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

DANIEL LEONARDO BELTRAN MELENDEZ
AUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2021

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

DANIEL LEONARDO BELTRAN MELENDEZ
AUTOR

TRABAJO DE GRADO PARA LA ESPECIALIZACION DE SEGURIDAD INFORMATICA

DIRECTO DE CURSO
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2021

RESUMEN

En el desarrollo de los escenarios, pudimos iniciar con los aspectos éticos y legales, que se pueden llegar a observar en las contrataciones, acuerdos de confidencialidad o también en casos relacionados con el ámbito de salvaguardar la información. Y para esto es claro que se debe conocer la legalidad en el actuar profesional, acá validaremos las leyes que rigen la seguridad de la información, como también los aspectos éticos que rigen a las profesiones de ingenierías. Iremos adquiriendo experticia en temas relacionados con la aplicación de la ética y las leyes que nos rigen.

Se efectuara un modelo de laboratorio basado en máquinas virtuales, el cual será indispensable para la ejecución de todos los escenarios de pentesting, desarrollaremos y evaluaremos paso a paso un laboratorio de pentesting, desde el perfil de un integrante de red team, realizando y siguiendo las etapas de intrusión al sistema objetivo, donde podremos validar el comportamiento de las herramientas que se seleccionaran para realizar los procesos de reconocimiento, escaneo, explotación y escalamiento de privilegios. Acá veremos y obtendremos una experiencia en dichas actividades, que nos permitirán conocer e identificar posibles vulnerabilidades que encontraremos a lo largo de nuestras carreras profesionales. También realizaremos un análisis profundo sobre los procedimientos realizados, y detallando el proceso de pentesting paso a paso con sus respectivas evidencias.

Después realizaremos actividades donde se pueden identificar las metodologías y pasos que se siguen en la implementación de auditorías, y procesos efectivos para la ejecución de actividades de un blue team. Claro que igualmente se toman metodologías del pentesting ya que se debe tener un conocimiento claro de la forma en que pueden afectar las vulnerabilidades de seguridad informática y como se realizan. También podremos aprender las principales características y funciones del SIEM que es la gestión de información y eventos de seguridad, también algunas herramientas que podemos usar para la contención de ataques informáticos.

TABLA DE CONTENIDO

TABAL DE ILUSTRACIONES

LISTA DE ANEXOS

GLOSARIO

Blue team: es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva.[1]

Ciberseguridad: es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.[2]

Copia forense: es generar una copia digital exacta, de un medio de almacenamiento, la cual se realiza bit a bit, para mantener todas las características del original.

Exploit: es un código que realiza un ataque explotando una vulnerabilidad en un sistema.

Máquina virtual: es un software que simula un entorno de hardware físico, creando una computadora virtual con las mismas funcionalidades que una física.

Opensource: Es el software que esta diseñado para que pueda ser usado por cualquiera, se puede ver, modificar y distribuir.

Red team: emulan a los atacantes, utilizando sus mismas herramientas o similares, explotando las vulnerabilidades de seguridad de los sistemas y/o aplicaciones (exploits), técnicas de pivoting (saltar de una máquina a otra) y objetivos (sistemas y/o aplicaciones) de la organización.[3]

Rejetto: es un programa que permite el envió y la recepción de archivos.

Shell: Es sencillo, una shell es un programa informático que puede servir como interfaz con los servicios del sistema que éste nos proporcione.

Virtualbox: es un potente producto de virtualización x86 y AMD64 / Intel64 para uso empresarial y doméstico.[4]

Meterpreter: en un payload que nos ofrece la Shell por excelencia obteniendo una gran flexibilidad a la hora de realizar la post explotación, además hay que saber que

[1] (UNIR, 2021)
[2] (INFOSECURITY, 2021)
[3] (UNIR, 2021)
[4] (ORACLE, 2021)

la comunicación entre meterpreter y la máquina remota (atacante) es vía SSL, lo que significa que la información que viaje entre las dos máquinas estará cifrada. [5]

[5] (SECURITY TWINS, 2021)

INTRODUCCIÓN

Inicialmente conoceremos las leyes que se encuentran reglamentadas en la ley colombiana, referentes a los delitos informáticos, y la protección de los datos personales, como también a las bases de pentesting – pruebas de penetración, el cual ser refiere a metodologías para el hacking ético, esto basado en la ejecución de las etapas de análisis que se realizan al ser parte de un red team, veremos las herramientas usadas para este tipo de actividades y con el desarrollo de los laboratorios podremos comprender la importancia de la ley y los métodos de mitigación de riesgos informáticos enfocados a la evaluación de los sistemas de seguridad que se tienen en las empresas.

Profundizaremos en el estudio de las normas éticas que rigen a los ingenieros en general y sus profesiones a fines, todo esto mediante el análisis de casos de estudio, y la aplicación de las normas establecidas, que nos permitirán identificar las buenas prácticas que se deben llevar en las diferentes actividades que realicemos.

En el desarrollo de este informe tendremos la posibilidad de generar experiencias asociadas a la seguridad informática, dándonos bases para poder proseguir con la adquisición de conocimientos en este ámbito profesional. Teniendo claras las metodologías que se aplican, como también conocer estándares y normas que se aplican, como las herramientas de software que podemos utilizar bajo licenciamiento libre.

Tendremos que complementar todos los escenarios para poder identificar claramente, los aspectos de seguridad que rodean las actividades de un red team y un blue team, y plantear las acciones que conlleven a mejorar la seguridad de Whitehouse, todo estará planteado en este informe final, donde tendremos paso a paso todas etapas de estas actividades.

OBJETIVOS

OBJETIVO GENERAL

Generar un informe con todas las características y detalles, que se desarrollaron para darle solución a los problemas de seguridad que presenta la compañía WhiteHouse, dando los resultados del análisis, pruebas, y demás desarrollos que se realizaron sobre los diferentes escenarios que teníamos que validar, como también identificar los ámbitos legales que puedan aplicar a estos.

OBJETIVOS ESPECIFICOS

- Tener claro y documentado que leyes colombianas existen actualmente para combatir los delitos informáticos y salvaguardar los datos personales.
- Analizar el escenario a investigar desde el ámbito de Red team, e identificar las vulnerabilidades que se puedan detectar, teniendo en cuenta las etapas del pentesting.
- Documentar el uso de las herramientas de software, con licenciamiento libre que sirven para realizar las etapas del pentesting.
- Ejecutar un análisis desde el ámbito de Blue team, y poder identificar las vulnerabilidades que se están explotando en un escenario controlado.
- Presentar software que facilite el monitoreo y mejore los niveles de seguridad basándonos en las actividades de Blue team, con licenciamiento libre.
- Presentar un informe detallado que pueda sustentar todos hallazgos que se analizaron en las diferentes actividades realizadas.

1. DEFINICION DEL PROBLEMA

1.1. MONTAJE BANCO DE TRABAJO

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

De manera simultánea The WhiteHouse security requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.[6]

1.2. ANÁLISIS LEGAL

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

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

[6] (QUINTERO, UNAD, 2021)

presión “característica” de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.[7]

1.3. ANÁLISIS RED TEAM

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

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.[8]

1.4. ANÁLISIS BLUE TEAM

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

[7] (QUINTERO, UNAD, 2021)
[8] (QUINTERO, UNAD, 2021)

experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.[9]

1.5. ANÁLISIS FINAL

The WhiteHose Security desea un informe técnico donde se plasme el proceso de los escenarios propuestos en cada una de las acciones como Blue team, Red team y aspectos legales que logró usted como experto en Ciberseguridad dentro del período de prueba de la organización. El informe es solicitado para ser analizado por los analistas Seniors en Seguridad con los que cuenta WhiteHouse Security, esto ayudará al proceso de selección de los expertos que harán parte de esta prestigiosa organización.[10]

[9] (QUINTERO, UNAD, 2021)
[10] (QUINTERO, UNAD, 2021)

2. INFORME TECNICO

2.1. MONTAJE BANCO DE TRABAJO

En el informe técnico tenemos diferentes escenarios, con los cuales WhiteHouse quiere validar nuestros conocimientos y experticia en el tema de seguridad informática, los cuales debemos analizar y solucionar.

2.1.1. Análisis de la legislación relacionada con delitos informáticos.

En primera instancia existe el código penal colombiano el cual se estableció con la ley 100 de 1980, bajo esta ley se tomaron las primeras medidas contra el uso de información sin tener una previa autorización del titular, como también el uso de esta información para fines delictivos o dañinos.
Este código penal tuvo un ligero ajuste en cuanto a los delitos informáticos, velando por la protección de los sistemas de comunicaciones que existían en la época en que se implementó la Ley 1032 de 2006, la cual tipificaba como delito el acceso o uso ilegal de los servicios de telecomunicaciones, o la prestación de estos sin las debidas autorizaciones.
Bajo la jurisdicción colombiana, se rige una ley que abarca las diferentes infracciones que conllevan a un delito informático, esta ley es la 1273 de 2009, la cual esta direccionada a salvaguardar la integridad de las tecnologías de la información y las comunicaciones.

Estos son los artículos que caracterizan 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.[11]

[11] (CONGRESO DE LA REPÚBLICA, 2009)

De igual forma a través del decreto 1377 de 2013 parcialmente se reglamentó la ley 1581 de 2012 que vela por la protección de los datos personales, estos datos requieren previa autorización para su manipulación o almacenamiento ya sea en sistemas de información o archivos, también es facultad del propietario de dichos datos la opción de conocer, rectificar o suprimir la información que haya sido registrada sobre ellos.

2.1.2. Análisis sobre el ejercicio de Pentesting.

Un pentesting (prueba de penetración) o también una auditoría consiste en la realización de ciertas pruebas ofensivas contra los sistemas de seguridad que existen en la estructura analizada, estas van desde un análisis de dispositivos hasta el del factor humano por medio de ingeniería social. Todas estas pruebas van enfocadas a identificar posibles vulnerabilidades y peligro de seguridad asociados, claro posteriormente se deben implementar y corregir estas posibles vulnerabilidades, todo esto asociado a las metodologías existentes Ec-Council, OSSTMM y pruebas de efectividad.
Antes de todo, debemos tener una previa autorización por parte del cliente para realizar estas actividades, donde se evalúa el nivel de intromisión permitido por parte de la prueba, como también la permisividad de los ataques, y el enfoque de esta prueba.

Estas son las etapas o fases que se deben abarcar en el momento de realizar una prueba de penetración:

Ilustración 1 Etapas de pentesting

Fuente: Propia.

2.1.2.1. Etapa de reconocimiento

Esta es la fase de reconocimiento donde se implementan métodos no invasivos, como ingeniería social, búsqueda de documentación publica que se pueda encontrar en la página corporativa, redes sociales donde tenga interacción la empresa a evaluar, también consulta de noticias. A través de estos ejercicios recolectamos información en la que nos podamos apoyar para las posteriores etapas.

2.1.2.2. Etapa de análisis de vulnerabilidades

En esta etapa podemos dividir las actividades en 2 momentos, el primero será el escaneo de puertos, servicios y SO, y luego tendremos identificación y análisis de vulnerabilidades.

- Escaneo de puertos, servicios, SO: Esta actividad como su nombre lo indica está orientada a detectar todos los host y servicios que se encuentren activos en la red analizada, también tendremos en cuenta información precisa de los servicios y software que manejen los hosts, como sistemas operativos, puertos abiertos, datos de hardware, etc. Una de las herramientas más utilizada para esta actividad es el NMAP que tiene practicas funciones, este es un ejemplo.

- Análisis de vulnerabilidades: En este proceso se inicia con en análisis de la información recaudada en las anteriores actividades, donde podemos profundizar el análisis de los dispositivos identificados con otras herramientas como Nessus u OpenVas, y tener un panorama completo de cuales vulnerabilidades podemos explotar. Estas aplicaciones se enfocan en inspeccionar los puertos, los servicios y también en categorizar las vulnerabilidades encontradas, de esta forma tendremos una conveniente investigación sobre cada 1 de los hosts analizados. permitiendo tener informes de los hosts que han sido analizados y el número de vulnerabilidades encontradas.

2.1.2.3. Fase de Explotación de vulnerabilidades

Esta es una de las etapas preferidas, ya que con los resultados obtenidos se procederá a conseguir acceso a los sistemas de la empresa objetivo, pero antes de esto debemos tener una planeación o estructura de la explotación, teniendo en cuenta los tipos de vulnerabilidades

encontradas, podemos verificar si existen exploits contra lo descubierto, o usar las credenciales obtenidas.
También debemos tener muy clara la afectación de los métodos que usemos para explotación de las vulnerabilidades ya que esto es una prueba de penetración y no queremos afectar la operabilidad de la empresa.
Teniendo claro estos, seleccionamos la herramienta y los exploits, lanzamos la herramienta Metasploit, recolectamos las evidencias de la explotación con el informe y las capturas realizadas.

2.1.2.4. Fase Elevación de privilegios o Post-explotación.

En esta etapa buscamos, encontrar permisos de administración sobre lo ya vulnerado o indagar si podemos llegar a otros sistemas no alcanzados inicialmente, esto mediante técnicas de pivoting u otras.
Nos debemos basar en la recopilación de todas las evidencias que pudimos encontrar y en valorar los impactos que puede generar la intrusión real y hasta qué punto se puede ingresar en los sistemas vulnerables

2.1.2.5. Fase de Informe

En esta etapa como su nombre lo indica, es en la que mostramos a nuestro cliente todas las actividades realizadas con sus respectivos resultados, desencadenando en reportes ejecutivos y técnicos, que permitan dar a entender a la parte gerencial los posibles riesgos y su valoración, como también a la parte técnica, darles a conocer sus falencias, y que conozcan todas sus vulnerabilidades explotadas, para realizar los correctivos óptimos que permitan mejorar sus niveles de seguridad. Como valor agregado se da a conocer las contramedidas que debe implementar la empresa para mitigar sus riesgos.

2.1.3. Explicación de las herramientas y servicios utilizados en ciberseguridad:

2.1.3.1. Herramientas:

- Metasploit: es una herramienta de validación de vulnerabilidad y explotación, muy usada para pruebas de penetración en secciones manejables. Existe la versión paga y la libre, la paga te presenta unas opciones de crear proyectos de trabajo, donde se independizan áreas

de trabajos por medios de agrupaciones lógicas. A menudo, tendrá diferentes requisitos para las distintas subredes de una organización. Por lo tanto, puede resultar eficaz tener varios proyectos para representar esos requisitos. La versión gratuita Metasploit framework Community, es muy similar, pero limitada, en su repertorio podemos encontrar la opción de ejecutar y crear exploits contra sistemas objetivos, con diferentes herramientas orientadas a la seguridad.

- NMAP: Es una herramienta de código abierto que permite el escaneo de la red y auditoria de seguridad, muy usada para monitore de la red, validando inventarios o supervisión de la actividad de los hosts o de un servicio, NMAP usa paquetes IP sin procesar para determinar si los hosts se encuentran disponibles en la red, también los servicios en los hosts identificados (nombre y versión de la aplicación), versiones del sistema operativos y decenas de otras características. Está diseñado para funcionar en redes grandes, pero es muy eficiente con host únicos, también es multiplataforma. También descubre características del hardware de red del host objetivo.

- OpenVas: OpenVAS es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste del rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad. El escáner obtiene las pruebas para detectar vulnerabilidades de un feed que tiene un largo historial y actualizaciones diarias.[12]

2.1.3.2. *Servicios* en línea:

- ExploitDB: La base de datos de exploits es un archivo compatible con CVE de exploits públicos y el software vulnerable correspondiente, desarrollado para su uso por probadores de penetración e investigadores de vulnerabilidades. Nuestro objetivo es servir la colección más completa de exploits recopilada a través de envíos directos, listas de correo y otras fuentes públicas, y presentarlas en una base de datos de fácil navegación y disponible de forma gratuita. La base de datos de exploits es un repositorio de exploits y pruebas

[12] (Greenbone, 2021)

de conceptos en lugar de avisos, lo que la convierte en un recurso valioso para quienes necesitan datos procesables de inmediato.[13]

- CVE: La misión del Programa CVE es identificar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas públicamente.[14] Es claro que este programa ayuda teniendo un registro de las vulnerabilidades que ellos mismo catalogan, y toda la información que se considere importante es publicada para que el cualquier persona y las organizaciones puedan tener una descripción clara de la vulnerabilidad que investigan, es muy importante esta labor ya que permite mantener centralizada la información de las vulnerabilidades y así no perder tiempo en identificar las características de las vulnerabilidades.

2.1.4. Evidencia de la implementación del “banco de trabajo” en su entorno local.

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

- Se realiza descarga de la última versión de virtual box.

Ilustración 2 Pagina web de virtual box

Fuente: Propia.

[13] (Offensive Security, 2021)
[14] (CVE, 2021)

- Se ejecuta virtual box para iniciar el montaje de las máquinas virtuales.

Ilustración 3 Ejecución del programa virtual box

Fuente: Propia.

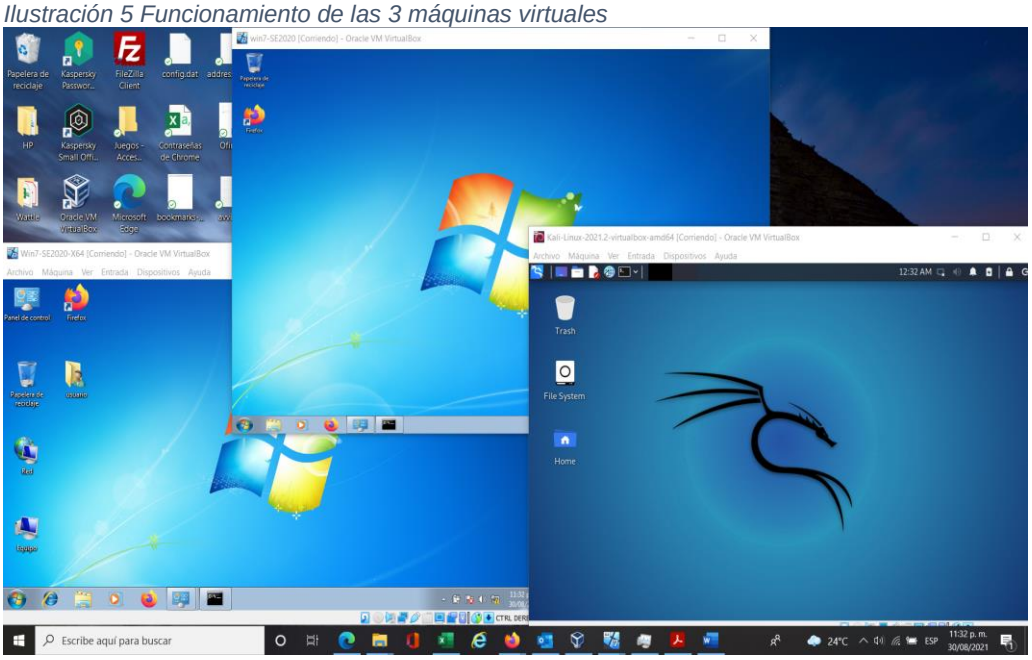
2.1.4.2. Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

- Las 3 máquinas virtuales en línea.

Ilustración 4 importación de las máquinas virtuales

Fuente: Propia.

Ilustración 5 Funcionamiento de las 3 máquinas virtuales



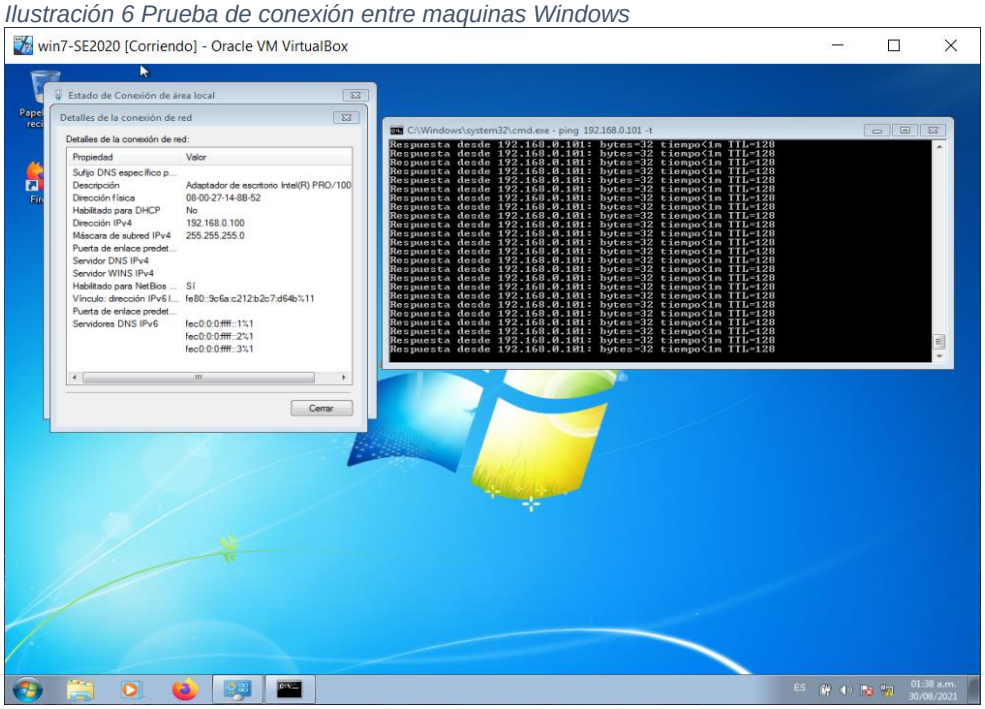
Fuente: Propia.

2.1.4.3. Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor 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 crea red interna con direccionamiento manual.

Comunicación entre maquinas Windows. Ping desde Windows 7 X86 (IP 192.168.0.100) a Windows 7 X64 (IP 192.168.0.101) se deshabilita el firewall para que funcione el ping.

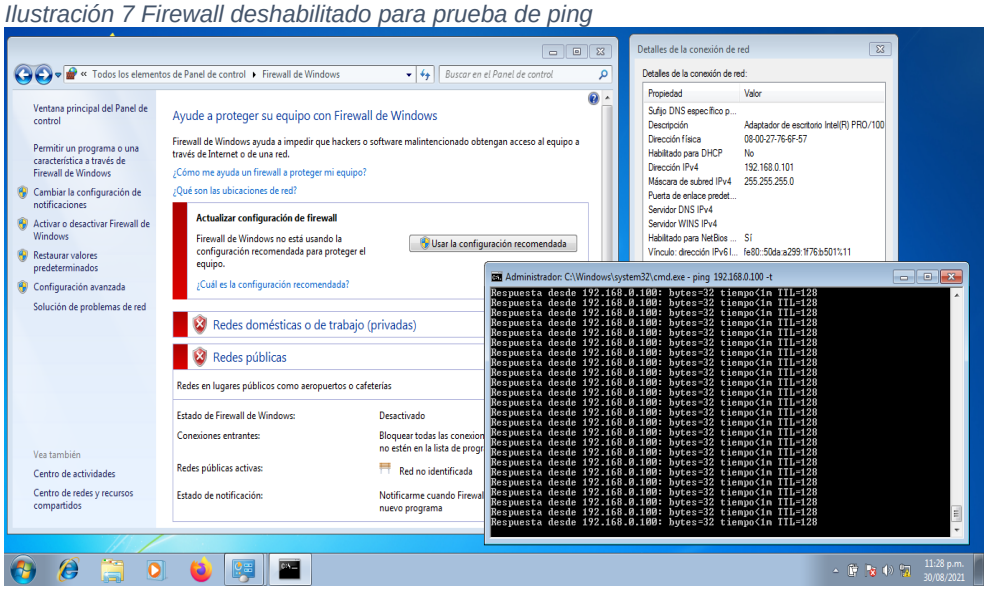
Ilustración 6 Prueba de conexión entre maquinas Windows



Fuente: Propia.

Ping desde Windows 7 X64 (IP 192.168.0.101) a Windows 7 X86 (IP 192.168.0.100.

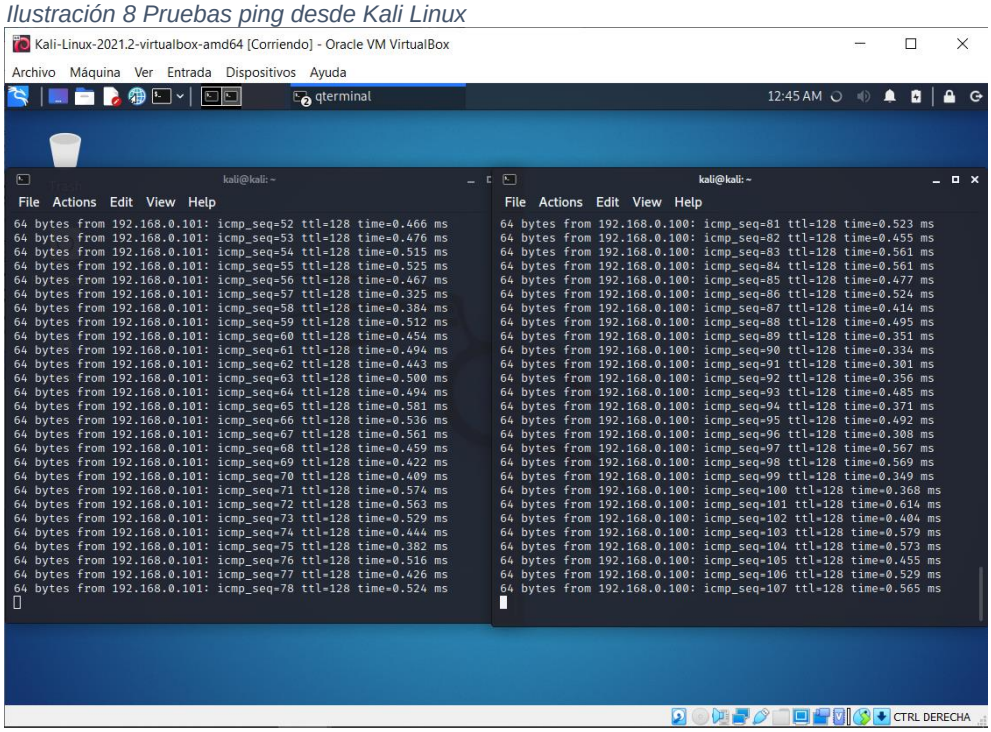
Ilustración 7 Firewall deshabilitado para prueba de ping



Fuente: Propia.

Validación de conexión con ping desde Kali a los 2 equipos Windows.

Ilustración 8 Pruebas ping desde Kali Linux



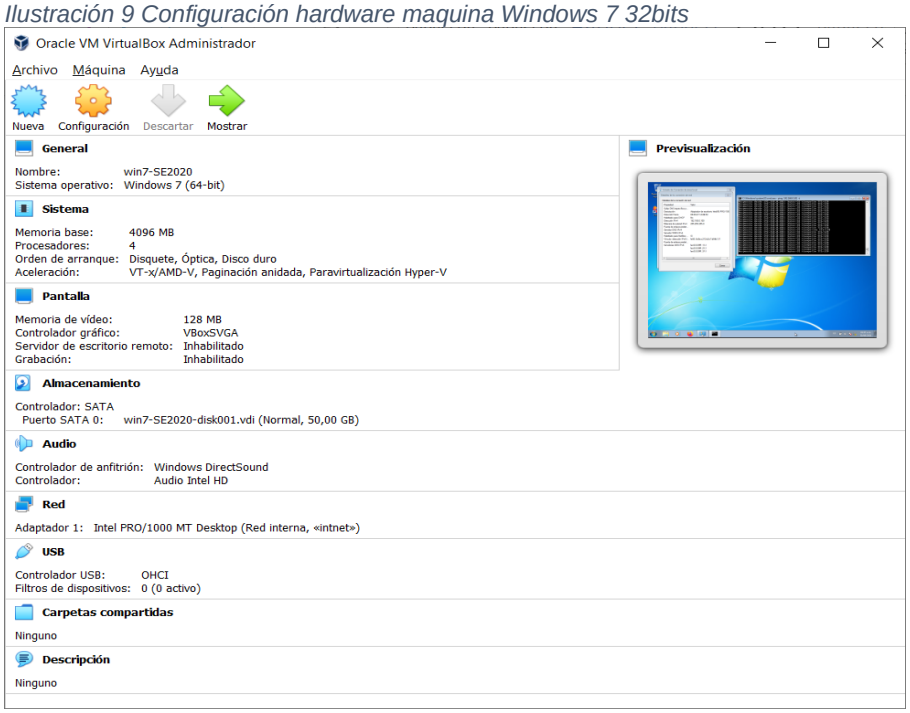
Fuente: Propia.

2.1.4.4. Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Para las máquinas virtuales se selección el hardware que venían por defecto en las imágenes que se importaron en el virtual box. Solo se cambió la configuración de la red, seleccionando una red de modo interno “intnet”, se configuro el direccionamiento de la red 192.168.0.0/24.

- Windows 7 X86 (IP 192.168.0.100) - 4GB ram, 4 cores, DD 50GB

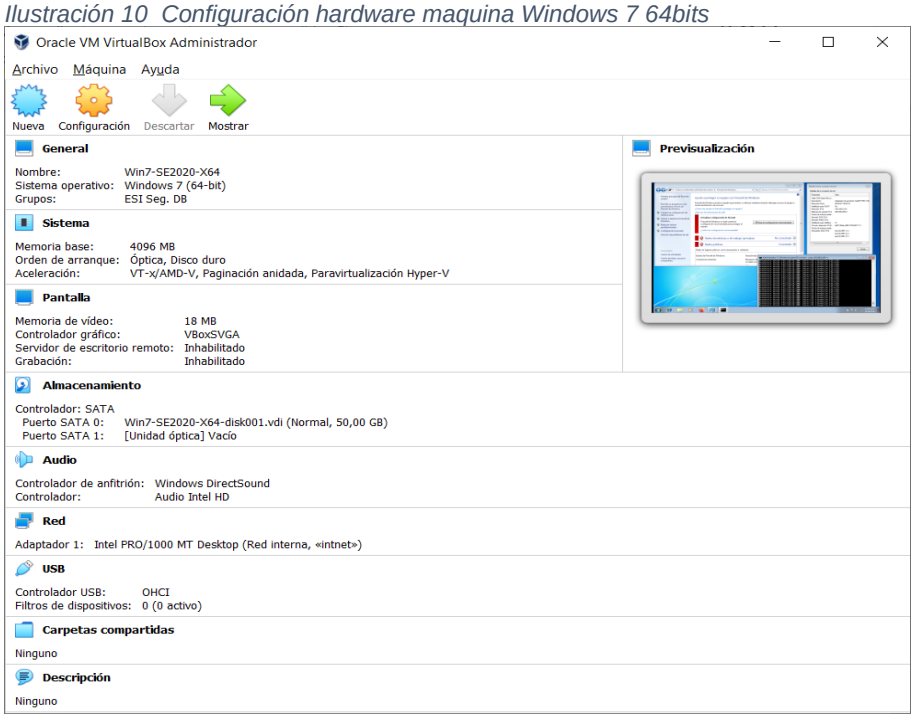
Ilustración 9 Configuración hardware maquina Windows 7 32bits



Fuente: Propia.

- Windows 7 X64 (IP 192.168.0.101 - 4GB ram, 1 cores, DD 50GB

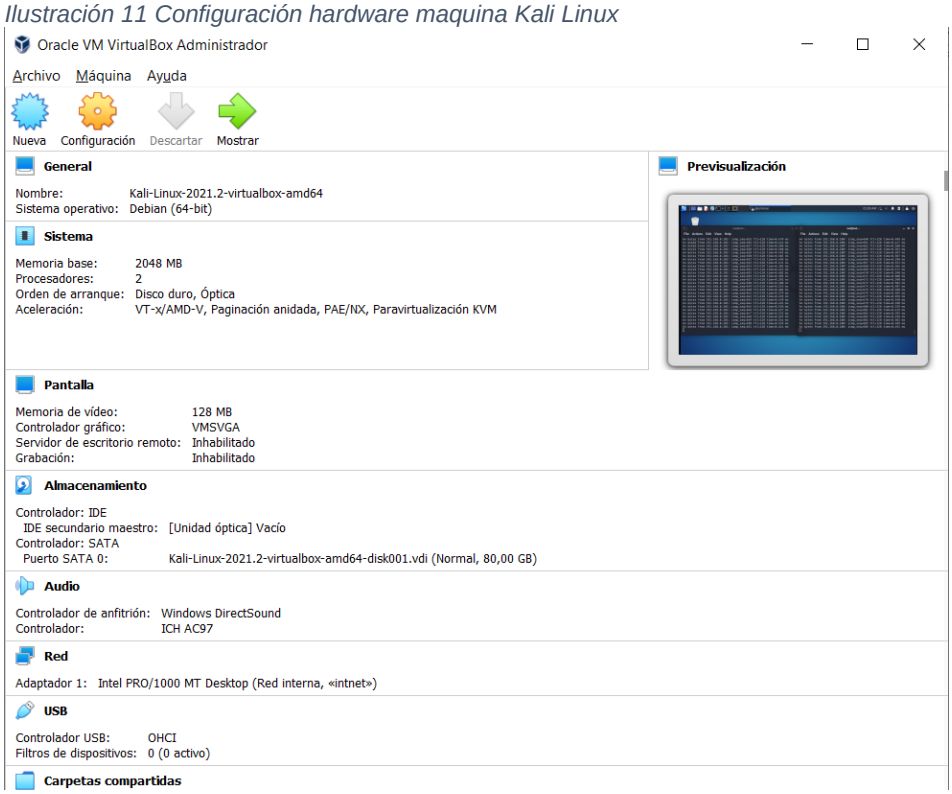
Ilustración 10 Configuración hardware maquina Windows 7 64bits



Fuente: Propia.

- Kali-linux-2021.2 (IP 192.168.0.110) - 2GB ram, 2 cores, DD 80GB

Ilustración 11 Configuración hardware maquina Kali Linux



Fuente: Propia.

2.2. ANALISIS LEGAL

2.2.1. Análisis de los anexos Escenario 2 y Acuerdo desde el punto de vista legal y no ético.

Inicialmente el anexo 2 tiene poca disposición ética por parte de la compañía ya que en el párrafo 2 indica que su contrato de vinculación: fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos.
En el anexo 3 podemos evidenciar diferentes prácticas que son ilegales como se evidencia en la primera clausula, donde especifican la prohibición de divulgar información a las autoridades legales, también está escrito que esta información puede ser sobre algunos procesos ilegales de la compañía y si esto es cierto, es una obligación ciudadana la divulgación de delitos ante las autoridades y también está estipulado en el código de ética denunciar toda transgresión a la ley.

En la tercera clausula numeral 2, tienen estipulado como información confidencial datos de chuzadas, algo que es un delito, como también la interceptación de información y el acceso abusivo a sistemas informáticos, todo esto hace parte de este numeral, donde es claro que se presentan irregularidades con la procedencia de la información confidencial.
En la cuarta clausula numeral 3, especifican que está prohibido denunciar actividades sospechosas de espionaje esto está catalogado como delito, también hablan sobre cualquier otro método de apropiación de información de terceros, esto es ilegal desde cualquier punto de vista ya que este tipo de actividades comprometen la confidencialidad de estos terceros a los que se les hace referencia.
En el numeral 4 de la cuarta clausula también vuelven a recalcar que está prohibido la denuncia en referencia a información ilegal que se pueda conocer.
En la misma clausula numeral 8, especifican que, como parte receptora de la información, sería responsable ante las autoridades sobre un posible allanamiento que se dé y se tenga información que en teoría fue entrega por la parte reveladora, esto insólito ya que simplemente esto es un proceso para participar en un trabajo.
En el documento también se encuentra irregularidades ya que en la cláusula 5 aparentemente faltan partes del documento o están eliminadas, también falta la cláusula 7 que no está.
En la cláusula octava también dejan muy mal parado al estudiante que haga parte del acuerdo, ya que estipulan que ante un evento en el cual se descubra que se tiene información ilegal por parte del receptor, este tendrá que responsabilizarse y dejar exonerado a la parte contratante.

2.2.2. Análisis de los anexos, en relación a la vulneración de la ley 1273 argumentando cualquier proceso ilegal.

Validando el anexo 3 se pueden encontrar claramente diferentes infracciones a la ley 1273, como los son:

En la tercera clausula numeral 2, especifican las chuzadas y la interceptación de información, esto es vulneración al artículo 269C ya que incurre en la interceptación de información entre el origen y el destino, también se puede identificar el artículo 269A ya que citan el acceso abusivo a sistemas informáticos, y claramente están violando la confidencialidad y la integridad de la información.
En el numeral 4 de la cuarta clausula podemos identificar una falencia ética estipulando la prohibición de denunciar ante las autoridades, cualquier

actividad sospechosa de espionaje u otros procesos donde se apropien de información de terceros, esto es vulneración al artículo 269F ya que este estipula la violación a los datos personales, y está definido en este acuerdo que todo dato confidencial puede llegar a ser datos íntimos personales o datos secretos de terceros.

2.2.3. Análisis de la propuesta laboral, teniendo presente en cuenta la revisión desde el punto de vista legal y ético.

No, la verdad no sería algo practico, evaluando la integridad ética no se debería participar en este tipo de proceso, ya que se puede evidenciar practicas totalmente desfasadas en las cuales se vulneran las leyes colombianas, como las normas éticas de cualquier profesión.
Dando un ejemplo claro es la negación a los deberes generales de los profesionales según el código de ética Copnia, donde claramente se recalca en el artículo 31, el deber como profesional de permitir las respectivas diligencias adelantadas por las autoridades policiales o la negación a denunciar los delitos que puedan ser detectados en el ejercicio de la profesión.
También es practico tener en cuenta lo estipulado en los deberes especiales del código de Ética, donde claramente está prohibido ejercer criterios profesionales partidistas, y esto se puede atribuir al interés de la compañía WhiteHouse Security donde intenta fomentar una inclinación favorable a con ellos, en donde sus actividades operacionales pueden comprometer a terceros, debido a la captación de información mediante procedimientos ilegales.
Claramente también se vulnera el artículo 34 donde especifican la prohibición de aceptar trabajos que vayan en contra de las disposiciones legales vigentes, y como hemos visto en este acuerdo confidencial, y lo recalcan claramente, especificando que existen procedimientos y/o actos ilegales dentro de las funciones a desarrollar.
También podemos ver que, al aceptar este acuerdo, estamos desprestigiando nuestra profesión, como también incumpliendo las disposiciones legales, como está indicado en el artículo 35.
Nuevamente en el artículo 39 se recalca que los secretos y la reserva de información confidencial, se sostiene salvo obligaciones legales de revelarla, y en este acuerdo en varias clausulas difieren de este concepto, negando la denuncia ante las autoridades.
Aparte tenemos las faltas graves, que derivan en la perdida de la tarjeta profesional, de estas podemos destacar que por la falta de ética que se ve en este acuerdo por parte del empleador, se asume toda responsabilidad al

firmar este acuerdo incurriendo en la vulnerabilidad a muchas practicas reglamentadas por el código de ética de Copnia, y esto llevara a dañar el perfil profesional o incurrir en algún delito por parte del firmante del acuerdo.

2.2.4. Análisis del caso “OPERACIÓN ANDROMEDA BUGGLY” desde su posición teniendo en cuenta los aspectos legales y éticos.

Desde el aspecto legal se detectaron muchas irregularidades y estas concluyeron que hubo negligencia por parte de los implicados directos, ya que estos actuaron más allá de sus deberes o funciones, se puede ver que se pudo manipular información sensible en muchos niveles, hasta se habla de secretos políticos, solo con esto se puede evidenciar que se cometieron varios delitos como el acceso abusivo a un sistema de información o la interceptación de información, dando pie a controversias en el ámbito político como en el lega, ya que según las investigaciones, esta fachada estaba facultada para operar por la Central de Inteligencia Técnica del Ejercito Nacional, con el nombre de operación Andrómeda.
También se tuvieron indicios de monitoreo del espectro, uso de software malicioso, ya que según un medio experto en seguridad informática de España, denuncio software que tenía asociada la IP que usaba el sitio Buggly, claramente esto es ilegal dado que los que realizaban estas actividades no estaban autorizados para realizaras, y aparte había personal externo que trabajaba sin supervisión done pudieron llegar a tener acceso a información sensible, o como se conoció que personal militar parte de la operación vendió acceso a correos de los miembros de las Farc.
Otros artículos de la ley 1273 que se vulneraron, fueron violación de datos personales de las personas interceptadas, esto evidencia que se violaron casi todos los artículos de la protección de la información y de los datos.

Respecto a la ética, podemos concluir que inicialmente el proyecto estaba cumpliendo los estatutos legales que les permitía ir estudiando las habilidades de los terceros que participaban, aunque muchas de estas personas no tenían conocimiento del objetivo que se buscaba dentro de Buggly; otro punto puede ser que a medida que se avanzaba en conocimiento, habilidades en hacking, reclutamiento de terceros, se empezaron a realizar actividades poco éticas que se mezclaban con ilegalidad, como las de dar facultades a terceros a información delicada del ámbito político, personal, de lideres regionales o grupos de guerrillas, que al final indican pudo terminar en el mercado negro.

2.3. ANALISIS RED TEAM

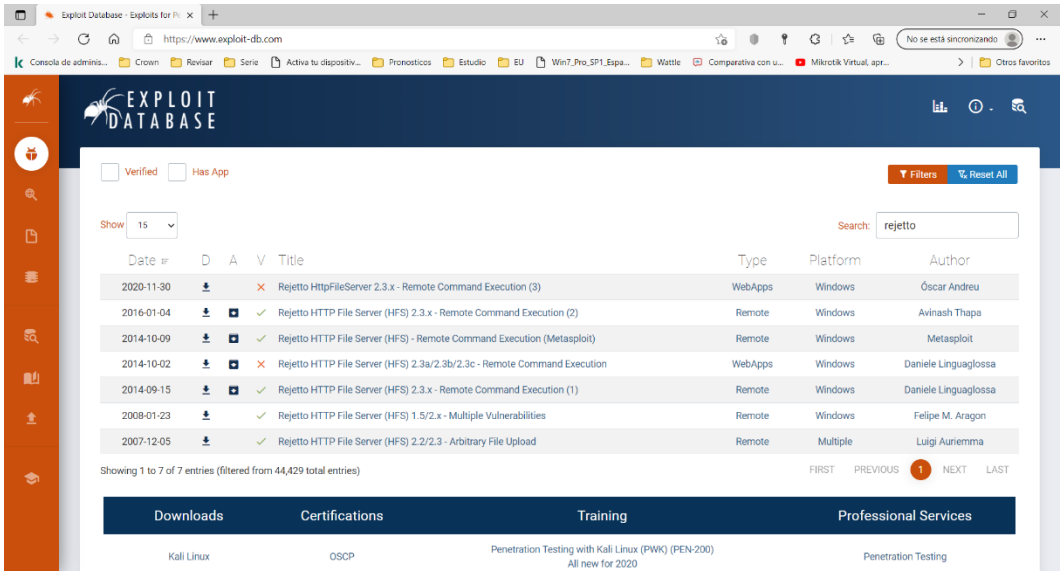
2.3.1. Informe de herramientas y procedimientos utilizados para dar solución al escenario de Red Team de acuerdo a los pasos del pentesting.

Según el análisis que se realizó sobre la documentación aportada, para el caso en cuestión, se pudieron desarrollar los pasos de pentesting de la siguiente forma.

2.3.1.1. Etapa de reconocimiento

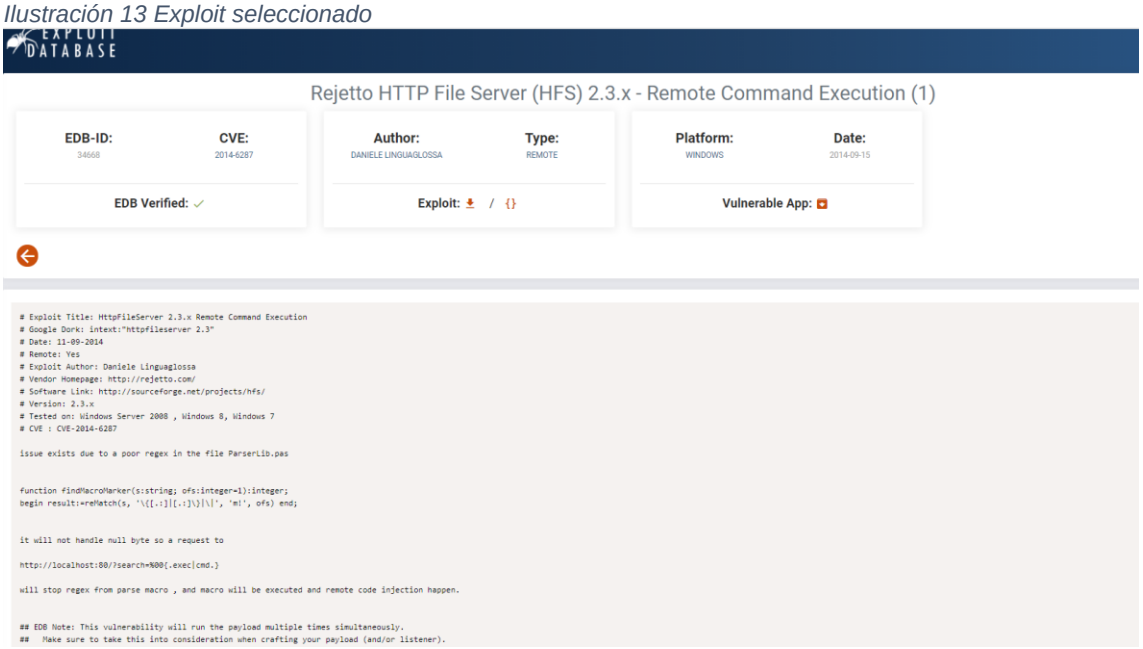
Se analizo la documentación del caso, en la cual se pueden identificar diferentes pistas que seguir, una de estas es la aplicación rejetto v2.3 a la cual se le realiza una investigación, en la que descubrimos diferentes vulnerabilidades según medios web enfocados a la ciberseguridad, también tenemos claro datos claves del host objetivo, como lo son el sistema operativo, la arquitectura.

*Ilustración 12 Información sobre **rejetto** en www.exploit-db.com*



Fuente: Propia.

Ilustración 13 Exploit seleccionado

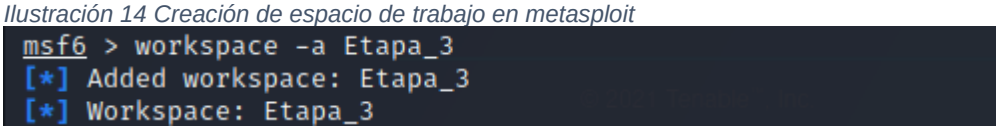


Fuente: Propia.

2.3.1.2. Etapa de escaneo de puerto, servicios y SO

Ya en el análisis de reconocimiento utilizaremos inicialmente la aplicación metasploit framework que viene lista en el Kali Linux, abrimos la aplicación y creamos el proyecto de pentesting para tener registro de todos los datos que recopilemos con cada comando, creamos el espacio de trabajo con los siguientes comandos.

Ilustración 14 Creación de espacio de trabajo en metasploit



Fuente: Propia.

NMAP esta herramienta es esencial para el escaneo del objetivo, entonces ya teniendo el espacio en metasploit, realizamos un análisis con el comando DB_NMAP el cual me permite utilizar la aplicación NMAP desde metasploit registrando toda la información relevante que encontremos.

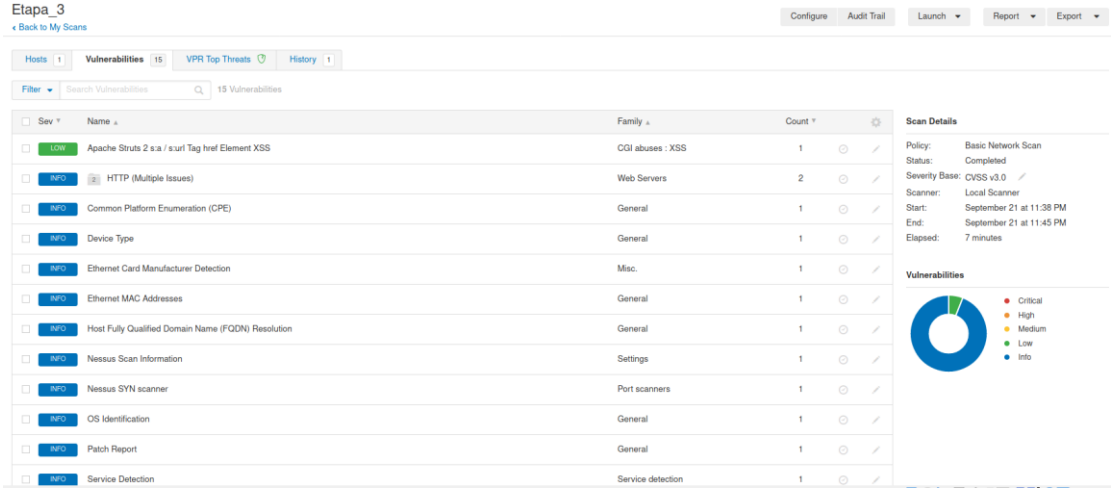
Ilustración 15 Escaneo del host objetivo

```
msf6 > db_nmap -sV 192.168.0.18
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-21 23:52 EDT
[*] Nmap: Nmap scan report for pc202006 (192.168.0.18)
[*] Nmap: Host is up (0.0015s latency).
[*] Nmap: Not shown: 999 filtered ports
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 80/tcp open  http    HttpFileServer httpd 2.3
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 11.09 seconds
```

Fuente: Propia.

Se realiza reconocimiento con otra aplicación conocida llamada Nessus, para ver si se pueden detectar más vulnerabilidades.

Ilustración 16 Búsqueda de vulnerabilidades con Nessus



Fuente: Propia.

Se realizan consultas más específicas para detectar, puertos, sistema operativo y servicios que se están corriendo en la maquina objetivo.

Ilustración 17 Buscando más detalles del host

```
msf6 > db_nmap -n -O 192.168.0.18
[*] Nmap: 'TCP/IP fingerprinting (for OS scan) requires root privileges.'
[!] Running Nmap with sudo
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-22 21:54 EDT
[*] Nmap: Nmap scan report for 192.168.0.18
[*] Nmap: Host is up (0.00045s latency).
[*] Nmap: Not shown: 999 filtered ports
[*] Nmap: PORT   STATE SERVICE
[*] Nmap: 80/tcp open  http
[*] Nmap: MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windo
ws 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0,
 Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows S
erver 2008
[*] Nmap: Network Distance: 1 hop
[*] Nmap: OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 7.01 seconds
```

Fuente: Propia.

2.3.1.3. Etapa de identificación y análisis de vulnerabilidades

Se realiza un análisis con un comando NMAP, que permite validar con las bases de datos de exploit contra las vulnerabilidades del equipo.
Se comparan las vulnerabilidades identificadas y se validan con la información recolectada, donde podemos identificar la vulnerabilidad conocida, para esta existe un exploit identificado con el ID 6287.

Ilustración 18 Búsqueda de vulnerabilidades con NMAP

Fuente: Propia.

Metasploit Framework, ya teniendo los datos del exploit a usar, se realiza la búsqueda con la aplicación metasploit, que nos permite buscar los exploits asociados a un nombre característico de la aplicación vulnerable, o número de identificación del exploit.

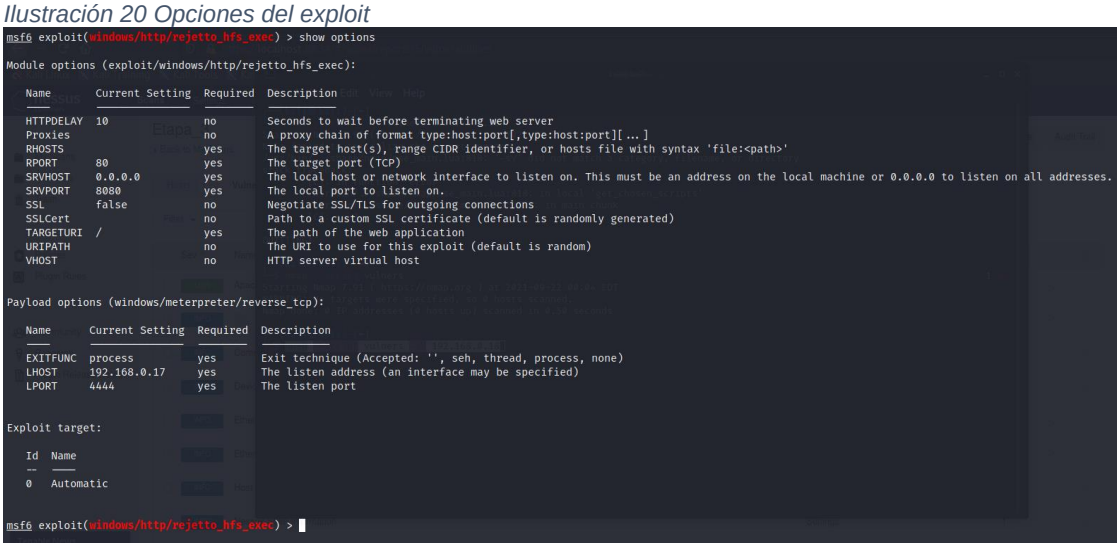
Ilustración 19 Búsqueda de vulnerabilidades

Fuente: Propia.

2.3.1.4. Etapa de explotación de vulnerabilidades

Ya teniendo todo la documentación y análisis previo, de las vulnerabilidades y exploit a usar, seleccionamos el exploit en la aplicación Metasploit Framework, y validamos las opciones que necesitamos configurar para usarlo.

Ilustración 20 Opciones del exploit



Fuente: Propia.

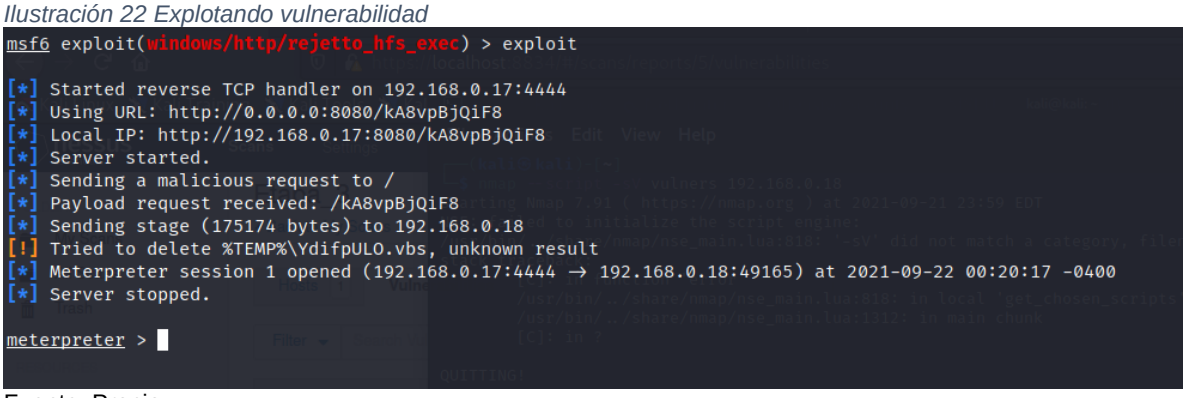
Tenemos que configurar el RHOSTS el cual identifica el host objetivo.

Ilustración 21 Configuración de host objetivo

Fuente: Propia.

Para esta ocasión no se necesita validar configuración, ya que las requeridas están ya predeterminadas correctamente. Procedemos a la explotación de la vulnerabilidad con el comando exploit, y la aplicación entrar a ejecutar el script que hace parte del exploit seleccionado.

Ilustración 22 Explotando vulnerabilidad

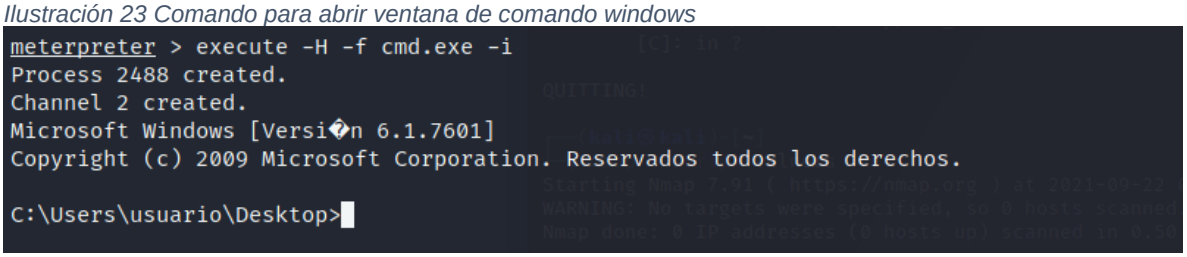


Fuente: Propia.

2.3.1.5. Etapa de elevación de privilegios

En esta etapa seguimos usando el metasploit que usa una serie de plugin para genera una herramienta de comandos que se ejecutan sobre el host objetivo, con los permisos de usuarios heredados en el ataque.
En esta herramienta podemos usar el siguiente comando para habilitar una sesión de comandos Windows con los tokens o permisos que se tienen.

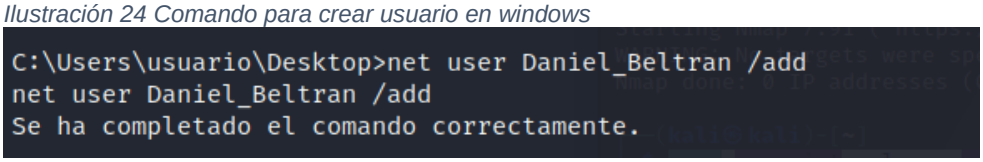
Ilustración 23 Comando para abrir ventana de comando windows



Fuente: Propia.

Ya con la sesión de comandos habilitada procedemos a crear el usuario que demuestra la posibilidad de afectación sobre el host objetivo.

Ilustración 24 Comando para crear usuario en windows



Fuente: Propia.

Concediendo permisos al usuario.

Ilustración 25 Asignar grupo al usuario creado

```
C:\Users\usuario\Desktop>net localgroup Administradores Daniel_Beltran /add
net localgroup Administradores Daniel_Beltran /add
Se ha completado el comando correctamente.
```

Fuente: Propia.

Validación de la creación del usuario con sus respectivos permisos.

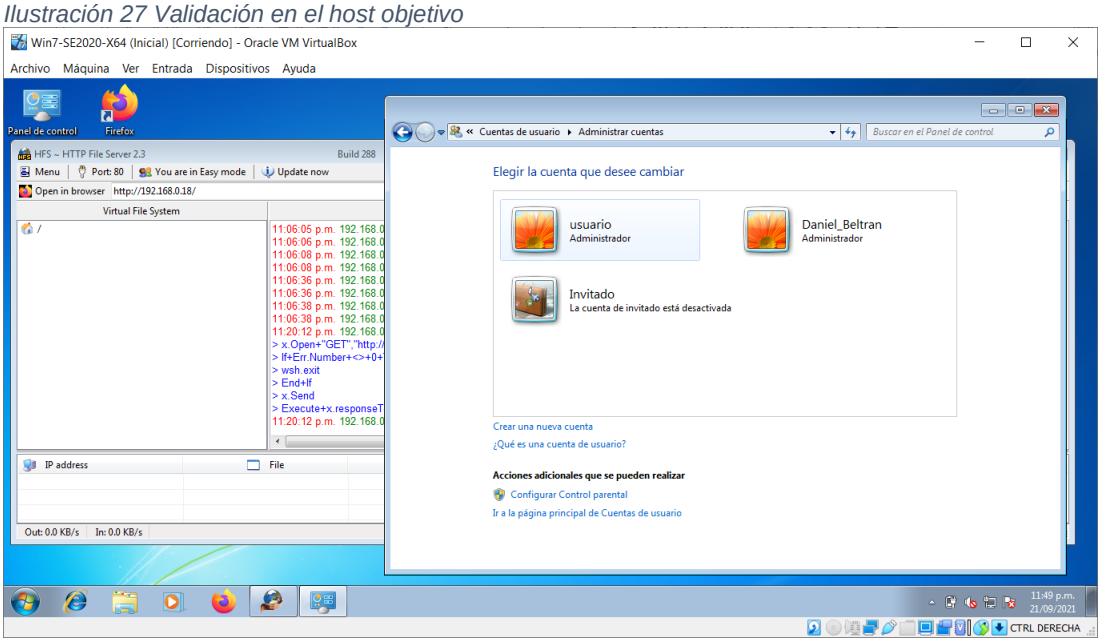
Ilustración 26 Consulta de usuarios del objetivo

```
C:\Users\usuario\Desktop>net localgroup Administradores
net localgroup Administradores
Nombre de alias      Administradores
Comentario           Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Miembros

-------------------------------------------------------------------------------
Administrador
Daniel_Beltran
usuario
Se ha completado el comando correctamente.
```

Fuente: Propia.

Validación en el equipo objetivo todo lo generado desde comandos.

Ilustración 27 Validación en el host objetivo



Fuente: Propia.

Para la elevación de privilegios, se usan los siguientes comandos desde la misma aplicación meterpreter de Metasploit framework.

Ilustración 28 Elevación de privilegios

```
meterpreter > getuid
Server username: PC202006\usuario
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Fuente: Propia.

Abrir ventana de comandos Windows con elevación de privilegios.

Ilustración 29 Ventana de comando con privilegios

```
meterpreter > shell
Process 2924 created.
Channel 3 created.
Microsoft Windows [Versi▯n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>net localgroup Administradores
net localgroup Administradores
Nombre de alias      Administradores
Comentario           Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Miembros

-------------------------------------------------------------------------------
Administrador
Daniel_Beltran
usuario
Se ha completado el comando correctamente.
```

Fuente: Propia.

2.3.2. Informe con análisis del caso de Red Team, que permitió dar solución al fallo identificado.

Fue esencial la información dada en el anexo 4, ya que disminuyó considerablemente varios aspectos de la investigación.

- Rejetto: este dato de la aplicación que está asociado al equipo donde posiblemente se está generando una fuga de información, fue clave porque con solo una búsqueda en Google, se puede identificar varios exploit asociados a este.
- Versión: este dato también es elemental, porque en la etapa de reconocimiento se encontró que el exploit atacaba diferentes versiones, solo con algunas se podía lograr correctamente el ataque.
- Shell reversa: también sirvió para reducir la búsqueda en el exploit, indicándonos el método final de explotación.
- Elevación de privilegios: esto ayudo a identificar uno de los objetivos iniciales al ejecutar el ataque.
- Versión del SO: esto ayudo para poder seleccionar el exploit que servía y correspondía con el sistema operativo a atacar.

- Copia del servidor: esta copia fue fundamental ya que, sin ella no se podría realizar el laboratorio de pentesting.

2.3.3. Informe de herramientas utilizadas para dar identificar fallos en el escenario propuesto.

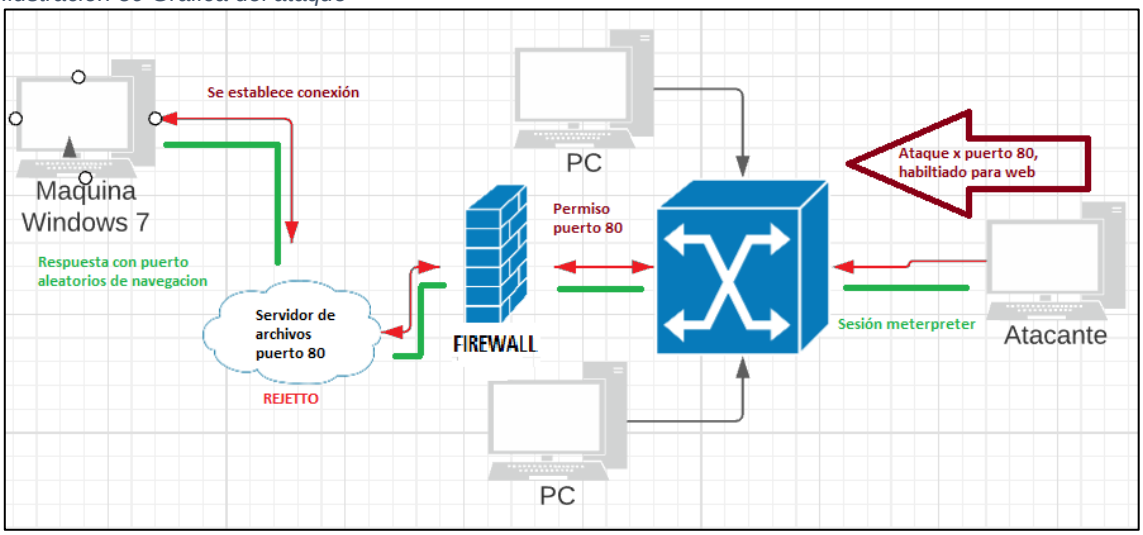
Se uso la herramienta NMAP y NESSUS, en ambas se pudo ver la vulnerabilidad activa en el puerto 80 sobre la máquina de Windows 7, esto claro con la aplicación rejetto funcionando, al realizar la explotación y establecer la conexión con meterpreter se identifica que se escucha desde la maquina atacante con el puerto 4444, y la sesión se establece con el puerto 49165.

Nota: Esto se encuentra en la Ilustración 11 Explotando vulnerabilidad.

2.3.4. Análisis del ataque presentado a cada una de las maquinas identificadas.

Básicamente el ataque permite la ejecución o manipulación de la maquina Windows 7, desde una consola de comandos con privilegios system, esto según entiendo por medio de la función findMacroMarker en parserLib.pas que se encuentra en Rejetto HTTP File Server antes de la versión 2.3c, ya en la consola el atacante puede llegar a ejecutar programas arbitrariamente, o profundizar su ataque a otros equipos de la red donde este la máquina, comprometiendo toda la red y sus sistemas.

Ilustración 30 Grafica del ataque

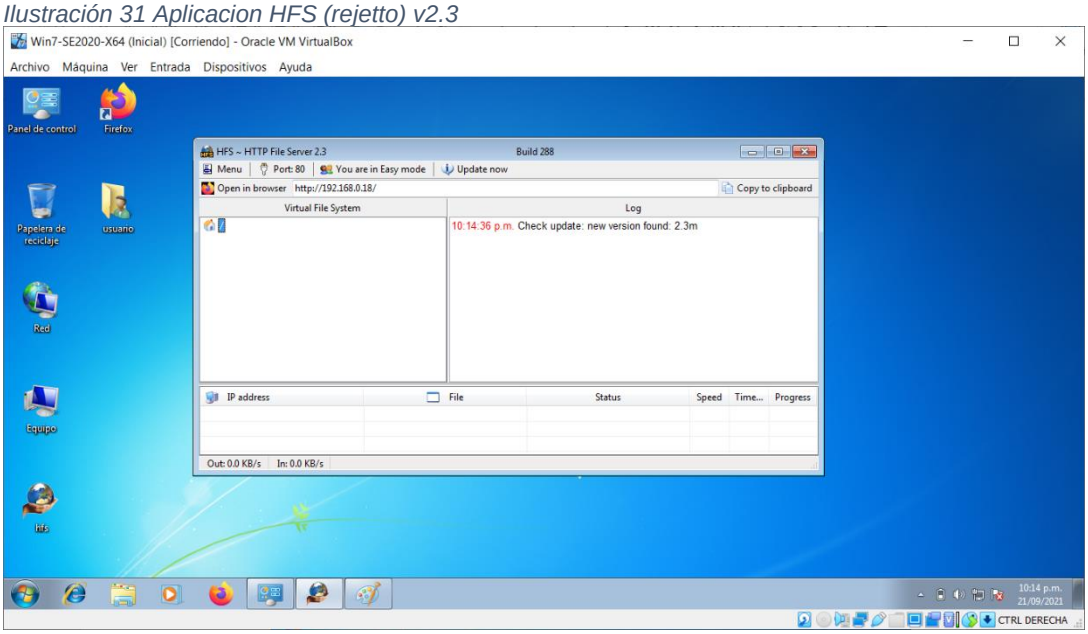


Fuente: Propia.

2.3.5. Informe de la explotación de vulnerabilidades en el escenario propuesto.

Primer paso se ejecutó la aplicación HFS (Rejetto) V2.3 en la maquina Windows 7 de 64 bits.

Ilustración 31 Aplicacion HFS (rejetto) v2.3



Fuente: Propia.

Escaneo del objetivo, con diferentes comandos de NMAP.

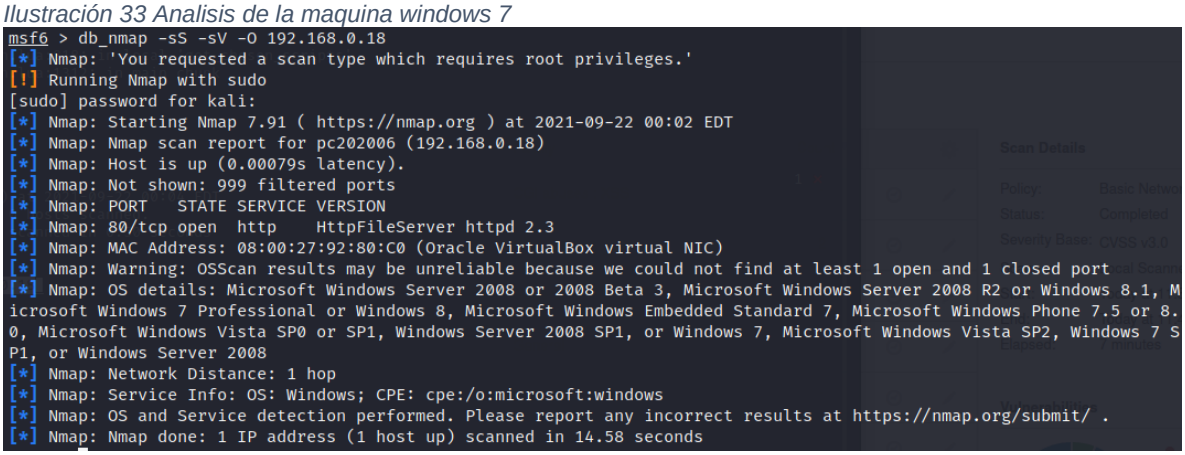
Ilustración 32 Scaneo del host objetivo

```
msf6 > db_nmap -sV 192.168.0.18
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-21 23:52 EDT
[*] Nmap: Nmap scan report for pc202006 (192.168.0.18)
[*] Nmap: Host is up (0.0015s latency).
[*] Nmap: Not shown: 999 filtered ports
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 80/tcp open  http    HttpFileServer httpd 2.3
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 11.09 seconds
```

Fuente: Propia.

Análisis de servicios y sistema operativo del objetivo.

Ilustración 33 Analisis de la maquina windows 7



Fuente: Propia.

Se realiza un análisis de las vulnerabilidades del equipo.

Ilustración 34 Búsqueda de vulnerabilidades con NMAP

Fuente: Propia.

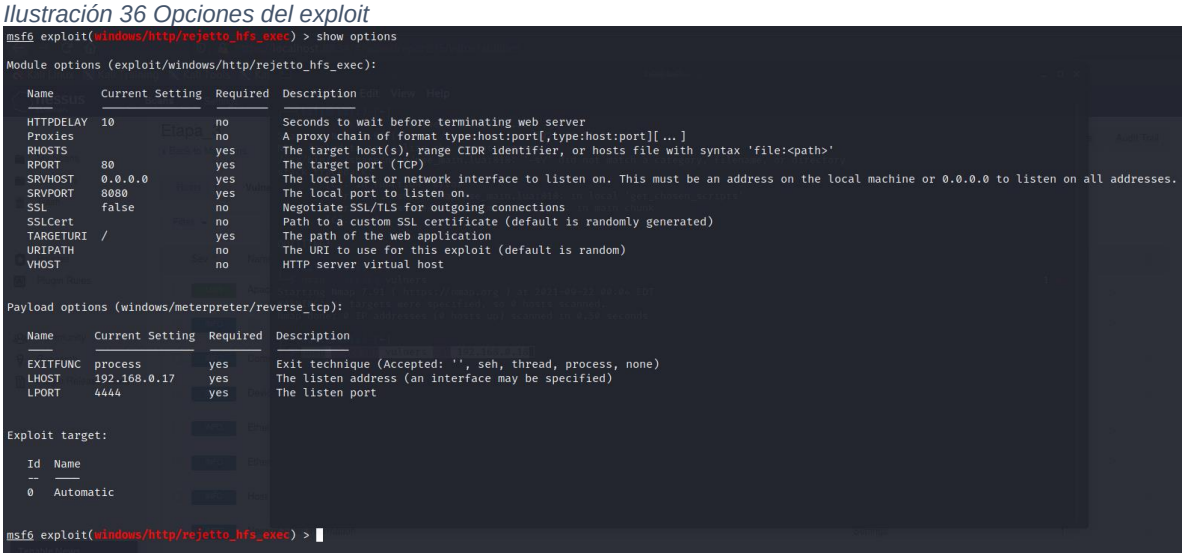
Buscamos los exploits asociados a un nombre característico de la aplicación vulnerable, o número de identificación del exploit.

Ilustración 35 Búsqueda de vulnerabilidades

Fuente: Propia.

Seleccionamos el exploit en la aplicación Metasploit Framework, y lo configuramos.

Ilustración 36 Opciones del exploit



Fuente: Propia.

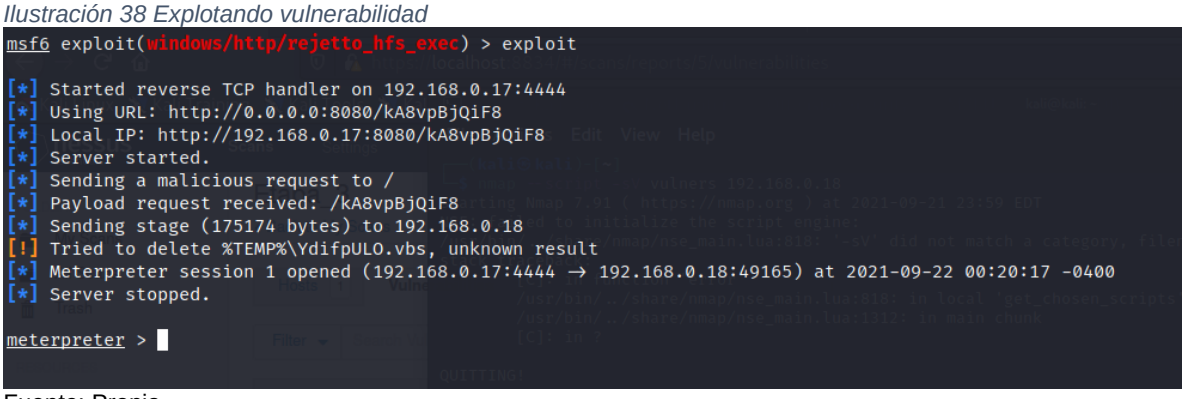
Configurar RHOSTS que es el host objetivo.

Ilustración 37 Configuración de host objetivo

Fuente: Propia.

Iniciamos la explotación de la vulnerabilidad.

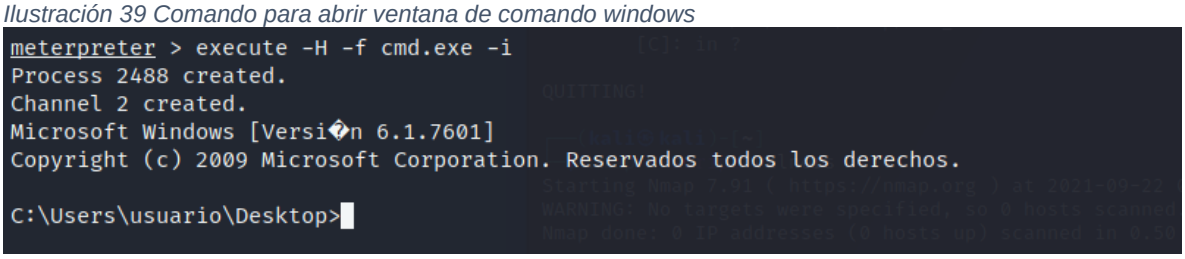
Ilustración 38 Explotando vulnerabilidad



Fuente: Propia.

Ya con la sesión del meterpreter, podemos ejecutar el siguiente comando para abrir una sesión de comandos.

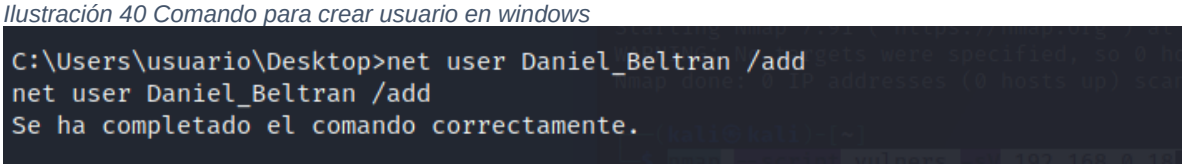
Ilustración 39 Comando para abrir ventana de comando windows



Fuente: Propia.

Podemos manipular la maquina Windows 7 desde la sesión de comandos, se crea el usuario

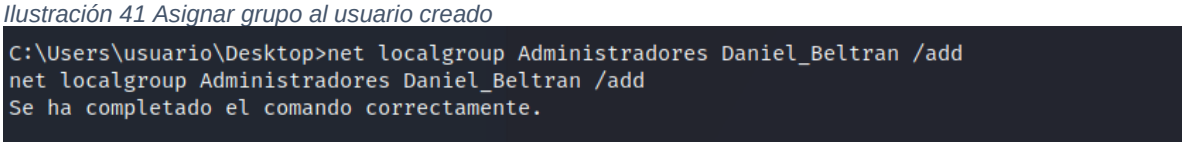
Ilustración 40 Comando para crear usuario en windows



Fuente: Propia.

Asignamos los permisos al usuario creado.

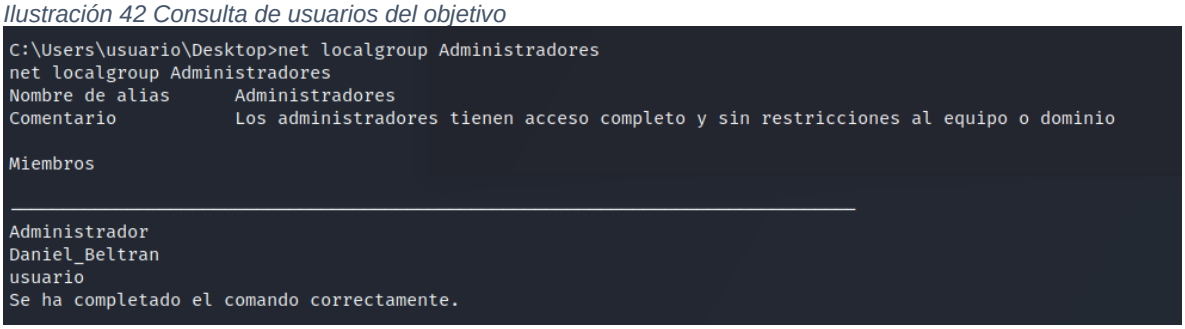
Ilustración 41 Asignar grupo al usuario creado



Fuente: Propia.

Verificamos los usuarios de la máquina.

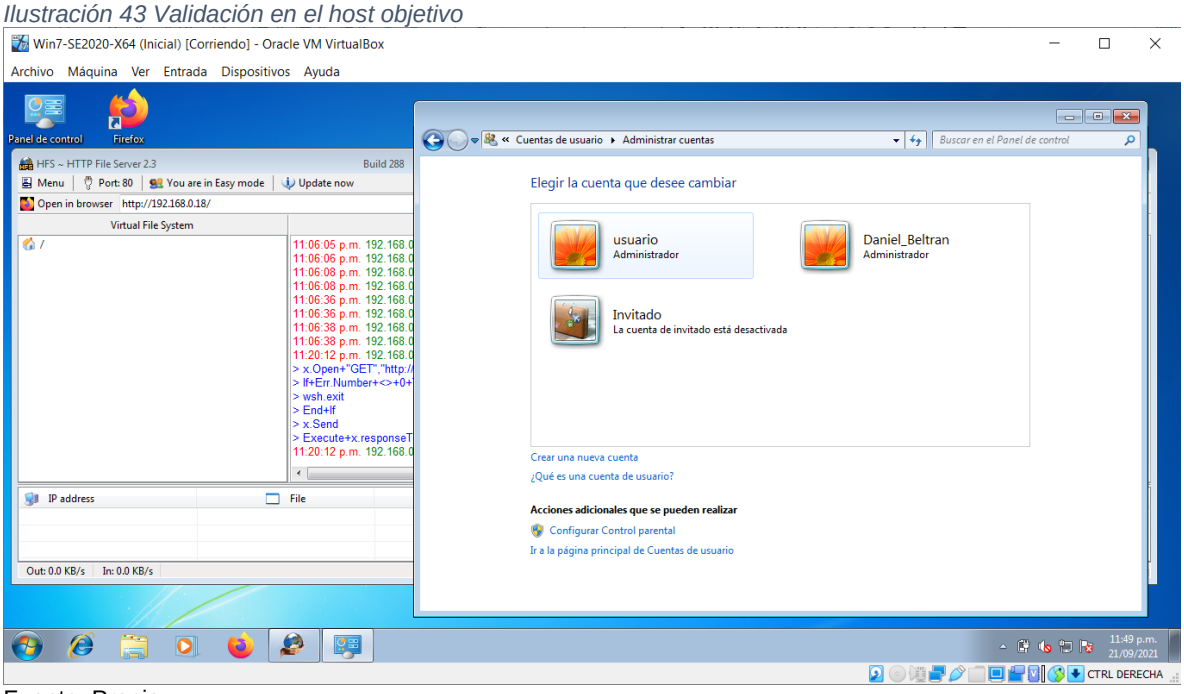
Ilustración 42 Consulta de usuarios del objetivo



Fuente: Propia.

Se verifican también el equipo por medio de las opciones de Windows.

Ilustración 43 Validación en el host objetivo



Fuente: Propia.

Si necesitamos elevar privilegios, que no fue el caso, desde el meterpreter ejecutamos los siguientes comandos.

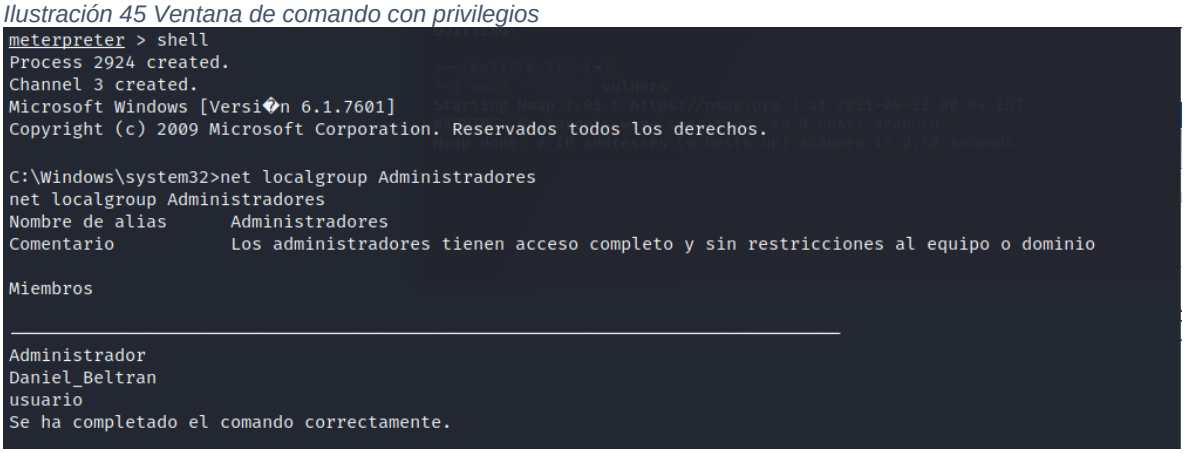
Ilustración 44 Elevación de privilegios

```
meterpreter > getuid
Server username: PC202006\usuario
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Fuente: Propia.

Igual que antes podemos abrir una sesión de comando con otro comando.

Ilustración 45 Ventana de comando con privilegios



Fuente: Propia.

2.4. ANÁLISIS BLUE TEAM

2.4.1. Análisis con acciones necesarias para contener un ataque en tiempo real.

En una organización inicialmente se debe identificar cual es el método de ataque o las posibles vulnerabilidades que se están explotaron. Esto se debe explorar de acuerdo con el modelo de seguridad que se tenga implementado, y sus pasos predefinidos para poder reducir los daños a la organización.

- Lo primero seria identificar mediante análisis de pentesting posibles focos que se encuentren activos, y poder detectar la vulnerabilidad explotada en los hosts comprometidos.
- Es esencial la identificación de los hosts comprometidos para poder aislarlos y no tener que deshabilitar todos los servicios o el resto de los dispositivos que hagan parte de la infraestructura tecnológica.
- Al contener el ataque a los dispositivos comprometidos podemos prevenir el pivoting el cual puede comprometer todos los demás sistemas que puedan tener conexión con los equipos comprometidos.
- Se realiza una copia forense de los equipos infectados para posteriormente poder analizarlos y detectar las vulnerabilidades explotadas, y entender el nivel de impacto que tuvo el ataque.
- Creando un ambiente controlado con las copias forenses utilizamos las diferentes herramientas gratuitas que existen para validar las vulnerabilidades de los equipos, podemos utilizar Metasploit, combinado con NMAP. También tenemos Armitage y otras.
- Validadas las vulnerabilidades con herramientas de pentesting, buscamos los posibles exploits utilizados en el ataque para poder ejecutar los

controles necesarios en los equipos o demás hosts de la red que puedan llegar a tener esta vulnerabilidad.

- Ya con la explotación ejecutada en el laboratorio, validamos que posibles afectaciones pudimos tener que no se tuvieron en cuenta, y validamos si necesitamos ampliar la búsqueda en algún equipo en producción que allá sido atacado posiblemente.

2.4.2. Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.

Ya con el proceso del laboratorio desarrollado por el grupo redteam, tienen claras varias falencias que se deben corregir para mitigar y reducir las vulnerabilidades de nuestro servidor.

Se tomarían las siguientes medidas de hardenización:

- Inicialmente debemos validar los usuarios que usan los dispositivos, ya que si no requieren tener privilegios de administración se deben suprimir y solo tener autorización a ejecutar lo autorizado.
- Actualizar todo el software que se esté usando, ya se sistema operativo, aplicaciones, antivirus, etc.
- Validar los puertos habilitados en el host, y corregir o cerrar todo posible puerto que pueda generar alguna vulnerabilidad.
- Validar los usuarios afectados, y cambiar las credenciales de estos.
- Verificar si todos los usuarios del dispositivo son necesarios, o solo se debería tener uno de consulta o producción.
- Implementar seguridad con un firewall, que permita la identificación de vulnerabilidades, como IDS, IPS, y otras.
- Implementar políticas de seguridad que permitan, limitar el alcance de los usuarios, y prevenir mediante estándares de configuración.
- Subdividir la red si es posible, para tener asilados servicios que no deban estar a posibles accesos malintencionados.

2.4.3. Análisis sobre las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos.

El equipo blueteam es normalmente un grupo interno que tiene la compañía, y se encuentra en constante búsqueda de las falencias y vulnerabilidades que se puedan encontrar sobre la infraestructura tecnológica de la empresa, de allí pueden aplicar o implementar procedimientos que permitan corregir estas fallas, el equipo blue team constantemente se encuentra monitorizando la infraestructura para detectar ataques en vivo, también tiene la tarea de implementar y desarrollar procedimientos que permita mejorar las políticas y estrategias del compañía en el área de seguridad informática.

El CSIRT está enfocado a la investigación e indagación sobre un evento, ya sea en vivo o que haya sucedido, y tiene similitud con el blueteam, ya que también deben evaluar y analizar la infraestructura tecnológica, pero además deben localizar los sistemas afectados y activar los sistemas de recuperación para restablecer los servicios tecnológicos de la compañía, sus principales objetivos son los de contener, erradicar y recuperar los sistemas de información ante algún evento de seguridad.

2.4.4. Análisis sobre la pertinencia de trabajar con CIS “Center For Internet Security” como propuesta de aseguramiento por parte de un equipo de Blue Team.

Primero tenemos dar la definición de CIS, esta es una organización sin fines de lucro impulsada por la comunidad, responsable de CIS Controls y CIS Benchmarks, las mejores prácticas reconocidas a nivel mundial para proteger los sistemas y datos de TI. Lideramos una comunidad global de profesionales de TI para hacer evolucionar continuamente estos estándares y proporcionar productos y servicios para protegerse de manera proactiva contra las amenazas emergentes. Nuestras CIS Hardened Images proporcionan entornos informáticos escalables, seguros y bajo demanda en la nube.[15]

Nos permite implementar pautas que puedan ser usadas para proteger los sistemas y dispositivos tecnológicos, como lo son configuraciones adecuadas en hardware o software, ya sean equipos de cómputo, dispositivos móviles o servidores.
Podemos utilizar las CIS para desarrollar una estructura del programa de seguridad de la información, y una normativa que permita una metodología de seguridad optima con funciones claras. Implementando estas buenas prácticas, podemos tener unas acciones defensivas que permitirán prevenir los ataques a la infraestructura tecnológica.

2.4.5. Análisis sobre las funciones y características principales de un SIEM.

Las principales características de SIEM son las de proveer análisis en tiempo real de alertas que puedan sean identificadas como peligrosas, ya sean generadas por equipos de redes o aplicaciones. Podemos definir que SIEM está basado en 2 métodos de administración, uno es el SIM que representa la Gestión de Información de Seguridad la cual está encargada almacenar la información, como también de analizarla, el otro es el SEM - Gestión de

[15] (Center for Internet Security, 2021)

Eventos de Seguridad este tiene como objetivo principal el monitoreo en tiempo real, validar los eventos si tiene relación.

Principales funciones:

- Identificar entre falsos positivos y ataques reales.
- Centraliza el monitoreo de todas las amenazas potenciales.
- Genera alertas redirigidas dependiendo de la clasificación de las alertas.
- Genera un análisis de conocimiento sobre los incidentes para una fácil resolución.
- Registra y documenta todas las etapas en un proceso de detención, actuación y resolución.
- Cumple con la legislación y normas actuales, en protección de datos y seguridad.

El software SIEM funciona recopilando datos de eventos y registros generados por las aplicaciones, los dispositivos de seguridad y los sistemas host de una organización y reuniéndolos en una única plataforma centralizada. SIEM recopila datos de eventos antivirus, registros de firewall y otras ubicaciones, clasifica estos datos en categorías.[16]

2.4.6. Informe de elección de 3 herramientas que permitan contener ataques informáticos.

- **Firewall**: Principal mente se podría implementar utilizando hardware que ya viene con licencias que permiten tener controles que ayudan a la contención de ataques, pero también existen las versiones open source como pfsense o opnsense, estos permiten implementar una seguridad perimetral e interna, dependiendo de su configuración limitando el tráfico que pueda estar en nuestra red, de acuerdo con los controles que se implemente. Tenemos controles de IPS, IDS, restricciones en puertos, bloqueos de hosts, etc.

- **Wazuh**: está catalogado como un SIEM, el cual es un excelente sistema de detección de intrusos, realiza análisis de los hosts, comprobando la integridad, detectando rootkits, también tiene generación de alertas, esta licenciada bajo software libre, y funciona en múltiples sistemas operativos.

- **OSSIM**: también es un SIEM, el cual se basa en un conjunto de herramientas, que se encuentra bajo licenciamiento libre, y sirve para administradores de red, ayuda a mejorar la seguridad, como también la

[16] (FIREEYE, 2021)

detección de intrusos y la prevención. Con controles de correlación, detalle a diferentes niveles, y reporte de incidentes.
SIEM de código abierto aborda esta realidad al proporcionar una plataforma unificada con muchas de las capacidades de seguridad esenciales que necesita, como:

- Descubrimiento de activos
- Evaluación de vulnerabilidad
- Detección de intrusiones
- Monitoreo de comportamiento
- Correlación de eventos SIEM[17]

2.5. ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM

Basados en las experiencias adquiridas es fundamental el trabajo en equipo y la planeación de las estrategias que se vayan a aplicar a los equipos. Algunos aspectos importantes serian:

- **Comunicación entre equipos**: Se debe tener un canal de comunicación entre los equipos para que se permita conocer los avances en cada aspecto de los equipos, como también las investigaciones que se estén adelantando.
- **Planes de acción**: Se debe tener documentadas las actividades que se estén realizando por parte de los equipos, para poder tener a detalle todas sus labores y realizar continuamente retroalimentación para mejorar procesos.
- **Capacitación**: Es fundamental tener una constante capacitación de los equipos, ya que las afectaciones cibernéticas se actualizan y mejoran en todo momento.
- **Pruebas**: Es fundamental tener prácticas de ataques, simulación de restauración de desastres, todo lo que conlleve a validar los panes que se tengan establecidos, y así recrear incidentes que puedan mejorar la respuesta de los equipos.

[17] (AT&T, 2021)

2.6. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN

- La implementación de los equipos Red team y Blue team, son primordiales cuando se vela por una infraestructura robusta, y tener estos 2 equipos trabajando por la protección de los sistemas, fortalece notablemente los aspectos de seguridad informática.
- Las políticas de seguridad son la pauta para lograr una mejor seguridad, ya que nos permite tener controles que podemos ir evaluando constantemente, y mejorar o actualizarlos.
- Es recomendable tener las configuraciones tanto de software como de los equipos, los mas orientadas a la seguridad, sin dejar escapar ningún dispositivo.
- Implementación los estándares de CIS, ayudaría a fortalecer las buenas practicas y mejorar notablemente la seguridad de los sistemas y dispositivos.
- Implementar sistemas de control SIEM, es muy recomendable ya que ayuda a identificar ataques, y centralizar el monitoreo de la infraestructura.
- Constante capacitación, tanto del personal de seguridad como de los empleados, con campañas de enseñanza, sobre las amenazas cibernéticas a las que pueden llegar a tener sus labores.
- La actualización y parcheo constante de nuestros sistemas, ya que son base fundamental para controlar las amenazas que surgen día a día.
- Implementación de sistemas de control como FIREWALL, VPN, Segmentación de las redes, y muchas más herramientas o metodologías que ayudan a mejorar la seguridad.

2.7. CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD

- La ciber seguridad es un área que siempre va a estar en constante evolución, y por eso es primordial que los profesionales de esta carrera se concienticen en lo importante que es la, mejora continua, ya que día a día se ven nuevas vulnerabilidades que pueden saltarse nuestras defensas cibernéticas.
- En este informe se plasma la importancia de los equipos Red team y Blue team, y lo importantes que son para las organizaciones, ya que constantemente velan por la protección de la información, ya sea analizando vulnerabilidades, o monitoreando la infraestructura.

- Es muy importante tener diferentes herramientas que permitan evaluar la seguridad, como vimos en este proyecto, existen muchas aplicaciones con diferentes propósitos, que nos ayudan a mejorar notablemente la seguridad informática, y como plus que existen muchas versiones libres a disposición.
- Es importante tener auditorias cada determinado tiempo, con un ente externo, ya que nos ayuda a romper paradigmas que a veces se crean, al realizar cotidianamente las mismas labores de seguridad.

CONCLUSIONES

- Reconocer e identificar las leyes y decretos que se rigen en la ley colombiana, referente a delitos informáticos y tratamiento de datos, para poder tener claro hasta dónde va la línea invisible que nos permite practicar actividades o simulaciones de ataques sin llegar a infringir las leyes estipuladas.

- Es muy importante para las compañías, practicar pruebas de penetración o auditarías de los sistemas, para identificar las vulnerabilidades y riesgos a los que están expuestos, y conocer las posibles afectaciones a las que tendrían lugar si llegan a ser víctimas de ciber delincuentes.

- Es indispensable conocer las etapas en las pruebas de penetración, como también las herramientas más comunes que se usan en estas actividades, ya que nuestra labor como especialistas en seguridad de la información nos llevan a siempre estar evaluando los sistemas que tengamos a nuestro cargo.

- Por medio de estas actividades, se puede conocer detalladamente los diferentes conceptos éticos que existen en el código de ética Copnia, y como debemos aplicar este manual, a las diferentes tareas que ejecutamos diariamente en el ámbito profesional.

- Se pudieron aplicar conceptos sobre las leyes y decretos que se rigen en la ley colombiana, referente a delitos informáticos y tratamiento de datos, esto validando las posibles infracciones que se pueden vulnerar según las actividades que se practiquen profesionalmente.

- Para las compañías es primordial, tener claras las leyes estipuladas en sus actividades operacionales, para no llegar a incurrir en ninguna actividad ilícita ante la ley, también se entiende que en algunos casos existen empresas que quieren aprovechar la ingenuidad o necesidad de los profesionales que acceden a ofertas laborales para realizar actividades poco éticas o ilícitas.

- En el desarrollo de estas pruebas técnicas, se pudo experimentar los procesos que se realizan desde el área de red team, y se culminó un proyecto de pentesting enmarcado en las buenas prácticas.

- También se profundizo en las aplicaciones de software utilizadas, y se pudieron mejorar los conocimientos sobres estas, como también el alcance que se tiene al usar solo software libre.

- Se pudo efectuar un análisis completo de un ataque a una maquina Windows 7, comprendiendo las vulnerabilidades que existen al tener herramientas y sistemas operativos desactualizados.

- Es muy importante para las compañías, tener implementadas las políticas de seguridad que ayudan a mitigar este tipo de vulnerabilidades.

- Podemos tener claro que el malware actual, requiere la ayuda de los usuarios para explotar las vulnerabilidades que puedan existir en nuestras plataformas, por eso debemos tener herramientas que nos permitan tener un análisis o monitoreo envió que ayuden a mitigar y evaluar la infraestructura tecnológica de las compañías.

- La imaginación de los hackers constantemente está en evolución, y por eso siempre existen nuevas vulnerabilidades día a día, por eso es indispensable tener equipos o implementación como las vistas en esta actividad para proteger nuestra información

REFERENCIAS

AT&T. (2021). *AT&T*. Obtenido de https://cybersecurity.att.com/products/ossim
Center for Internet Security. (10 de 2021). *Center for Internet Security*. Obtenido de https://www.cisecurity.org/about-us/

CONGRESO DE LA REPÚBLICA. (5 de ENERO de 2009). *secretariasenado.* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CVE. (29 de MARZO de 2021). *CVE*. Obtenido de https://cve.mitre.org/
FIREEYE. (2021). *FIREEYE*. Obtenido de https://www.fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html

Greenbone. (2021). Obtenido de https://www.openvas.org/
INFOSECURITY. (7 de OCTUBRE de 2021). *INFOSECURITY*. Obtenido de https://www.infosecuritymexico.com/es/ciberseguridad.html

Offensive Security. (2021). *The Exploit Database*. Obtenido de https://www.exploit-db.com/

ORACLE. (MAYO de 2021). *VIRTUAL BOX*. Obtenido de https://www.virtualbox.org/
QUINTERO, J. F. (4 de 9 de 2021). *UNAD.* Obtenido de https://campus109.unad.edu.co/ecbti95/pluginfile.php/680/mod_folder/content/0/Anexo%202%20-%20Escenario%202.pdf?forcedownload=1

QUINTERO, J. F. (6 de 9 de 2021). *UNAD.* Obtenido de https://campus109.unad.edu.co/ecbti95/pluginfile.php/682/mod_folder/content/0/Anexo%204%20-%20Escenario%203.pdf?forcedownload=1

QUINTERO, J. F. (26 de 8 de 2021). *UNAD.* Obtenido de https://campus109.unad.edu.co/ecbti95/pluginfile.php/677/mod_folder/content/0/Anexo%201%20-%20Escenario%201.pdf?forcedownload=1

QUINTERO, J. F. (20 de 9 de 2021). *UNAD.* Obtenido de https://campus109.unad.edu.co/ecbti95/pluginfile.php/684/mod_folder/content/0/Anexo%205%20-%20Escenario%204.pdf?forcedownload=1

QUINTERO, J. F. (20 de 9 de 2021). *UNAD.* Obtenido de https://campus109.unad.edu.co/ecbti95/pluginfile.php/687/mod_folder/content/0/An

exo%206%20-%20Escenario%205.pdf?forcedownload=1

SECURITY TWINS. (27 de 12 de 2021). *SECURITY TWINS*. Obtenido de https://securitytwins.com/2018/12/27/conociendo-a-meterpreter-i/

UNIR. (2021). *Universidad Internacional de La Rioja*. Obtenido de https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

BIBLIOGRAFÍA

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

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

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

EXPLOIT DATABASE. (s.f.) Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). Recuperado el 19 de 09 del 2021 de https://www.exploit-db.com/exploits/39161

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

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

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

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

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

Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Mintic. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

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

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

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

OFFENSIVE SECURITY. (s.f.) Privilege Escalation. Recuperado el 21 de 09 del 2021 de https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/

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

Red team notes 2.0. (2021). Rejetto HTTP File Server (HFS) 2.3. (s.f.). Recuperado el 19 de 09 del 2021 de https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/initial-access/t1190-exploit-public-facing-applications/rejetto-http-file-server-hfs-2.3

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

ANEXOS

- Anexo A Video sustentación:

https://youtu.be/bLVqYT_zIrw

- Anexo B Validación Turnitin

	Título de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud
Ver recibo digital	Etapa 5	1670742387	10/10/2021 23:25	14%