que primero que todo los contratos los realiza una persona con ningún vínculo laboral a la organización y la alta gerencia no los revisa para saber si cuentan con lo necesario para garantizar la legalidad del asunto.

3.3 Evidencia de procesos Ilegales Anexo 3

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

Considero como experto en seguridad informática que la organización Whitehouse

Security debe tener reserva de información confidencial con todos sus empleados pero que todo esté dentro de la ley colombiana y si se incurre enalgún proceso ilegal pueda ser denunciado ante las autoridades competentes.

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"

La organización Whitehouse Security maneja grandes volúmenes de información pues es el producto de las actividades realizadas cada día de ofensa y defensa,pero importante recalcar que las actividades de chuzadas sin una orden judicialprevia, interceptación de información y acceso abusivo a sistemas informáticos sin tener consentimiento legal al sistema que se quiere atacar es delito según la ley colombina.

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

En base a la ley colombiana no denunciar ante las autoridades competentes actividades sospechosas de espionaje es delito y está en contra de la ética profesional que tenemos como especialistas en seguridad informática.

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

En base a la ley colombiana Abstenerse de denunciar y publicar la información confidencial e ilegal está en contra de la ética profesional que tenemos como especialistas en seguridad informática pues toda práctica ilegal debe ser denunciada ante las autoridades.

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

En mi conocimiento el responsable directo por lo que se realice dentro de la organización Whitehouse Security es la misma organización, es una falta de ética que responsa un contratista por las actuaciones de una organización.

Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 -

Acuerdo acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

En razón de que se encontraron procesos ilegales y poco éticos en los anexos 2 – escenario 2 y el anexo 3 se mencionan a continuación algunos artículos de la ley 1273 que se vulneran en el acuerdo firmado por el estudiante y la organización Whitehouse Security.

3.4 Ley 1273

Accesos abusivos a sistemas informáticos

3.4.1 Artículo 269 A

"Acceso abusivo a un sistema informático. El que, sin autorización o por fuerade lo acordado, acceda en todo o en parte a un sistema informático protegido ono con una medida de seguridad, o se mantenga dentro del mismo en contra dela voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."[13]

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"

3.4.2 Artículo 269 B

"Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistemainformático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses."[14]

[13] COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009 (04 enero 2009). Consultado el 28 de noviembre de 2020. Disponible en Internet: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

[14] ID.

3.4.3 Artículo 269I

"HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a unusuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código."[15]

3.4.4 Artículo 269J

"**TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes."[16]

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿Usted como experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, 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 códigode ética para ingenieros.

3.5 Punto de vista en "operación Andrómeda buggly"

Deberá buscar la noticia del caso "OPERACIÓN ANDROMEDA BUGGLY" en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.

Mi punto de vista al respecto del "CASO ANDRÓMEDA BUGGLY" ocurrido en la cuidad de Bogotá considero que Colombia es un país que a pesar de su lucha incansable por aportar a la seguridad informática y al hacking ético aún falta mucho, se debe tener una alianza entre las entidades públicas, privadas y la voluntad de gobierno que se busque solo el bien común no el particular o el de

[15] COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009 (04 enero 2009). Consultado el 28 de noviembre de 2020. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

[16] ID.

un partido político.

Colombia es un país que ha tenido una gran cantidad de especialistas en seguridad informática personas con anhelos, sentido de pertenencia, ética y moral que buscar contribuir a la ayuda comunitaria, al bien y al servicio, considero que en aquel tiempo existía el desconocimiento en muchas normasy en oportunidades laborales. La fachada Andrómeda hace un reclutamientode personal experto en seguridad informática y en hacking ético donde deslumbran con cómodas instalaciones, salas de video juegos, espacios de diversión, torneos de futbol, restaurantes, charlas y conferencias sobre el tema.

La falta de oportunidad laboral y de reglamentación en esta rama del conocimiento hace que los profesionales busquen otros países para ejercer.En aquel entonces realizaron un reclutamiento de personal en la cual sacaban todo el provecho del conocimiento de los mismos, “fue una estrategia de cazar talentos” la cual produjo resultados tanto buenos como malos, los cuales pasaron por el desconocimiento en la norma y la falta de experiencia como resultado de esto se cometieron delitos informáticos y a infringir la norma actual del estado colombiano.

Lo más desafortunado es el desconocimiento y aprovechamiento de quien dirigían, afecto la reputación de muchos expertos y se permitió que grupos no legales con fines económicos y de poder político se aprovecharan de todo esto y difamara la labor de todos nosotros.

Finalmente me gustaría aportar que la seguridad informática y el hacking ético es una realidad que cada vez coger más fuerte a nivel mundial, como lo manifesté al comienzo de la respuesta de este punto de vista considero que debemos unir fuerzas de todas ramas judiciales del estado y las entidades privadas para sacar el provecho a todos los grandes expertos que tenemos para un bien común que busquemos la integridad confidencialidad disponibilidad de la información del estado, sin ninguna corrección.

4 DESARROLLO DEL TRABAJO ETAPA 3

4.1 Ejecución pruebas de intrusión

La actividad consiste en: de manera individual se deberá leer el problema que se encuentra en el anexo 4 – escenario 3 referente a equipo Red Team y por medio del banco de trabajo con figurado previamente deberá dar respuesta a las siguientes preguntas orientadoras:

4.1.1 Herramientas software que utilizó para llevar a cabo el a nexo 4 – escenario 3

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

En la presente actividad se utilizaron varias herramientas para el correcto desarrollo de la misma, las cuales fueron las siguientes:

4.1.1.1 NMAP

Figura 17. Imagen NMAP

Fuente: Darkcrizt | | Software Libre. Llega la nueva versión de Nmap 7.80 y estosson sus cambios más importantes. [en línea]. Consultado: 01 de marzo de 2022. Disponible en internet:

https://www.Linuxadictos.com/llega-la-nueva-version-de- nmap-7-80-y-estos-son-sus-cambios-mas-importantes.html

- Dentro de sus principales características se pueden destacar las siguientes:
- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo, listando aquellas que responden ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting).
- Obtiene algunas características del hardware de red de la máquina objeto dela prueba."[17]

Lo más importante de esta herramienta es que se puede escanear las redes, puertos y servicios de un sistema y cada vez ofrece a los usuarios mejores experiencias y mejores resultados. En esta actividad se utilizó el script para comprobar vulnerabilidades y las más conocidas en este caso son:

Auth: ejecuta todos sus scripts disponibles para autenticación.
Default: ejecuta los scripts básicos por defecto de la herramienta.
Discovery: recupera información del target o víctima.
External: script para utilizar recursos externos.
Intrusive: utiliza scripts que son considerados intrusivos para la víctima o target.
Malware: revisa si hay conexiones abiertas por códigos maliciosos o backdoors (puertastraseras).
Safe: ejecuta scripts que no son intrusivos
Vuln: descubre las vulnerabilidades más conocidas.
All: ejecuta absolutamente todos los scripts con extensión NSE disponibles.[18]

4.1.1.2 Metasploit

"Metasploit ayuda a los equipos de seguridad a hacer más que solo verificar vulnerabilidades, administrar evaluaciones de seguridad y mejorar la conciencia de seguridad.[19]

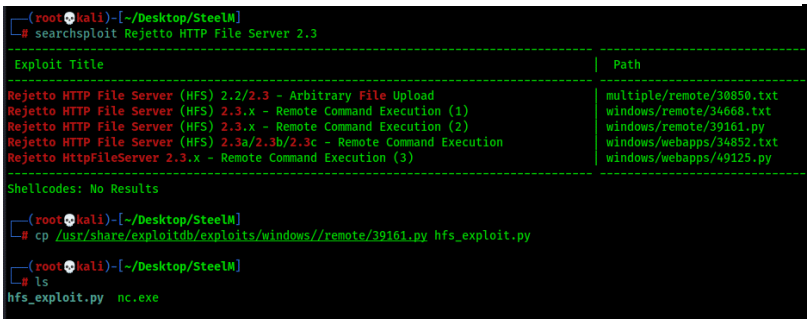
[17] Darkcrizt | | Software Libre. Llega la nueva versión de Nmap 7.80 y estos son sus cambios más importantes. [On Line]. Consultado: 01 de marzo 2022. Disponible en: https://www.Linuxadictos.com/llega-la-nueva-version-de-nmap-7-80-y-estos-son-sus-cambios-mas-importantes.html
[18] CORTES, Chris. Auditando con Nmap y sus scripts para escanear vulnerabilidades. [en línea]. 12 febrero 2015 Consultado: 1 de marzo de 2022. Disponible en: https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/
[19] RAPID7. El marco de prueba de penetración más utilizado del mundo. [en línea]. 25 de febrero 2022 Consultado: 02 de marzo de 2022. Disponible en internet: https://www.metasploit.com/

Figura 18. Imagen Metasploit

Fuente: AVILA. Fredy. Generación de Payloads en Metasploit #1. [Online]. 21 de abril de 2018. Consultado: 02 de marzo 2022. Disponible en internet: https://securityhacklabs.net/articulo/generacion-de-payloads-en-metasploit-1

4.1.1.3 Rejetto v.2.3

Figura 19. Programa que se identificó que es el que producía la pérdida de información.



Fuente: MUDUSA. Explotación Manual | Escalada de privilegios | Montaña de acero |THM | [en línea]. 02 de febrero Consultado: 11 de Marzo de 2022. Disponible en internet: https://systemweakness.com/manual-privilege-escalation-rejetto-http-file-server- Windows-rce-1148a025c15a

4.2 Datos e información del anexo 4 – escenario 3 que le fueron deayuda para identificar el fallo de seguridad

A continuación, se describe los datos e información del anexo 4 – escenario 3 que fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 7 X64.

- Fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia.

- Aplicación llamada rejetto v. 2.3 bajo un Windows 7 con arquitectura X64.

- Exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.

- Falla de seguridad.

- Escalamiento de privilegios.

4.3 ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la máquina Windows 7 ? ¿qué puerto abre la aplicación específica en el anexo?

Las herramientas utilizadas para identificar los fallos de seguridad al interior de la organización en una de sus máquinas (Windows 7) fueron las siguientes:

- NMAP

Figura 20. NMAP

Fuente: Darkcrizt | | Software Libre. Llega la nueva versión de Nmap 7.80 y estosson sus cambios más importantes. [en línea]. Consultado: 01 de marzo de 2022. Disponible en internet: https://www.Linuxadictos.com/llega-la-nueva-version-de- nmap-7-80-y-estos-son-sus-cambios-mas-importantes.html

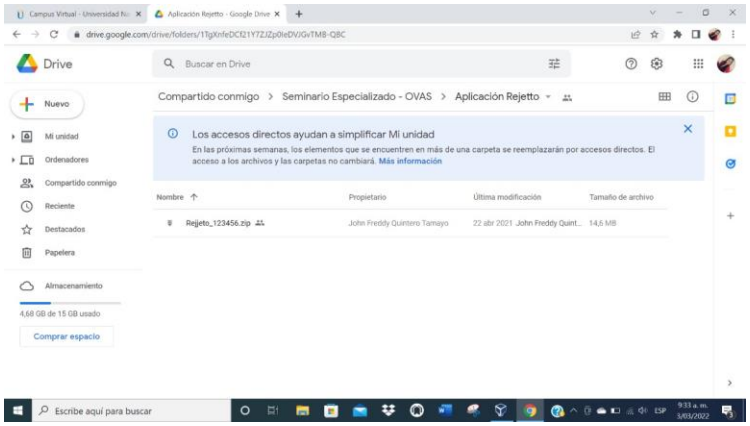
- METASPLOIT

Figura 21. Metasploit

Fuente: AVILA. Fredy. Generación de Payloads en Metasploit #1. [en línea]. 21 de abril de 2018. Consultado: 02 de marzo 2022. Disponible en internet: https://securityhacklabs.net/articulo/generacion-de-payloads-en-metasploit-1

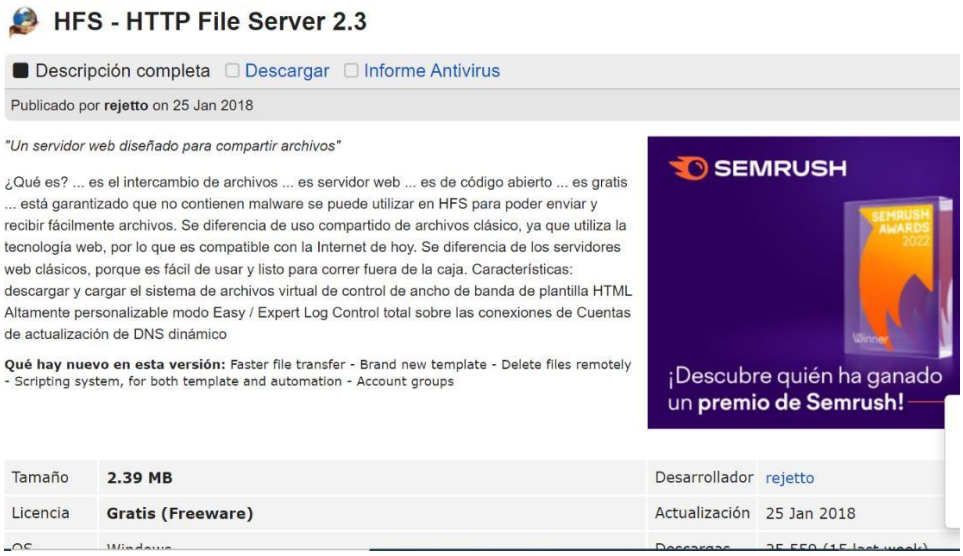
Descarga de **rejjeto_123456** del drive enviado por el docente

Figura 22. rejjeto_123456



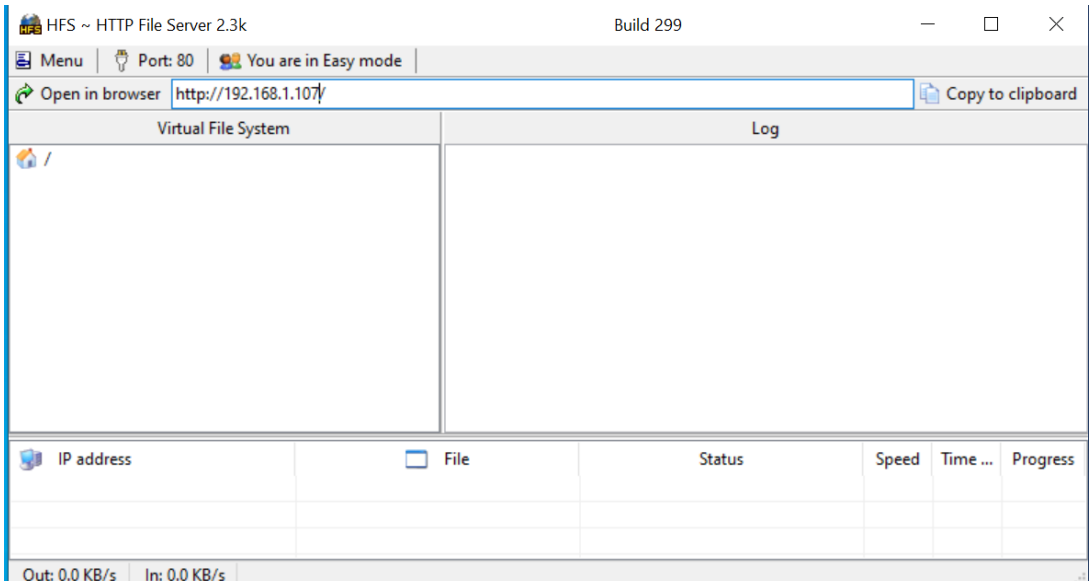
Fuente: Propia

Figura 23. Rejjeto



Fuente: Propia

Figura 24. descarga e instalación Rejjeto

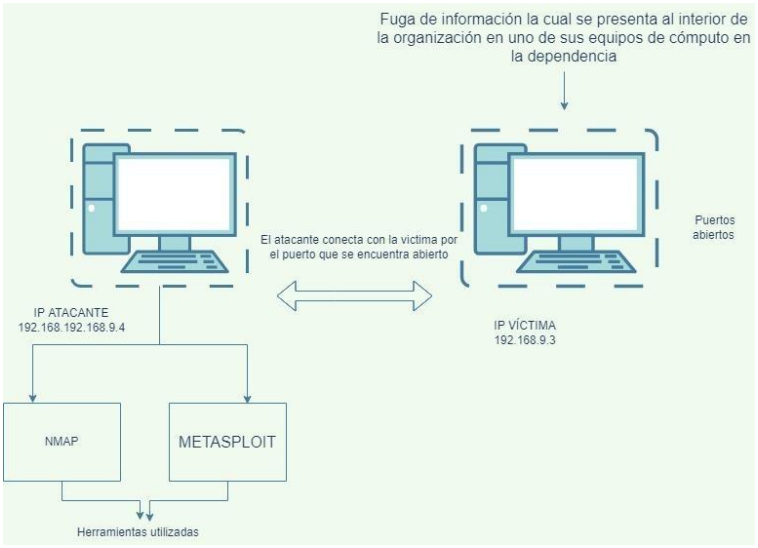


Fuente: Propia

4.4 Explique con sus palabras y de manera específica cómo afecta elataque a la máquina (Windows 7 x64), haga uso de gráficos para explicar el ataque.

Un shell inverso ocurre cuando el host (en este caso, la víctima), comunicarse con el atacante a través de un puerto abierto, en este caso usando un puerto abierto de la aplicación rejetto v 2.3, al obtener esto la comunicación permite que la máquina atacanteacceda a la máquina víctima shell y ejecutar cualquier tipo de comando, en el caso de laempresa, se puede ver creando un usuario con permisos, desde equipo, pero al accedera la máquina es vulnerable a cualquier tipo de ataque que desea realizar en la máquina.

Figura 25. gráfico ataque



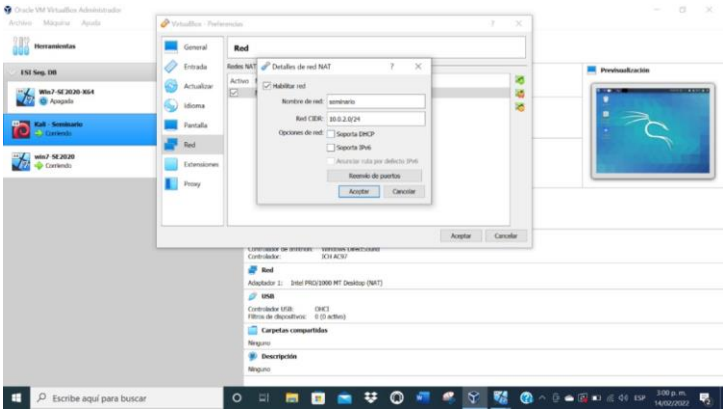
Fuente: Propia

4.5 Documentar cada uno de los pasos que ejecutó para explotar la vulnerabilidad en la máquina Windows

Documente cada uno de los pasos que ejecutó y sus respectivasevidencias para explotar la vulnerabilidad en la máquina Windows.

Para poder tener conexión entre las máquinas debemos crear una red la cual asigne pornombre “seminario” y el direccionamiento manual el cual tiene una cobertura alta.

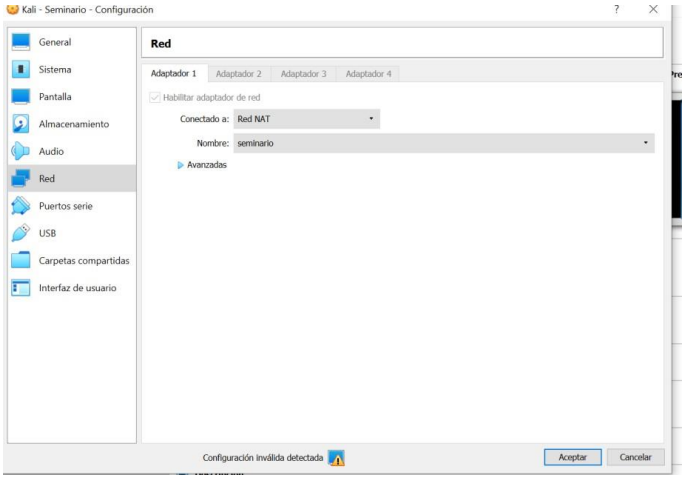
Figura 26. creación de red "seminario"



Fuente: propia

En cada una de las máquinas se debe hacer la modificación en: red conectado a red NAT, también en nombre “seminario” que fue la red que inicialmente se creó.

Figura 27. cambio de red en Kali Linux por "seminario"

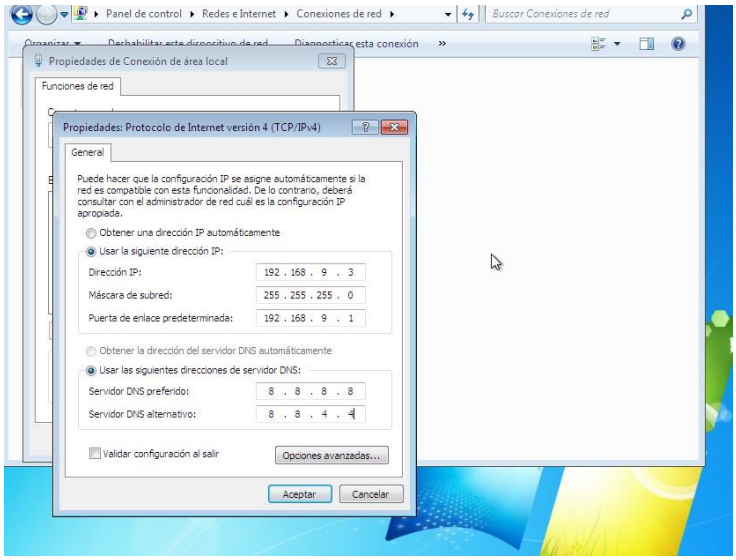


Fuente: propia

Para tener conexión entre las máquinas debemos asignar direccionamiento ip manualmente. En la máquina de Windows quedaron así:

Windows7 x84 192.168.9.3
Windows7 x64 192.168.1.107

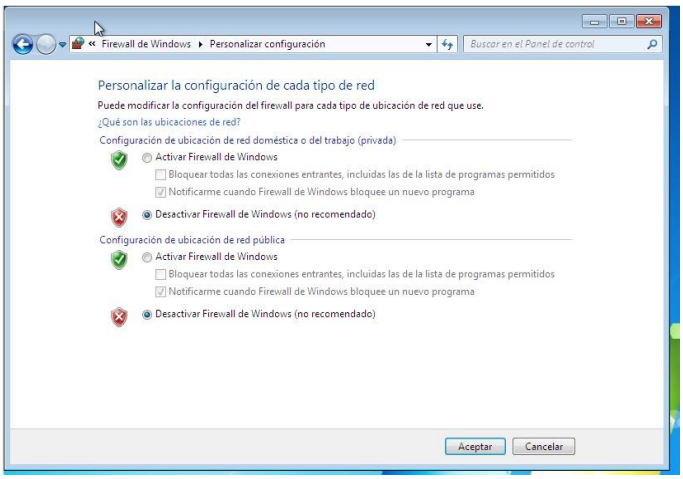
Figura 28. cambio de direccionamiento IP



Fuente: propia

En Windows se debe verificar que tengamos firewall desactivado para que se tenga unabuena conexión.

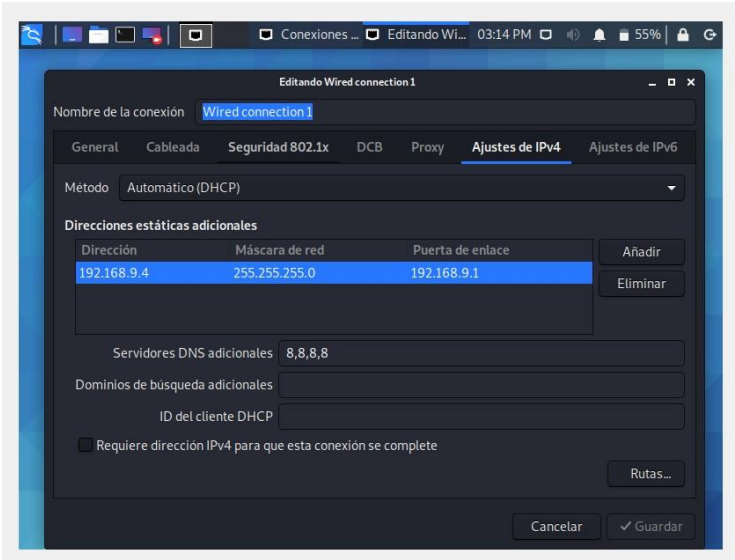
Figura 29. desactivar firewall de Windows



Fuente: propia

Evidenciar con printscreen el montaje del banco de trabajoy explicar cómo se encuentra desplegado “características técnicas de hardware”.

Figura 30. cambio de dirección IP en Kali Linux

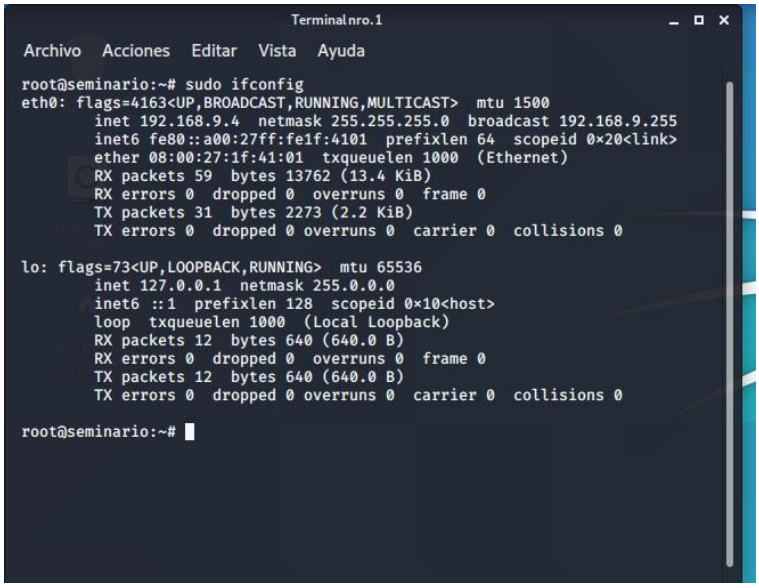


Fuente: propia

Se realiza la consulta de la dirección IP en Kali Linux **IP:**

192.168.9.4

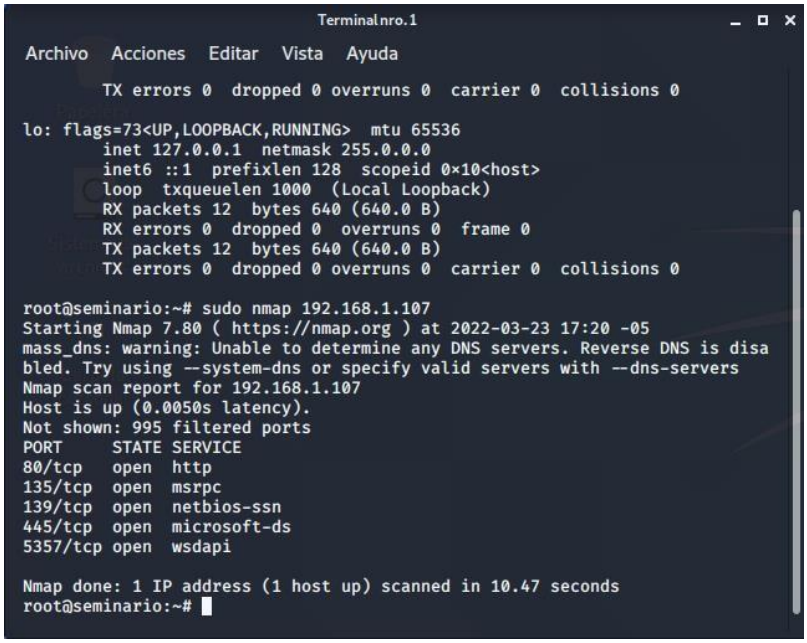
Figura 31. Consulta de IP en Kali Linux



Fuente: Propia

Se consulta la dirección IP del sistema operativo Windows 7 x64 y de identifica la IP: 192.168.1.107

Figura 32. Escaneo de puertos con Nmap desde Kali Linux a Windows x64



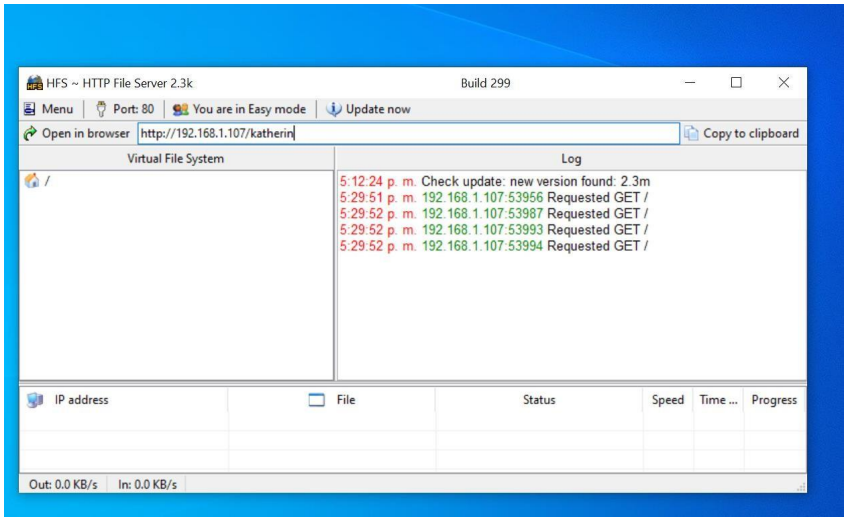
Fuente: Propia

Figura 33. Escaneo de puertos con Nmap desde Kali Linux a Wn x64

Fuente: Propia

Se efectúa la aplicación **rejetto v.2.3** ya instalada en Kali Linux y se hace elanálisis de Windows 7 x64 con la dirección IP: **192.168.1.107**

Figura 34.Ejecución de la aplicación rejetto



Fuente: Propia

Se crea un usuario administrador en Windows 7 x64 con el propósito de comprobar la vulnerabilidad y hacer el exploit

Se accede al panel de control desde la máquina víctima, cuentas de usuario, administrar cuentas y se evidencia la creación del usuario KatherinSanchez y luego se ejecuta el comando net localgroup revisar la carpeta donde quedo el usuario.

Figura 35.Comprobación de usuario

Fuente: Propia

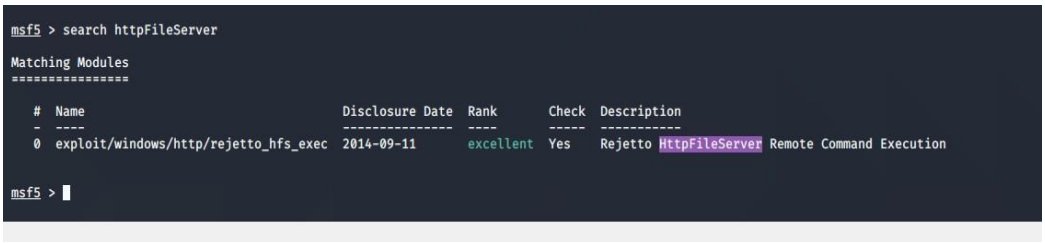
Metasploit se ingresa a la consola y se hace la explotación de la vulnerabilidad por mediodel comando **msfconsole.**

Figura 36. Ingreso a la consola con el comando msfconsole

Fuente: Propia

En el Metasploit se realiza la búsqueda de la vulnerabilidad con el siguiente comando: **search httpFileServer**

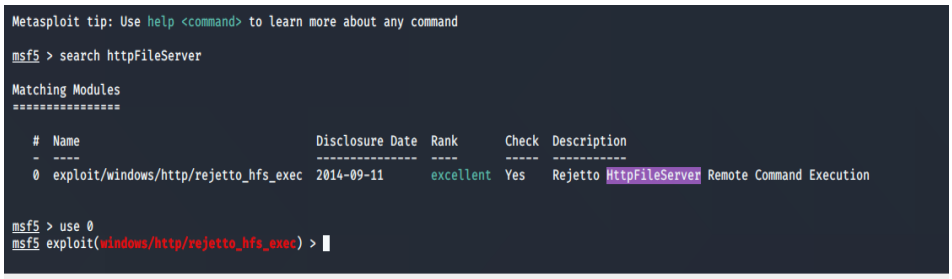
Figura 37. search" httpFileServer



Fuente: Propia

Se ejecutar el comando **use 0** para ingresar a él.

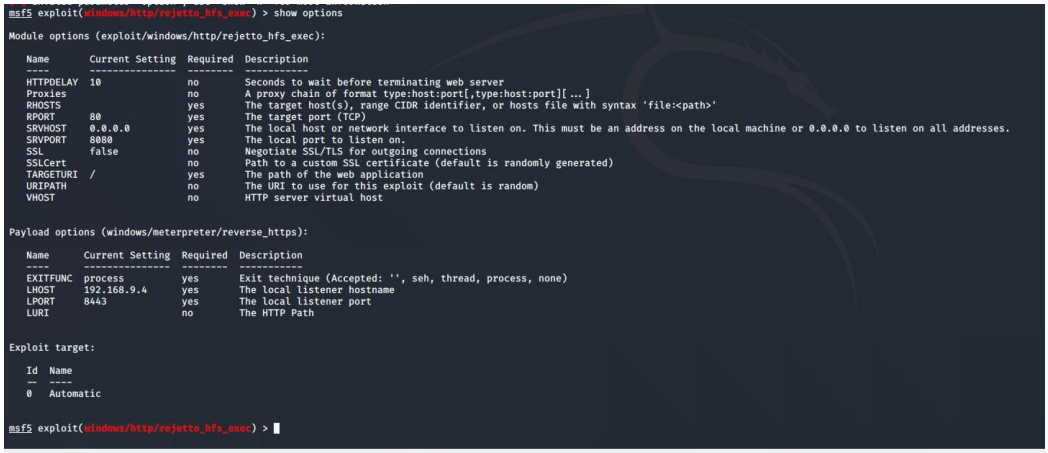
Figura 38. Use 0



Fuente: Propia

Con el comando **show options** se escoge la variable dentro del Metasploit

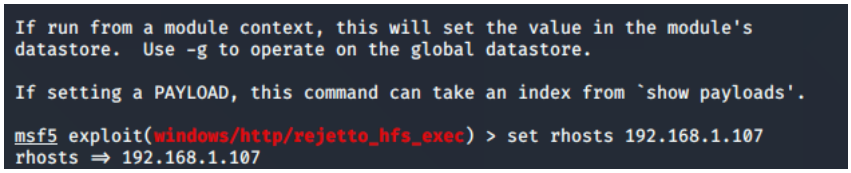
Figura 39. show options



Fuente: Propia

set rhosts se realiza el ataque apuntando a la dirección IP del Window x64, la IP192.168.1.23 entonces se ejecuta así: set rhosts **192.168.1.107**

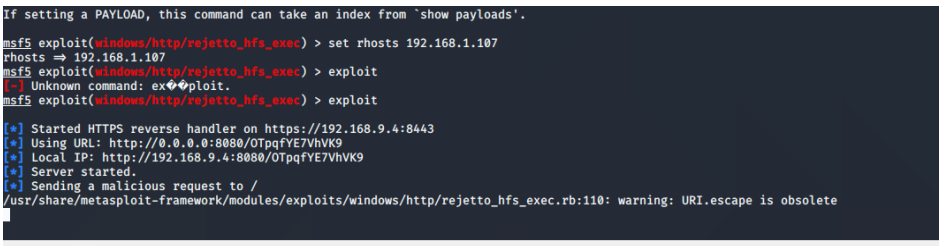
Figura 40. set rhosts



Fuente: Propia

Por último, el comando **Exploit** para su comprobación

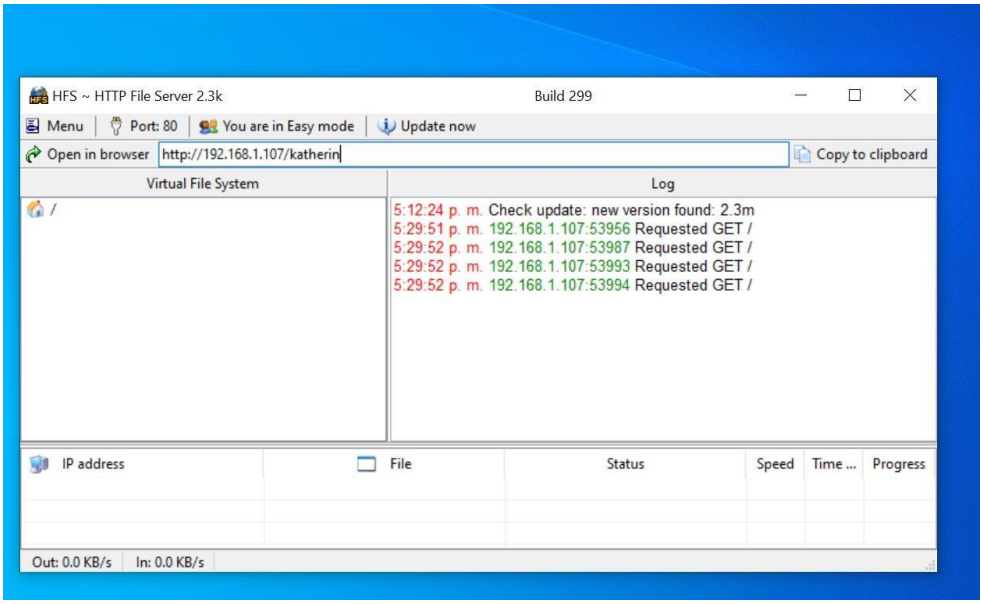
Figura 41. Exploit



Fuente: Propia

Ahora en la máquina víctima Windows 7 x64 se observa el ataque

Figura 42. Explotación de vulnerabilidad en Win7 x64 desde Kali Linux



Fuente: Propia

5 DESARROLLO DEL TRABAJO ETAPA 4

5.1 Contención de ataques informáticos

La actividad consiste en:

De manera individual usted deberá leer el problema que se encuentra en el anexo 5 – escenario 4 referente a equipo Blueteam y por medio del banco de trabajo conFigurado en la actividad anterior deberá dar respuesta a las siguientes preguntas orientadoras:

5.1.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataqueen tiempo real? especifique su respuesta con argumentos técnicos.

Como especialista en seguridad informática y argumentando mi respuesta técnicamenteyo realizaría los siguientes pasos si llegara a encontrarme un ataque en tiempo real.

Primero que todo se analiza la situación y recogerán todos los datos que ayuden a entender qué pasó, por dónde "entraron" los ciberdelincuentes, cuántas personas se vieron afectadas y cuál fue el tipo de ataque pues dependiendo del tipo se sabrá cómo proceder ya que no con todos se procede del mismo modo.

- Fundamental saber el origen del ataque si fue por medio de
- Archivos adjuntos correo electrónico
- Insertando a los equipos USB, USBs, DVDs o CDs con virus.
- Puertos abiertos
- Mensajes de redes sociales
- Descarga de programas, juegos o aplicaciones de internet
- Anuncios falsos entre muchos mas

continuamos tratando de parar la afectación de los equipos por el ataque, realizando los pasos antes expuestos en orden y profesionalmente podemos evitar una afectación graveen los equipos; por último y no menos importante se debe realizar un informe técnico donde se describa toda la situación presentada, se expone ante los directivos de la organización para posteriormente tomar las acciones pertinentes, si fue un error humanoque se justifique sus acciones y se haga responsable de daños y perjuicios, capacitaciones al personal de todas las modalidades de ataque y como evitarlas para contener y minimizar daños futuros.

Como nota aclaratoria si el ataque fue efectivo se debe trabajar con equipos forenses para analizar para un análisis detallado, los daños efectuados y el objetivo del atacante y con herramientas de análisis de vulnerabilidades para evitar.

5.1.2 ¿teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team quémedidas de hardenización propondría para que el ataque no se repita?

Las medidas para endurecimiento del sistema serían las siguientes:

- Tener un sistema operativo actualizado Unix, DOS, AmigaOS, OS/2. En la actualidad aquellos más conocidos e implementados vienen siendo: Microsoft Windows, Mac OS X y Linux en sus últimas versiones.
- Activación de firewall.
- Dentro de la empresa o la organización contar siempre con un paquete. actualizadode antivirus los cuales es objetivo es detectar y eliminar virus informáticos.
- Contar con equipo profesional en seguridad informática los cuales ejecuten programas y software especializados en seguridad para verificar que vulnerabilidades y amenazas cuenta la empresa.
- Cierre de puertos que no se utilicen.
- Desinstalar programas de dudosa procedencia.
- Capacitación continua al personal sobre seguridad informática.
- Tener copia de respaldo de información.
- Cambio continuo de contraseñas y que cuenten con la seguridad adecuada.

5.1.3 ¿Describa con sus palabras las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos?

El equipo de Blueteam se encarga de analizar sistemas, vulnerabilidades, mitigaciones riesgo, desarrollar estrategia, monitorear comportamiento y evaluar las amenazas mientras los equipos de respuesta a incidentes informáticos actúan sobre los ataques que se han producido, respaldados por informes.

5.1.4 ¿Si dentro de un equipo blueteam le indican que debe trabajar con cis "centerfor internet security" usted lo utilizaría para qué fin?

"El Center for Internet Security, Inc. (CIS ®) hace que el mundo conectado sea un lugarmás seguro para las personas, las empresas y los gobiernos a través de nuestras competencias básicas de colaboración e innovación.

Somos una organización sin fines de lucro impulsada por la comunidad, responsable de CIS Controls ® y CIS Benchmarks ™ , las mejores prácticas reconocidas a nivel mundialpara proteger los sistemas y datos de TI. Lideramos una comunidad global de profesionales de TI para desarrollar continuamente estos estándares y proporcionar productos y servicios para proteger de manera proactiva contra las amenazas emergentes. Nuestras CIS Hardened Images® brindan entornos informáticos seguros, bajo demanda y escalables en la nube."[20]

Visión de la CEI: Liderar a la comunidad global para proteger nuestro mundo conectadoen constante cambio.

Misión de la CEI: Nuestra misión es hacer del mundo conectado un lugar más seguro mediante el desarrollo, la validación y la promoción de soluciones de mejores prácticas oportunas para ayudar a las personas, las empresas y los gobiernos a defenderse de las ciberamenazas generalizadas.

Todos los controles y mejores prácticas considerados por CIS como un factor de complemento al trabajo del equipo azul RED TEAM, pues la misma utiliza estos regulaciones e información que CIS tiene sobre amenazas y ataques la ciberseguridad permite tener un sistema más seguro, equipado con lo último Actualizaciones sobre tendencias en ciberseguridad.

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

[20] CIS. Sobre nosotros El Center for Internet Security. [En línea]. 25 de febrero 2022 Consultado: 11 de marzo de 2022. Disponible en internet: https://www.cisecurity.org/about-us

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

Es un sistema de seguridad diseñado para proporcionar a las empresas una respuesta rápida y precisa para detectar y responder a cualquier amenaza a sus sistemas informáticos. Un sistema SIEM tiene un control completo sobre todos los eventos que ocurren en una empresa para poder detectar tendencias o patrones inusuales y tomar medidas inmediatas. SIEM es una evolución de dos tecnologías de seguridad.

La función principal que realiza un sistema SIEM es almacenar e interpretar registros. Este proceso se lleva a cabo en tiempo real y, por lo tanto, proporciona un alto grado de capacidad de respuesta, puede prevenir o resolver cualquier incidente relacionado con laseguridad informática. Un sistema SIEM recopila toda la información de forma centralizada en una base de datos, lo que permite un análisis en profundidad para detectar tendencias y patrones de comportamiento para diferenciar esos casos raros.

"Las principales características que dispone un buen sistema SIEM para la seguridad y respuesta rápida de una empresa son:

- Identificar entre amenazas reales y falsos incidentes.
- Monitorizar de forma centralizada todas las amenazas potenciales.
- Redirigir la actuación a personal cualificado para resolverlas.
- Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución.
- Documentar todo el proceso de detección, actuación y resolución.
- Cumplir con las normas y legislaciones vigentes en cuestión de protección dedatos y seguridad."[21]

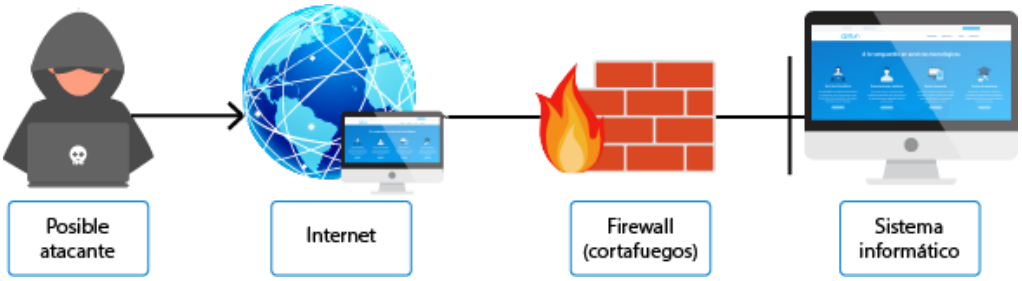
5.1.6 Definir por lo menos 3 herramientas de contención de ataques informáticos "Hardware o Software".

FIREWALL: Brindan la seguridad necesaria para Internet de las cosas (IoT), como termostatos inteligentes y bombillas inteligentes. Estos nuevos dispositivos a menudo vienen con características de seguridad más débiles que pueden hacer que su red sea vulnerable, pero los firewalls de hardware ayudan a prevenir tales violaciones de seguridad. Un firewall es un programa de software o un dispositivo de hardware que filtra e inspeccionala información entrante a través de una conexión

[21] AMBIT. ¿Qué significa SIEM y cómo funciona? [en línea]. 29 de abril 2021 Consultado: 12 de marzo de 2022. Disponible en internet: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo- funciona

a Internet. Representan la primera líneade defensa porque evitan que el malware o los atacantes accedan a su red e informaciónantes de que puedan causar algún daño potencial. Pero hay más de un tipo de firewall por ahí. Es importante conocer la diferencia entre un firewall de hardware y un firewall desoftware para protegerse mejor en casa y en lugares públicos.

Figura 43. Firewall



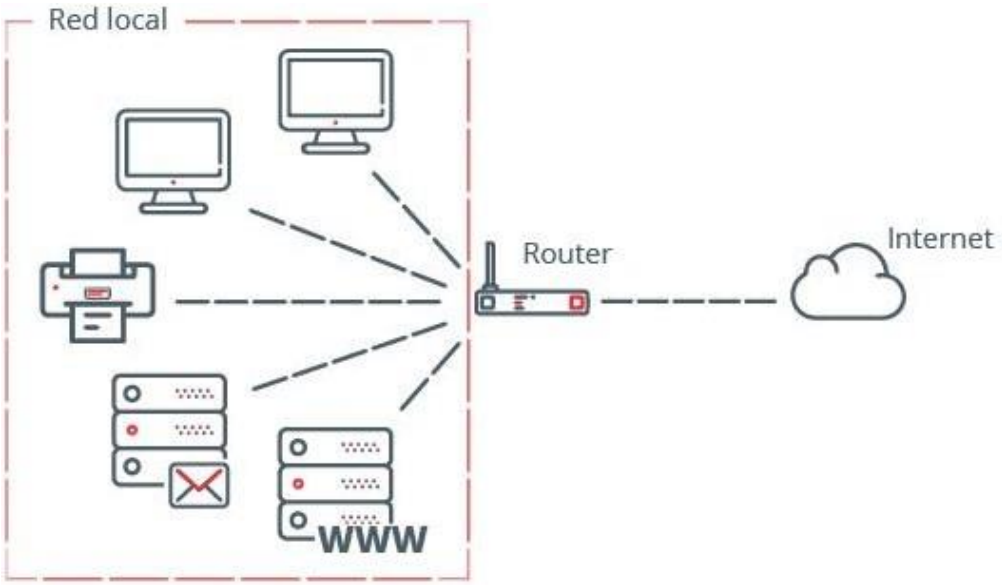
Fuente: ANTIUN Ingeniería S.L. Firewall. [en línea]. 25 de febrero 2022 Consultado: 11 de marzo de 2022. Disponible en internet: https://antiun.com/firewall/

DMZ: **“**Una DMZ ayuda a las señales electrónicas a evitar la estricta seguridad del firewall y del enrutador y abre todos los puertos para una entrega más rápida de los paquetes de datos. Es una manera fácil de mejorar la conectividad, como cuando juegas juegos en línea, transfiere archivos a través de Internet, o crea un sitio web en tu propio servidor, ysimilares La principal desventaja de una DMZ, sin embargo, es que deja una computadoraabierta a todos, lo que puede implicar dejar datos dentro de ella abierta a intrusos. Deberáproceder con la configuración DMZ con precaución. Puede utilizar el reenvío de puertos como una alternativa a DMZ, ya que crea una regla para abrir un determinado puerto o un rango de puertos que sólo recibe una solicitud de datos específica. Para saber más acerca del reenvío de un solo puerto”[22]

Son usados muy a menudo para ubicar servidores como servidores de correo electrónico,web y DNS. Y estable tráfico de datos entre DMZ y la red.

Figura 44. DMZ

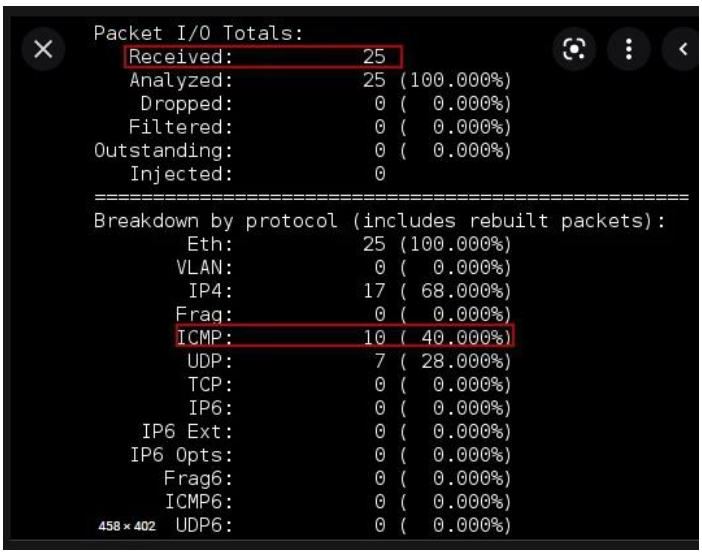
[22] LINKSYS. Activación de la función DMZ en la cuenta de la nube de Linksys. [en línea]. 2022 Consultado:
12 de marzo de 2022. Disponible en internet: https://www.linksys.com/ec/support- article?articleNum=142514



Fuente: INCIBE. Qué es una DMZ y cómo te puede ayudar a proteger tu empresa. [en línea]. 19 DE septiembre 2019 Consultado: 12 de marzo de 2022. Disponible en internet: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu- empresa

SNORT: Herramienta de código abierto para análisis y registro de paquetes en tiempo real, puedeidentificar los ataques DoS y DDoS, útil para la detección de gusanos, exploits yexploración de puertos. Nos permite saber si el tráfico coincide con alguna de las reglaslo cual rechazará dicho tráfico y bloqueará al atacante.

Figura 45. SNORT



Fuente: ORTEGON. Daniel. ¿Qué es Snort?: Primeros pasos. [en línea]. 21 de

marzo 2017 Consultado: 12 de marzo de 2022. Disponible en internet: https://openwebinars.net/blog/que-es-snort/

6 CONCLUSIONES

En base a lo que están exponiendo considero que Colombia es un país que poco a poco ha ido evolucionando en temas tecnológicos de igual manera en normatividad sobre delitos informáticos sin embargo en relación al desarrollo del margen legal en Colombia en pro de defender la confidencialidad, integridad y disponibilidad de los sistemas informáticos esta falta mucho por regular y hacer cumplir.

La virtualización del sistema operativo permite que el hardware de la computadora ejecute muchas imágenes del sistema operativo simultáneamente. Una de las situacionesmás comunes es probar software o aplicaciones en un entorno diferente al de otra computadora. Esto puede potencialmente ahorrarle mucho dinero al ejecutar múltiples servidores virtualmente en una sola máquina.

La ciberseguridad es un factor importante para toda organización, teniendo habilidad paradistinguir cuestiones éticas. El entorno de trabajo permite a los expertos hacer lo correctoantes cualquier situación.

7 RECOMENDACIONES

- Valorar la viabilidad de implementar programas de formación específicos en el ámbito de la seguridad de la información, donde se establezcan las funciones que cumplen los equipos de ciberseguridad Red Team y Blue Team. El objetivo del plandebe ser preparar a los funcionarios y contratistas para las nuevas tendencias, amenazas, vulnerabilidades, resiliencia, soluciones tecnológicas innovadoras, gestión de riesgos de seguridad cibernética y amenazas cibernéticas. Esto permitirá a las entidades tener un equipo humano que trabaje con todas las habilidades para lidiar con los nuevos desafíos que puedan surgir.

- En el proceso de mejora continua y gestión de proyectos de las empresas privadas colombinas se busca realizar análisis periódicos y actuales sobre las diferentes amenazas que existen y pude estar expuesta la empresa ya que en base a esto existe los equipos de seguridad informática como lo son Red Team y Blue Team.

- Realizar análisis de vulnerabilidad en dispositivos, canales, aplicaciones y comunicaciones que apoyan el proceso de intercambio de evaluación de seguridad de la información en las empresas privadas de Colombia para identificardeficiencias y así realizar una serie de medidas de prevención y mitigación del riesgo.

8 VIDEO DE SUSTENTACIÓN

https://youtu.be/yct2UognCU4

BIBLIOGRAFÍA

ALVAREZ, Karina. PROPUESTA DE UNA METODOLOGÍA DE PRUEBAS DE PENETRACIÓN ORIENTADA A RIESGOS. Universidad Espíritu Santo Maestría enAuditoría de Tecnología de Información Guayaquil - Ecuador Abril del 2018. P.4

AMBIT. ¿Qué significa SIEM y cómo funciona? [en línea]. 29 de abril 2021 Consultado: 12 de marzo de 2022. Disponible en internet: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

ANÓN. s. f. «rm - borrar ficheros y /o directorios - Cambiate a Linux». [en línea]. 2015 Consultado: 19 de julio de 2021. Disponible en internet: https://cambiateaLinux.com/rm- borrar-ficheros-directorios

ANÓN. s. f. Chapter 15. Nmap Reference Guide | Nmap Network Scanning. [Online]. 2015 Consultado: 19 de julio de 2021. Disponible en internet: https://nmap.org/book/man.html

ANTIUN Ingeniería S.L.. Firewall. [en línea]. 25 de febrero 2022 Consultado: 11 de marzode 2022. Disponible en internet: https://antiun.com/firewall/

AVILA. Fredy. Generación de Payloads en Metasploit #1. [en línea]. 21 de abril de 2018. Consultado: 02 de marzo 2022. Disponible en internet: https://securityhacklabs.net/articulo/generacion-de-payloads-en-metasploit-1

B. Gustavo. Cómo conFigurar el servidor FTP en Ubuntu VPS[en línea]. 15 de diciembre 2020 Consultado: 10 de octubre de 2021. Disponible en internet: https://www.hostinger.co/tutoriales/como-conFigurar-servidor-ftp-en-ubuntu-vps/

CIS. Sobre nosotros El Center for Internet Security. [en línea]. 25 de febrero 2022 Consultado: 11 de marzo de 2022. Disponible en internet: https://www.cisecurity.org/about-us

COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones"Lineamientos de política para la Ciberseguridad y Ciberdefensa". [Online]. MINTIC, julio

23 del 2011. Consultado el 22 de octubre de 2020. Disponible en Internet:https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011

COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones"Lineamientos de política para la Ciberseguridad y Ciberdefensa". [Online]. MINTIC, abril
11 del 2016. Consultado el 22 de octubre de 2020. Disponible en Internet:
https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Darkcrizt | | Software Libre. Llega la nueva versión de Nmap 7.80 y estos son sus cambios más importantes. [en línea]. Consultado: 01 de Marzo de 2022. Disponible en internet:https://www.Linuxadictos.com/llega-la-nueva-version-de-nmap-7-80-y-estos-son-sus- cambios-mas-importantes.html

INCIBE. Qué es una DMZ y cómo te puede ayudar a proteger tu empresa. [en línea]. 19DE septiembre 2019 Consultado: 12 de marzo de 2022. Disponible en internet:https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu- empresa

LINKSYS. Activación de la función DMZ en la cuenta de la nube de Linksys. [en línea]. 2022 Consultado: 12 de marzo de 2022. Disponible en internet: https://www.linksys.com/ec/support-article?articleNum=142514

ORTEGON. Daniel. Qué es Snort: Primeros pasos. [Online 21 de marzo 2017 Consultado: 12 de marzo de 2022. Disponible en internet: https://openwebinars.net/blog/que-es-snort/